FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Una introducción a la cohomología de grupos

Rut Arias Ferreiros

2021-22

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Una introducción a la cohomología de grupos

Rut Arias Ferreiros

2021-22

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álxebra
Título: Introducción a la cohomología de grupos
Breve descrición do contido El objetivo de este trabajo es el estudio de los grupos de cohomología de un grupo G con coeficientes en un G-módulo. Se estudiarán estos grupos y se dará una interpretación de estos grupos para $n = 0, 1, 2$. También se estudiarán los módulos coinducidos y se probarán los teoremas de reducción. Se obtendrán algunos resultados clásicos de la teoría de grupos. Se deberán introducir previamente los conceptos de categoría, funtor, transformación natural y el funtor Hom en la categoría de módulos, así como los módulos proyectivos e inyectivos. También se deben estudiar algunas propiedades de funtores derivados.
Recomendacións
Outras observacións

Índice general

Resumen

El objetivo de este trabajo es el estudio de los grupos de cohomología $H^n(G, A)$ de un grupo G con coeficientes en un G-módulo a la izquierda A, utilizando los funtores derivados Ext^n_G. Se estudian propiedades de estos grupos, se da una interpretación para $n = 0$ y $n = 1$, en este último caso para G-módulos de coeficientes triviales y para un G-módulo cualquiera en términos de derivaciones. Se calcula la cohomología de los grupos cíclicos y se estudia la resolución estándar normalizada de $\mathbb{Z}$, que es muy útil en el estudio y cálculo de la cohomología. Se da una interpretación del segundo grupo de cohomología $H^2(G, A)$ en términos de extensiones de G por A utilizando el concepto de "factor set" de $G \times G$ en A. Finalmente, se prueba el teorema de Schur-Zassenhaus que afirma que si H es un subgrupo normal de un grupo finito E y m.c.d.$(|H|, |E/H|) = 1$, entonces el grupo E es isomorfo al producto semidirecto de H por E/H.

Abstract

The aim of this work is to study the cohomology groups $H^n(G, A)$ of G with coefficients in the G-module A, using the derived functors Ext^n_G. We study the properties of these groups and give an interpretation for $n = 0$ and $n = 1$, in this last case for trivial G-modules and for any G-module in terms of derivations. We compute the cohomology of ciclic groups and give a description of the normalized standard resolution of $\mathbb{Z}$, very useful in order to compute the cohomology. We prove that the second cohomology group $H^2(G, A)$ classifies extensions with abelian kernel, using the concept of "factor set". Finally, we prove the Schur-Zassenhaus theorem that states that if H is a normal subgroup of a finite group E, and H and E/H have coprime order, then E is isomorphic to the semidirect product of H by E/H.

Introducción

El nacimiento del álgebra homológica podría decirse que tuvo lugar al comienzo de la segunda guerra mundial con la formalización de las nociones de homología y cohomología de un espacio topológico. Algunos matemáticos, entre ellos Eilenberg. comprendieron que el mismo formalismo podía aplicarse a sistemas algebraicos y estos conceptos se extendieron a todas las áreas del álgebra. Esta fase de desarrollo comienza en 1956 con la publicación del libro Cartan y Eilenberg [2] en el que aparecen los conceptos de funtores derivados, módulos proyectivos y módulos inyectivos. Posteriormente aparecieron otros libros sobre el tema, el libro de MacLane [4], el libro de Hilton y Stammbach [3] y unas notas de Rotman posteriormente desarrolladas en el libro [6]. También cabe destacar el libro de Bourbaki N. [1] dedicado exclusivamente a este tema.

Los orígenes de la cohomología de grupos pueden encontrarse en la primera década del siglo XX en un trabajo de Schur sobre representaciones proyectivas y en el trabajo de Schreier de 1926 sobre extensiones de grupos. Su origen topológico yace en el descubrimiento de Hurewicz de 1936 de que si X es un espacio asférico, es decir un espacio conexo por caminos cuyos grupos de homotopía superior $\Pi_n(X)$ son nulos, para $n \geq 2$, entonces todos los grupos de homología y cohomología de X están determinados por el grupo fundamental $\Pi_1(X)$. Los grupos de cohomología de un grupo G con coeficientes en un G-módulo fueron introducidos por Eilenberg y MacLane en 1943, en relación con un teorema de Hopf sobre acciones de grupos fundamentales. Posteriormante se encontraron numerosas aplicaciones algebraicas y topológicas. Artin, Tate y Hochschild, entre otros, contribuyeron al estudio de esta teoría para grupos finitos y teoría de cuerpos de clases. Actualmente es esencial en cualquier enfoque moderno de la teoría algebraica de números y en geometría aritmética.

La memoria consta de dos capítulos, un primer capítulo de preliminares y un segundo capítulo dedicado a la cohomología de grupos, donde se utiliza sistemáticamente el lenguaje y resultados del capítulo anterior.

El objetivo fundamental del primer capítulo es introducir el conceptos de grupos de homología (resp. cohomología) de un complejo de cadenas (resp. cocadenas) de módulos y las propiedades de los funtores derivados Ext necesarias para el estudio de la cohomología

de grupos. Comienza con el estudio de algunos lemas clásicos sobre sucesiones exactas en una categoría de módulos, como el lema de los tres y el lema de la serpiente.

Se estudian las propiedades de exactitud del funtor Hom y se prueba la existencia de resoluciones proyectivas para cualquier módulo. Se estudia la homotopía entre complejos de cadenas (resp. cocadenas) y se prueba mediante el teorema de comparación que las resoluciones proyectivas de un módulo son únicas salvo una equivalencia de homotopía. Se prueba también la exactitud de la sucesión exacta larga de cohomología asociada a una sucesión exacta corta de complejos de cocadenas.

Para dos R-módulo a la izquierda M y N definimos

$$\mathrm{Ext}^n_R(M,N) = H^n(\mathrm{Hom}_R(\mathbf{P},N)), \quad n \in \mathbb{N}$$

es decir $\mathrm{Ext}^n_R(M,N)$ es el n-ésimo grupo de cohomología del complejo de cocadenas

$$\mathrm{Hom}(\mathbf{P},N)\colon 0 \to \mathrm{Hom}(P_0,N) \to \mathrm{Hom}(P_1,N) \to \cdots \to \mathrm{Hom}(P_n,N) \to \cdots$$

donde $\mathbf{P}$ es una resolución proyectiva de M. Se prueba que $\mathrm{Ext}^n_R(M,N)$ no depende de la resolución proyectiva de M considerada.

Utilizando la sucesión exacta de cohomología asociada a una sucesión exacta de complejos de cocadenas se prueba que si $0 \to M' \rightarrowtail M \to M'' \to 0$ es una sucesión exacta corta de R-módulos, se tiene una sucesión exacta larga de grupos abelianos

$$\cdots \to \mathrm{Ext}^n_R(M'',N) \to \mathrm{Ext}^n_R(M,N) \to \mathrm{Ext}^n_R(M',N) \to \mathrm{Ext}^{n+1}_R(M'',N) \to \cdots$$

y que si $0 \to N' \to N \to N'' \to 0$ es una sucesión exacta corta de R-módulos, se tiene una sucesión exacta larga de grupos abelianos

$$\cdots \to \mathrm{Ext}^n_R(M,N') \to \mathrm{Ext}^n_R(M,N) \to \mathrm{Ext}^n_R(M,N'') \to \mathrm{Ext}^{n+1}_R(M,N') \to \cdots$$

Estás sucesiones exactas largas se utilizan en capítulo II para el estudio de la cohomología de grupos.

El segundo capítulo comienza haciendo un estudio de los G-módulos y del anillo de grupo entero $\mathbb{Z}G$. Se introducen los grupos de cohomología de un grupo G con coeficientes en un G-módulo utilizando los funtores Ext^n:

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

Con el objeto de tener los elementos suficientes para dar una interpretación de los grupos del primer grupo de cohomología $H^1(G,A)$ se introduce el concepto clásico de derivación en grupos y se obtiene la representabilidad del funtor

$$\mathrm{Der}(G,-)\colon \colon \mathbf{Mod}_G \longrightarrow \mathbf{Ab}$$

por el ideal aumentación IG del anillo $\mathbb{Z}G$. Se da una interpretación de los grupos de cohomología en dimensiones 0 y 1 (en este último caso para módulos de coeficientes triviales) obteniendo además, para un G-módulo cualquiera una interpretación de $H^1(G,A)$ como cociente del grupo de derivaciones $\mathrm{Der}(G,A)$ por el subgrupo del derivaciones interiores.

Se estudia la relación entre derivaciones y producto semidirecto y a partir de ella se obtiene la anulación de los grupos de cohomología de un grupo libre cualquiera en dimensiones $n \geq 2$. En relación con este resultado, Stallings y Swan probaron que un grupo G es libre si, y solo si, $H^n(G,A) = 0$, para todo G-módulo A y todo $n \geq 2$; este resultado da una relación entre la cohomología de grupos y la teoría de grupos.

En la sección 4 se calcula la cohomología de los grupos cíclicos. Si $C_k = \langle \tau \rangle$ es un grupo cíclico finito de orden k y A es un C_k-módulo entonces se prueba que

$$H^n(C_k,A) \cong \begin{cases} \{a \in A \mid \tau\, a = a\}, \text{ para } n = 0 \\ \{a \in A \mid N\, a = 0\}/(\tau - \mathbf{1})\, A, \text{ para } n = 1,3,5,7,\ldots \\ \{a \in A \mid \tau\, a = a\}/NA, \text{ para } n = 2,4,6,8,\ldots \end{cases}$$

Se dice que los grupos cíclicos finitos tienen cohomología periódica.

En la sección 5 se estudia la resolución $\mathbf{B}$ estándar o barra de $\mathbb{Z}$ que es muy útil en el estudio y cálculo de la cohomología. Por ejemplo, utilizando esta resolución se prueba que si G es un grupo finito y A es un G-módulo, entonces

$$|G|\, H^n(G,A) = 0, \quad n > 0,$$

y en particular se prueba que todos los elementos de $H^n(G,A)$ tienen orden finito que es un divisor del orden de G. Como corolario se obtiene la anulación de los grupos de cohomología para $n > 0$ de un grupo finito G con coeficientes en un G-módulo finito A cuando m.c.d.$(|G|,|A|) = 1$.

En 1926, Schereir resolvió el problema de extensión. El problema de extensión consiste en encontrar, dado un grupo abeliano A y un grupo G, todos los grupos E tales que $0 \to A \to E \to G \to 0$ sea una sucesión exacta corta. La prueba de Schreier consiste en obtener suficientes propiedades de una extensión de G por A, de forma que permitan reconstruirla. La demostración utiliza el concepto de "factor set". Un factor set es una aplicación $f\colon G \times G \to A$ que verifica

$$x \circ f(y,z) + f(x,yz) = f(x,y) + f(xy,z), \quad f(x,\mathbf{1}) = f(\mathbf{1},y) = 0, \quad x,y,z \in G.$$

En la sección 6 se da una interpretación del segundo grupo de cohomología $H^2(G,A)$ en término de extensiones de G por A que se basa en la de Schreier. Para ello se identifica el conjunto de 2-ciclos $Z^2(G,A)$ del complejo $\mathrm{Hom}_G(\mathbf{B},A)$, siendo $\mathbf{B}$ la resolución estándar

de $\mathbb{Z}$, con el conjunto de factor sets de $G \times G$ en A y se asocia a cada extensión de G por A un factor set. Se dice que las extensiones $0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ y $0 \to A \xrightarrow{i'} E' \xrightarrow{p'} G \to 1$ son equivalentes si existe un homomorfismo de grupos $h\colon E \to E'$ tal que el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle h} & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{i'} & E' & \xrightarrow{p'} & G & \longrightarrow & 1 \end{array}$$

es conmutativo. Si denotamos por $\mathrm{M}(G, A)$ el conjunto de clases de equivalencia de extensiones de G por A, se prueba que existe una aplicación biyectiva

$$\begin{array}{rccc} \Delta: & M(G,A) & \longrightarrow & H^2(G,A) \\ & [E] & \rightsquigarrow & [f] \end{array}$$

dada por $\Delta(E) = [f]$, siendo f un factor set asociado a E.

En la última sección se define el producto semidirecto $H \rtimes_\sigma G$ de un grupo H por un grupo G con un homomorfismo de grupos $\sigma\colon G \to \mathrm{Aut}(H)$. El objetivo de esta sección es probar el teorema de Schur-Zassenhauss. El teorema de Schur-Zassenhaus afirma que si si H es un subgrupo normal de un grupo finito E y $\mathrm{m.c.d.}(|H|, |E/H|) = 1$, entonces E es isomorfo al producto semidirecto de H por E/H.

La demostración se hace primero en el caso en que H es un grupo abeliano utilizando que si $\mathrm{m.c.d.}(|G|, |A|) = 1$, entonces $H^2(G, A) = 0$ y la biyección entre $H^2(G, A)$ y el conjunto de clases de equivalencia de extensiones. Si H no es abeliano, el teorema se demuestra por inducción sobre el orden de H, utilizando el caso abeliano y los teoremas de Sylow.

Una clase de módulos, además de la clase de los módulos inyectivos, donde los grupos de cohomología se anulan para $n \geq 1$ es la clase de los módulos coinducidos. Estudiamos este tipo de módulos y estudiamos la estructura de G-módulo por acción diagonal lo que permite demostrar un teorema de reducción para cohomología.

Agradecimientos

Me gustaría agradecer a mi tutora, María Jesús Vale Gonsalves, todo el apoyo que me ha brindado en la realización de este trabajo; por todo lo que me ha enseñado e incentivado durante estos últimos años.

Capítulo 1

Preliminares

1.1. Categorías

En esta sección vamos a introducir los conceptos de teoría de categorías necesarios para la comprensión de este trabajo.

Definición 1.1. Una categoría $\mathcal{C}$ es una clase $\mathrm{Obj}(C)$ cuyos elementos e llaman objetos, tal que para cada par de objetos (X, Y) de $\mathcal{C}$ se tiene un conjunto $\mathcal{C}(X, Y)$ y para cada terna de objetos X, Y, y Z se tiene una ley de composición

$$\begin{array}{rcl} \circ : \mathcal{C}(X,Y) \times \mathcal{C}(Y,Z) & \longrightarrow & \mathcal{C}(X,Z) \\ (\ f\ ,\ g\ ) & \longmapsto & g \circ f \end{array}$$

verificando los siguientes axiomas:

(1) $\mathcal{C}(X_1, Y_1) \cap \mathcal{C}(X_2, Y_2) = \varnothing$, si $X_1 \neq X_2$ o $Y_1 \neq Y_2$.

(2) Dados $f \in \mathcal{C}(X, Y)$, $g \in \mathcal{C}(Y, Z)$ y $h \in \mathcal{C}(Z, T)$, entonces

$$h \circ (g \circ f) = (h \circ g) \circ f$$

(3) Para cada objeto X existe un morfismo $\mathrm{id}_X \in \mathcal{C}(X, X)$ tal que para cada $f \in \mathcal{C}(X, Y)$ y cada $g \in \mathcal{C}(Y, X)$,

$$f \circ \mathrm{id}_X = f, \qquad \mathrm{id}_X \circ g = g.$$

Los elementos de $\mathcal{C}(X, Y)$ se llaman morfismos de X a Y, el morfismo id_X se llama identidad y el axioma (2), asociatividad de la composición. Si $f \in \mathcal{C}(X, Y)$, escribiremos $f : X \to Y$. Se dice que un morfismo $f \in \mathcal{C}(X, Y)$ es un isomorfismo, si existe un morfismo $g \in \mathcal{C}(Y, X)$, tal que $g \circ f = \mathrm{id}_X$ y $f \circ g = \mathrm{id}_Y$, y denotaremos con frecuencia g por f^{-1}.

Ejemplos 1.2. (1) La categoría **Sets** es la categoría cuyos objetos son los conjuntos, sus morfismos son las aplicaciones entre conjuntos y la composición es la composición usual de aplicaciones.

(2) La categoría **Gr** es aquella cuyos objetos son los grupos, los morfismos son los homomorfismos de grupos y la composición es la composición de aplicaciones usual.

(3) La categoria **Ab** es aquella cuyos objetos son los grupos abelianos, los morfismos son los homomorfismos de grupos abelianos y la composición es la composición de aplicaciones usual.

(4) La categoría **Top** es la que tiene como objetos los espacios topológicos, los morfismos son las aplicaciones continuas y la composición es la usual.

Definición 1.3. Sean $\mathcal{C}$ y $\mathcal{D}$ categorías. Un funtor covariante F de $\mathcal{C}$ a $\mathcal{D}$ y se denota por $F : \mathcal{C} \to D$ es una correspondencia que asigna a cada objeto X en $\mathcal{C}$ un objeto $F(X)$ en $\mathcal{D}$ y a cada morfismo $f \in \mathcal{C}(X, Y)$ un morfismo $F(f) \in \mathcal{D}(F(X), F(Y))$ y que verifica las siguientes condiciones:

(1) Para cada $f \in \mathcal{C}(X, Y)$ y $g \in \mathcal{C}(Y, Z)$ se tiene

$$F(g \circ f) = F(g) \circ F(f)$$

(2) Para cada objeto X in $\mathcal{C}$, se tiene que $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$.

Definición 1.4. Sean $\mathcal{C}$ y $\mathcal{D}$ categorías. Un funtor contravariante F de $\mathcal{C}$ a $\mathcal{D}$ y se denota por $F : \mathcal{C} \to D$ es una correspondencia que asigna a cada objeto X en $\mathcal{C}$ un objeto $F(X)$ en $\mathcal{D}$ y a cada morfismo $f \in \mathcal{C}(X, Y)$ un morfismo $F(f) \in \mathcal{D}(F(Y), F(X))$ y que verifica las siguientes condiciones:

(1) Para cada $f \in \mathcal{C}(X, Y)$ y $g \in \mathcal{C}(Y, Z)$ se tiene

$$F(g \circ f) = F(f) \circ F(g)$$

(2) Para cada objeto X in $\mathcal{C}$, se tiene que $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$.

Ejemplos 1.5. (1) Sea $\mathcal{C}$ una categoría y X un objeto de $\mathcal{C}$. La correspondencia $F\colon \mathcal{C} \to$ **Sets** que asigna a cada objeto $Y \in \mathcal{C}$ el conjunto $F(Y) = \mathcal{C}(X, Y)$ y a cada morfismo $f : X \to Y$ la aplicación $F(f) : \mathcal{C}(X, Y) \to \mathcal{C}(X, Y')$ dada por $F(f)(g) = g \circ f$, es un funtor covariante. Denotaremos F por $\mathcal{C}(X, -)$ y $F(f)$ por $\mathcal{C}(X, f)$ o por f_*.

(2) Sea $\mathcal{C}$ una categoría y Y un objeto de $\mathcal{C}$. La correspondencia $G\colon \mathcal{C} \to \mathbf{Sets}$ que asigna a cada objeto $X \in \mathcal{C}$ el conjunto $G(X) = \mathcal{C}(X, Y)$ y a cada morfismo $f\colon X \to X'$ la aplicación $G(f) : \mathcal{C}(X', Y) \to \mathcal{C}(X, Y)$ dada por $G(f)(g) = g \circ f$, es un funtor contravariante. Denotaremos G por $\mathcal{C}(-, Y)$ y $G(f)$ por $\mathcal{C}(f, Y)$ o por f^*.

Definición 1.6. Sean F y G funtores de $\mathcal{C}$ a $\mathcal{D}$. Una transformación natural $t\colon F \to G$ es una colección de morfismos $t_X\colon F(X) \to G(X)$, uno para cada objeto X in $\mathcal{C}$, tal que para cada morfismo $f : X \to Y$ en $\mathcal{C}$, el diagrama

$$\begin{array}{ccc} F(X) & \xrightarrow{t_X} & G(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle F(g)} \\ F(Y) & \xrightarrow{t_Y} & G(Y) \end{array}$$

es conmutativo. Si t_X es un isomorfismo para cada $X \in \mathcal{C}$, entonces se dice que t es una equivalencia natural y que los funtores F y G son naturalmente equivalentes.

Definición 1.7. Sea $\mathcal{C}$ una categoría. Se dice que un objeto 0 es un objeto cero de $\mathcal{C}$ si para todo objeto X en $\mathcal{C}$ los conjuntos $\mathcal{C}(X, 0)$ y $\mathcal{C}(0, X)$ tienen cada uno un único elemento. Sea $\mathcal{C}$ una categoría con objeto cero 0. Cada conjunto $\mathcal{C}(X, Y)$ tiene un morfismo que es la composición de los morfismos $X \to 0$ y $0 \to Y$ y se llama morfismo cero de X en Y y se denota por $0 : X \to Y$.

Dos objetos cero de $\mathcal{C}$ son isomorfos. El morfismo cero no depende del objeto cero considerado.

Definición 1.8. Llamaremos categoría preaditiva a una categoría con objeto cero en la cual el conjunto $\mathcal{C}(X, Y)$ es un grupo abeliano y donde la composición

$$\begin{array}{rcl} \circ\colon \mathcal{C}(X,Y) \times \mathcal{C}(Y,Z) & \longrightarrow & \mathcal{C}(X,Z) \\ (\, f \quad , \quad g\,) & \longmapsto & f \circ g \end{array}$$

es bilineal, es decir

$$(f + f') \circ g = f \circ g + f' \circ g, \quad f \circ (g + g') = f \circ g + f \circ g', \quad f, f' \in \mathcal{C}(X, Y), \;\; g, g' \in \mathcal{C}(Y, Z).$$

Definición 1.9. Sean $\mathcal{C}$ y $\mathcal{D}$ categorías preaditivas. Se dice que un funtor $F : \mathcal{C} \to \mathcal{D}$ es aditivo si para cualesquiera objetos X y Y en $\mathcal{C}$ y morfismos $f, g \in \mathcal{C}(X, Y)$ se tiene

$$F(f + g) = F(f) + F(g)$$

Lema 1.10. *Si $\mathcal{C}$ es una categoría preaditiva el elemento neutro de $\mathcal{C}(X,Y)$ es el morfimo cero $0: X \to Y$ en $\mathcal{C}$ y si $F: \mathcal{C} \to \mathcal{D}$ es un funtor aditivo, entonces F lleva morfismos cero a morfismos cero.*

Demostración. Si $f \in \mathcal{C}(Y,Z)$, entonces $f \circ 0 = 0$. Se tiene

$$0 + 0 = \mathrm{id}_Y \circ 0 + \mathrm{id}_Y \circ 0 = (\mathrm{id}_Y + \mathrm{id}_Y) \circ 0 = 0.$$

y entonces 0 es el elemento neutro de $\mathcal{C}(X,Y)$. Además,

$$F(0) = F(0+0) = F(0) + F(0),$$

luego $F(0) = 0$. □

1.2. Módulos

Sean R y S anillos unitarios. La aplicación $f: R \to S$ es un homomorfismo de anillos si verifica que $f(r_1 + r_2) = f(r_1) + f(r_2)$, $f(r_1\, r_2) = f(r_1)\, f(r_2)$, $f(1) = 1$. Los endomorfismos de un grupo abeliano M, que denotaremos por End(M), forman un anillo unitario con las operaciones adición y multiplicación dadas por:

$$(f+g)(m) = f(m) + g(m), \quad (f \circ g)(m) = f(g(m)), \quad f, g \in En(M), \quad m \in M.$$

Definición 1.11. Sea R un anillo unitario. Un R-módulo a la izquierda es un grupo abeliano M junto con un homomorfismo de anillos $\alpha\colon R \to \mathrm{End(M)}$.

Si denotamos $(\alpha(r))(m)$ por $r\, m$, la aplicación o *acción de R sobre M*, $\bar{\alpha}\colon R \times M \to M$, dada por $\bar{\alpha}(r,m) = r\, m$ verifica las siguientes propiedades

M1: $(r_1 + r_2)\, m = r_1\, m + r_2\, m$

M2: $(r_1\, r_2)\, m = r_1\, (r_2\, m)$

M3: $r\, (m_1 + m_2) = r\, m_1 + r\, m_2$

M4: $1\, m = m$

para todo $m, m_1, m_2 \in M$, $r, r_1, r_2 \in R$. Recíprocamente, dada una aplicación $\bar{\alpha}\colon R \times M \to M$ que verifica las condiciones $M1$, $M2$, $M3$ y $M4$, si denotamos $\bar{\alpha}(r,m)$ por $r\, m$, entonces la aplicación $\alpha\colon R \to \mathrm{End}_{\mathbb{Z}}(\mathrm{M})$, dada por $(\alpha(r))(m) = m\, r$, es un homomorfismo de anillos.

Por comodidad en este capítulo, utilizaremos el término R-módulos para referirnos a los R-módulos a la izquierda.

Definición 1.12. Sean M y N R-módulos. Un homomorfismo $f\colon M \to N$ de R-módulos es un homomorfismo de grupos abelianos que verifica que $f(r\,m) = r\,f(m)$, para todo $r \in R$, $m \in M$.

La aplicación identidad de M es un homomorfismo de R-módulos que denotaremos por $\mathrm{id}_M\colon M \to M$ y la composición de homomorfismos de R-módulos es un homomorfismo de R-módulos.

Si M y N son R-módulos a la izquierda el conjunto de homomorfismos de R-módulos a la izquierda de M en N, que denotaremos por $\mathrm{Hom}_R(M,N)$, tiene estructura de grupo abeliano con la operación

$$(f+g)(m) = f(m) + g(m), \quad f,g \in \mathrm{Hom}_R(M,N), \quad m \in M.$$

Denotaremos por $\mathbf{Mod}_R$ la categoría de R-módulos. Los objetos de $\mathbf{Mod}_R$ son los R-módulos por la izquierda, $\mathbf{Mod}_R(M,N) = \mathrm{Hom}_R(M,N)$ y la composición es la usual. La categoría de R-módulos a la izquierda es una categoría preadiva. El objeto cero es el módulo cero.

Se tiene el funtor covariante aditivo

$$\mathbf{Mod}_R(M,-)\colon \mathbf{Mod}_R \to \mathbf{Ab}$$

que denotaremos por $\mathrm{Hom}_R(M,-)$ y si $h\colon N_1 \to N_2$ es un homomorfismo de R-módulos, denotaremos por h_* el homomorfismo de grupos abelianos $\mathrm{Hom}_R(M,h) : \mathrm{Hom}(M,N_1) \to \mathrm{Hom}(M,N_2)$, $h_*(f) = h \circ f$. Análogamente, se tiene un funtor contravariante aditivo

$$\mathbf{Mod}_R(-,N)\colon \mathbf{Mod}_R \to \mathbf{Ab}$$

que denotaremos por $\mathrm{Hom}_R(-,N)$ y si $h\colon M_1 \to M_2$ es un homomorfismo R-módulos, denotaremos por h^* el homomorfismo de grupos abelianos $\mathrm{Hom}_R(h,N)\colon \mathrm{Hom}(M_2,N) \to \mathrm{Hom}(M_1,N)$, $h^*(f) = f \circ h$.

Si f es inyectivo, utilizaremos a veces el símbolo $f : M \rightarrowtail N$ y si f es sobreyectivo el símbolo $f : M \twoheadrightarrow N$. Decimos que $f : M \to N$ es un isomorfismo de R-módulos si es un isomorfismo en la categoría $\mathbf{Mod}_R$. Se tiene que f es un isomorfismo de R-módulos si es un homomorfismo sobreyectivo e inyectivo. Si existe un isomorfismo de R-módulos $f\colon M \to N$, entonces se dice que M y N son R-módulos isomorfos y se denota por $M \cong N$.

Sea M un R-módulo. Se dice que M' es un submódulo de M si M' es un subgrupo de M y si para cada $m \in M'$ y $r \in R$ se tiene que $r\,m \in M'$. Si M' es un submódulo de M el grupo cociente M/M' es un R-módulo donde

$$r\,(m + M') = r\,m + M'.$$

Se tiene un homomorfismo inyectivo $i : M' \rightarrowtail M$ y un homomorfismo sobreyectivo $p : M \twoheadrightarrow M/M'$. Si $f : M \to N$ es un homomorfismo de R-módulos el conjunto $\ker f = \{m \in M \mid f(m) = 0\}$ es un submódulo de M y el conjunto $\operatorname{im} f = f(M) = \{f(m) \mid m \in M\}$ es un submódulo de N. La aplicación $\bar{f} : M/\ker f \to \operatorname{im} f$ dada por $\bar{f}(m+\ker f) = f(m)$, es un isomorfismo de R-módulos. El R-módulo $N/f(M)$ se llama conúcleo de f y lo denotaremos por $\operatorname{coker} f$.

Si M_1 y M_2 son submódulos de M y $M_1 \subset M_2$, entonces se tiene un isomorfismo de R-módulos

$$\frac{M/M_2}{M_1/M_2} \cong M/M_1.$$

Definición 1.13. Sean $f_1 \colon M_1 \to M_2$ y $f_2 \colon M_2 \to M_3$ homomorfismos de R-módulos. Se dice que la sucesión $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$ *es exacta en* M_2 si $\ker f_2 = \operatorname{im} f_1$. Se dice que la sucesión $M_0 \to M_1 \cdots \to M_n \to M_{n+1}$ *es exacta*, si es exacta en $M_1, M_2, \ldots, M_n$.

La sucesión $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ es exacta si, y solo si, f_1 es un homomorfismo inyectivo, $\ker f_2 = f_1(M_1)$ y f_2 es un homomorfismo suprayectivo. Si la sucesión $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ es exacta, entonces se dice que es una sucesión *exacta corta.*

Definición 1.14. La sucesión exacta corta de R-módulos $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ se dice que *rompe* si existe un homomorfismo de R-módulos $s \colon M_3 \to M_2$ tal que $f_2 \circ s = 1$.

Definición 1.15. Sean M_1, M_2, M_3 y M_4 R-módulos y sean f_1, f_2, h_1 y h_2 homomorfismos de R-módulos. Decimos que el diagrama

$$\begin{array}{ccc} M_1 & \xrightarrow{f_1} & M_2 \\ {\scriptstyle h_1}\downarrow & & \downarrow{\scriptstyle h_2} \\ N_1 & \xrightarrow{f_2} & N_2 \end{array}$$

es conmutativo si $h_2 \circ f_1 = f_2 \circ h_1$.

Lema 1.16. (Lema de los tres) *Consideremos el siguiente diagrama conmutativo donde las filas son sucesiones exactas cortas de R-módulos*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \longrightarrow & 0 \\ & & {\scriptstyle h_1}\downarrow & & \downarrow{\scriptstyle h_2} & & \downarrow{\scriptstyle h_3} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \longrightarrow & 0 \end{array}$$

Si dos cualesquiera de los homomorfismos h_1, h_2 y h_3 son isomorfismos, entonces el tercero es también isomorfismo.

Demostración. Solo probaremos uno de los tres posibles casos, ya que los otros dos son análogos. Supongamos que h_1, h_3 son isomorfismos; tenemos que ver que h_2 es un isomorfismo. Primero veamos que $\ker f = 0$. Si $m_2 \in \ker h_2$, entonces $0 = (g_2 \circ h_2)(m_2) = (h_3 \circ f_2)(m_2) = h_3(f_2(m_2))$. Dado que h_3 es un isomorfismo, se sigue que $f_2(m_2) = 0$. Por la exactitud de la sucesión superior, existe $m_1 \in M_1$ con $f_1(m_1) = m_2$. Entonces $0 = h_2 \circ f_1(m_1) = g_1 \circ h_1(m_1)$. Dado que la composición $g_1 \circ h_1$ es inyectiva, se sigue que $m_1 = 0$. Por lo tanto $m_2 = f_1(m_1) = 0$.

En segundo lugar veamos que h_2 es sobreyectivo. Sea $n_2 \in N_2$. Tenemos que probar que $n_1 = h_2(m_2)$ para algún $m_2 \in M_2$. Dado que h_3 es un isomorfismo, entonces existe $m_3 \in M_3$ con $h_3(m_3) = g_2(n_2)$. Dado que f_2 es sobreyectiva, entonces existe $m_2' \in M_2$ tal que $f_2(m_2') = m_3$. Obtenemos que $g_2(n_2 - h_2(m_2')) = 0$. Por la exactitud de la fila inferior existe $n_1 \in N_1$ con $g_1(n_1) = n_2 - h_2(m_2')$. Como h_1 es isomorfismo, existe $m_1 \in M_1$ tal que $h_1(m_1) = n_1$. Se tiene

$$h_2(f_1(m_1) + m_2') = (g_1 \circ h_1)(m_1) + h_2(m_2') = g_1(n_1) + h_2(m_2') = n_2.$$

Poniendo $m_2 = f_1(m_1) + m_2'$, tenemos que $h_2(m_2) = n_2$.

□

Lema 1.17. (Lema de la serpiente) *Consideremos el siguiente diagrama conmutativo donde las filas son sucesiones exactas de R-módulos*

$$\begin{array}{ccccccccc} & & M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle h_1} & & \downarrow{\scriptstyle h_2} & & \downarrow{\scriptstyle h_3} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & & \end{array}$$

Existe un homomorfismo $\omega\colon \ker h_3 \to \operatorname{coker} h_1$*, que llamaremos homomorfismo de conexión, tal que la siguiente sucesión es exacta:*

$$\ker h_1 \xrightarrow{{f_1}^k} \ker h_2 \xrightarrow{{f_2}^k} \ker h_3 \xrightarrow{\omega} \operatorname{coker} h_1 \xrightarrow{{g_1}^c} \operatorname{coker} h_2 \xrightarrow{{g_2}^c} \operatorname{coker} h_3$$

Donde f_1^k *y* f_2^k *son los homomorfismos inducidos por* f_1 *y* f_2 *entre los núcleos de* h_1 *y* h_2*, respectivamente y* g_1^c *y* g_2^c *son los homomorfismos inducidos por* g_1 *y* g_2 *entre los conúcleos de* h_1 *y* h_2*.*

Demostración. Tenemos que demostrar que existe un homomorfismo $\omega\colon \ker h_3 \to \operatorname{coker} h_1$ "conectando" estas dos sucesiones. La aplicación ω se define de la siguiente manera:

Sea $m_3 \in \ker h_3$, tomamos $m_2 \in M_2$ con $f_2(m_2) = m_3$. Dado que $(g_2 \circ h_2)(m_2) = h_3(f_2(m_2)) = h_3(m_3) = 0$ existe $n_1 \in N_1$ con $h_2(m_2) = g_1(n_1)$. Definimos $\omega(m_3) = [n_1] = n_1 + \operatorname{im} h_1 \in \operatorname{coker} h_1$.

Veamos que ω está bien definido, es decir, que $\omega(m_3)$ es independiente de la elección de m_2. Sea $m_2' \in M_2$ con $f_2(m_2') = m_3$ y $n_1' \in N_1$ tal que $h_2(m_2') = g_1(n_1')$. Se tiene que existe $m_1 \in M_1$ tal que $m_2' = m_2 + f_1(m_1)$, luego

$$g_1(n_1') = h_2 m_2' = h_2(m_2 + f_1 m_1) = h_2 m_2 + = g_1 h_1 m_1 = g_1 n_1 + g_1 h_1 m_1 = g_1(n_1 + h_1 m_1).$$

Por ser g_1 un homomorfismo inyectivo, $n_1' = n_1 + h_1(m_1)$ y entonces $[n_1'] = [n_1]$. Claramente δ es un homomorfismo.

Veamos la exactitud en $\ker h_3$. Si $m_3 \in \operatorname{im} f_2^k$, entonces existe $m_2 \in \ker h_2$ tal que $m_3 = f_2(m_2)$. Por tanto, $0 = h_2(m_2) = g_1(n_1)$ y dado que g_1 es un homomorfismo inyectivo, $n_1 = 0$ y entonces $\omega(m_3) = [n_1] = 0$. Así, $\operatorname{im} f_2^k \subset \ker \omega$.

Si $m_3 \in \ker \omega$ y $m_3 = f_2(m_2)$, $h_2(m_2) = g_1(n_1)$, entonces $\omega(m_3) = [n_1] = 0$, con lo cual existe $m_1 \in M_1$ con $h_1(m_1) = n_1$. Consideremos $m_2' = m_2 - f_1(m_1)$. Claramente $f_2(m_2') = m_3$ y $m_2' \in \ker h_2$, puesto que

$$h_2(m_2') = h_2(m_2) - (h_2 \circ f_1)(m_1) = h_2(m_2) - g_1(n_1) = 0.$$

Así, $\ker \omega \subset \operatorname{im} f_2^k$.

Veamos la exactitud en $\operatorname{coker} h_1$. Sea $\omega(m_3) = [n_1]$, $m_3 = f_2(m_2)$, $h_2(m_2) = g_1(n_1)$. Se tiene

$$g_1^c[n_1] = [g_1(n_1)] = [h_2(m_2)] = 0.$$

Por tanto, $\operatorname{im} \omega \subset \ker g_1^c$.

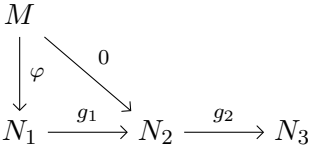
Si $[n_1] \in \operatorname{coker} h_1$ y $g_1^c[n_1] = [g_1(n_1)] = 0$. entonces $g_1(n_1) \in \operatorname{im} h_2$, de donde se sigue que existe $m_2 \in M_2$ tal que $g_1(n_1) = h_2(m_2)$. Pongamos $m_3 = f_2(m_2)$. Se tiene que $m_3 \in \ker h_3$, puesto que $h_3(m_3) = h_3 f_2 m_2 = g_2 h_2 m_2 = g_2 g_1(n_1) = 0$, y $\omega(m_3) = [n_1]$. Así, $\ker g_1^c = \operatorname{im} \omega$. □

Proposición 1.18. *Sea $0 \to N_1 \xrightarrow{g_1} N_2 \xrightarrow{g_2} N_3 \to 0$ una sucesión exacta corta de R-módulos. Para todo R-módulo M la sucesión de grupos abelianos inducida*

$$0 \to \operatorname{Hom}_R(M, N_1) \xrightarrow{g_{1*}} \operatorname{Hom}_R(M, N_2) \xrightarrow{g_{2*}} \operatorname{Hom}_R(M, N_3)$$

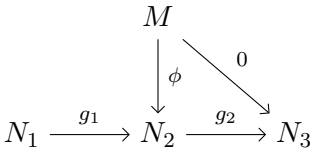
es exacta.

Demostración. Primero veremos que g_{1*} es inyectiva. Supongamos que $g_{1*}(\varphi) = g_1 \circ \varphi = 0$.



Puesto que $g_1 \colon N_1 \to N_2$ es inyectiva, eso implica que $\varphi \colon M \to N_2$ es la aplicación cero, por tanto g_{1*} es inyectiva.

Se tiene que $\operatorname{im} g_{1*} \subset \ker g_{2*}$, puesto que para todo $\varphi \in \operatorname{Hom}_R(M, N_1)$ se tiene que $g_{2*}(g_{1*}(\varphi)) = g_2 \circ g_1 \circ \varphi = 0$. Veamos que $\ker g_{2*} \subset \operatorname{im} g_{1*}$. Consideremos el siguiente diagrama,



Si $g_{2*}(\phi) = g_2 \circ \phi = 0$, entonces $\operatorname{im} \phi \subset \ker g_2 = \operatorname{im} g_1$. Dado que g_1 es inyectiva, ϕ da lugar a un (único) homomorfismo $\varphi \colon M \to N_1$ tal que $g_1 \circ \varphi = \phi$ y entonces $\phi \in \operatorname{im} g_{1*}$. □

Proposición 1.19. *Sea* $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ *una sucesión exacta corta de* R*-módulos: Para todo* R*-módulo* N *la sucesión inducida*

$$0 \longrightarrow \operatorname{Hom}_R(M_3, N) \xrightarrow{f_2^*} \operatorname{Hom}_R(M_2, N) \xrightarrow{f_1^*} \operatorname{Hom}_R(M_1, N)$$

es exacta.

Demostración. Veamos que f_2^* es inyectiva. Si $f_2^*(\varphi) = \varphi \circ f_2 = 0$, entonces por ser f_2 suprayectiva, $\varphi = 0$.

Veamos ahora que $\ker {f_1}^* = \operatorname{im} {f_2}^*$.

Dado que $f_2 \circ f_1 = 0$, se tiene que ${f_1}^* \circ {f_2}^* = (f_2 \circ f_1)^* = 0$ y entonces $\operatorname{im} {f_2}^* \subset \ker {f_1}^*$.

Para probar que $\ker {f_1}^* \subset \operatorname{im} {f_2}^*$, consideremos un homomorfismo de R-módulos $\psi \colon M_2 \to N$ tal que ${f_1}^*(\psi) = \psi \circ f_1 = 0$. Existe un único homomorfismo de R-módulos $\varphi \colon M_3 \to N$ tal que $\varphi \circ f_2 = \psi$. Así, ${f_2}^*(\varphi) = \psi$ y entonces $\psi \in \operatorname{im} {f_2}^*$.

□

1.3. Coproducto y producto de módulos

Definición 1.20. Sea $\{M_i\}_{i \in I}$ una familia de R-módulos. Se llama *coproducto* de los módulos M_i, y se denota por $(\bigoplus M_i)_{i \in I}$ o por $\bigoplus M_i$, al R-módulo cuyos elementos son familias $(m_i)_{i \in I}$, con $m_i \in M_i$ y $m_i \neq 0$ solo para un número finito de elementos $i \in I$, con las operaciones

$$(m_i)_{i \in I} + (m_i')_{i \in I} = (m_i + m_i')_{i \in I}, \quad r\,(m_i)_{i \in I} = (r\,m_i)_{i \in I}.$$

Para cada $j \in I$, llamamos *aplicaciones inyección* a los homomorfismos de R-módulos $\mu_j \colon M_j \to \oplus M_i$, dados por $\mu_j(m_j) = (m'_i)_{i\in I}$, con $m'_i = 0$, para $i \neq j$ y $m'_j = m_j$, para $m_j \in M_j$.

Definición 1.21. Sea $\{M_i\}_{i\in I}$ una familia de R-módulos. Se llama *producto directo* de los módulos M_i, y se denota por $(\prod M_i)_{i\in I}$ o por $\prod M_i$ al R-módulo cuyos elementos son familias $(m_i)_{i\in I}$, con $m_i \in M_i$, con las operaciones

$$(m_i)_{i\in I} + (m'_i)_{i\in I} = (m_i + m'_i)_{i\in I}, \quad r\,(m_i)_{i\in I} = (r\,m_i)_{i\in I}.$$

Para cada $j \in I$, llamamos *aplicaciones proyección* a los homomorfismos de R-módulos $p_j \colon \prod M_i \to M_j$, dados por $p_j((m_i)_{i\in I}) = m_j$, para $m_j \in M_j$.

Observación 1.22. Si I es un conjunto finito, entonces $(\bigoplus M_i)_{i\in I} = (\prod M_i)_{i\in I}$.

1.4. Módulos libres y módulos proyectivos.

Definición 1.23. Sea M un R-módulo y sea $S \subset M$. Se llama *submódulo generado* por S al menor submódulo de M que contiene a S; lo denotaremos por $\langle S\rangle$. Si $S \neq \varnothing$, los elementos de $\langle S\rangle$ son los elementos de M de la forma

$$\sum_{s\in S} r_s\, s, \quad r_s \in R,$$

y donde $r_s \neq 0$ solo para un número finito de elementos $s \in S$. Si $M = \langle S\rangle$, se dice que S es un *conjunto de generadores* de M y si M tiene un conjunto finito de generadores se dice que M es *finitamente generado*.

Se dice que S es *linealmente independiente* si

$$\sum_{s\in S} r_s\, s = 0 \quad \Rightarrow \quad r_s = 0, \quad \forall s \in S$$

Se dice que un R-módulo F es *libre sobre un subconjunto* S de F si S es un conjunto de generadores de F y es linealmente independiente. El conjunto S se dice que es una *base* de F. Se dice que F es un R-módulo *libre* si es libre sobre algún subconjunto.

Proposición 1.24. (1) *Sea S un conjunto y $R_s = R$ para todo $s \in S$. El módulo $\bigoplus_{s\in S} R_s$ es libre con base el conjunto $\{\mu_s(1) \mid s \in S\}$.*

(2) *Si F es un R-módulo libre con base $S \subset F$, entonces $F \cong \bigoplus_{s\in S} R_s$, donde $R_s = R$ como R-módulo.*

(3) *Todo módulo isomorfo a un módulo libre es libre.*

Demostración. (1) Dado que

$$(r_s)_{s\in S} = \sum_{s\in S} \mu_s(r_s) = \sum_{s\in S} r_s\, \mu_s(1),$$

se tiene que $\bigoplus_{s\in S} R_s = \langle \mu_s(1) \mid s \in S\rangle$. El conjunto $\{\mu_s(1) \mid s \in S\}$ es linealmente independiente puesto que si $\sum_{s\in S} r_s\, \mu_s(1) = (r_s)_{s\in S} = 0$, entonces $r_s = 0$, para todo $s \in S$.

(2) Definimos $\varphi\colon F \to \bigoplus_{s\in S} R_s$ como sigue: todo elemento $a \in F$ se expresa de forma única como

$$a = \sum_{s\in S} r_s\, s;$$

pongamos $\varphi(a) = (r_s)_{s\in S}$. La aplicación inversa de φ es la aplicación

$$\psi\colon \bigoplus_{s\in S} R_s \to F.$$

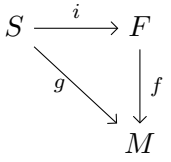
dada por $\psi((r_s)_{s\in S}) = \sum_{s\in S} r_s\, s$

(3) Sea $f\colon M \to N$ un isomorfismo de R-módulos. Si M es un R módulo libre con base el conjunto S, entonces N es un R-módulo libre con base $f(S)$. □

Definición 1.25. Sea S un conjunto. Se llama *R-módulo libre sobre S* al R-módulo $(\bigoplus R_s)_{s\in S}$, donde $R_s = R$, para todo $s \in S$.

Los módulos libres tienen la siguiente propiedad universal:

Proposición 1.26. *Sea F un módulo libre con base S y $i\colon S \to F$ la inclusión. Para cada R-módulo M y cada aplicación $g\colon S \to M$, existe un único homomorfismo de R-módulos $f\colon F \to M$ que extiende a g, es decir, tal que $f(s) = g(s)$, para todo $s \in S$.*



Demostración. Sea $a = \sum_{s\in S} r_s\, s$. Pongamos

$$f(a) = \sum_{s\in S} r_s\, m_s.$$

Se tiene que f es un homomorfismo de R-módulos y es el único homomorfismo tal que $f \circ i = g$. □

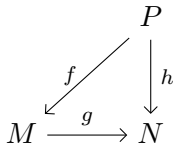
Proposición 1.27. *Todo R-módulo es isomorfo al cociente de un módulo libre F.*

Demostración. Sea M un R-módulo y pongamos $F = (\bigoplus R_m)_{m\in M}$. Consideremos la aplicación $i\colon M \to F$ dada por $i(m) = \mu_m(1)$. La aplicación R-lineal $f\colon F \to M$ dada por

$$f((r_m)_{m\in M} = \sum r_m\, m,$$

es un homomorfismo de R-módulos que verifica que $f\circ i = \mathrm{id}_M$. Por tanto, f es suprayectiva y $M \cong F/\ker f$. □

Definición 1.28. Se dice que un R-módulo P es *proyectivo* si para cada homomorfismo de R-módulos sobreyectivo $g\colon M \twoheadrightarrow N$ y cada homomorfismo de R-módulos $h\colon P \to N$, existe un homomorfismo de R-módulos $f\colon P \to M$ tal que $g \circ f = h$, es decir, tal que el diagrama



es conmutativo.

Proposición 1.29. *Todo R-módulo libre es proyectivo.*

Demostración. Sea F un R-módulo libre y S una base de F. Sean $h\colon P \to N$ y $g\colon M \to N$ homomorfismos siendo g sobreyectivo. Consideremos la aplicación $\varphi\colon S \to M$ tal que $\varphi(s) = m_s$, siendo $m_s \in M$ tal que $g(m_s) = h(s)$. Por la propiedad universal del módulo libre F, existe un único homomorfismo $f\colon F \to M$ tal que $f(s) = m_s$. Así, $g(f(s)) = h(s)$ para todo $s \in S$. Por tanto, $g \circ f = h$. □

Definición 1.30. Una presentación R-proyectiva de M es una sucesión exacta corta de R-módulos, $0 \to L \to P \to M \to 0$, donde P es proyectivo.

Por la proposición anterior todo R-módulo tiene presentaciones R-proyectivas.

Proposición 1.31. *Si P_1 y P_2 son R-módulos proyectivos, entonces $P_1 \bigoplus P_2$ es un R-módulo proyectivo.*

Demostración. Sea $g\colon M \to N$ un homomorfismo de R-módulos sobreyectivo. Por ser P_i un R-módulo proyectivo, para $i = 1, 2$, existen homomorfismos de R-módulos $f_i\colon P_i \to M$ tal que $g \circ f_i = h \circ \mu_i$, para $i = 1, 2$. La aplicación $f\colon P_1 \bigoplus P_2 \to M$ dada por $f(x_1, x_2) = f_1(x_1) + f_2(x_2)$ para $x_1 \in P_1$ y $x_2 \in P_2$, es un homomorfismo de R-módulos que verifica que $g \circ f = h$. □

Lema 1.32. *Sea* $0 \to M_1 \to M_2 \to M_3 \to 0$ *una sucesión exacta de* R*-módulos. Existe una sucesión exacta corta de módulos proyectivos* $0 \to P_1 \to P_2 \to P_3 \to 0$ *y homomorfismos sobreyectivos* $\epsilon_1 \colon P_1 \twoheadrightarrow M_1$, $\epsilon_2 \colon P_2 \to M_2$ *y* $\epsilon_3 \colon P_3 \to M_3$, *tales que el siguiente diagrama*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_1 & \longrightarrow & P_2 & \longrightarrow & P_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \epsilon_1} & & \downarrow{\scriptstyle \epsilon_2} & & \downarrow{\scriptstyle \epsilon_3} & & \\ 0 & \longrightarrow & M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \longrightarrow & 0 \end{array}$$

es conmutativo.

Demostración. Sean $\epsilon_1 \colon P_1 \to M_1$ y $\epsilon_3 \colon P_3 \to M_3$ homomorfismos sobreyectivos de R-módulos con P_1 y P_3 proyectivos. Sea $P_2 = P_1 \bigoplus P_3$, $\mu_1 \colon P_1 \to P_2$ la inyección y $p_2 \colon P_2 \to P_3$ la proyección. Dado que P_3 es proyectivo, existe un homomorfismo $g \colon P_3 \to M_2$ tal que $f_2 \circ g = \epsilon_3$.

$$\begin{array}{ccc} & & P_3 \\ & \swarrow^{g} & \downarrow{\scriptstyle \epsilon_3} \\ M_2 & \xrightarrow{f_2} & M_3 \end{array}$$

Sea $\epsilon_2 \colon P_2 \to M_2$ el homomorfismo dado por $\epsilon_2(x_1, x_3) = f_1\epsilon_1(x_1) + g(x_3)$. El homomorfismo ϵ_2 hace conmutativo el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_1 & \xrightarrow{\mu_1} & P_2 & \xrightarrow{p_2} & P_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \epsilon_1} & & \downarrow{\scriptstyle \epsilon_2} & & \downarrow{\scriptstyle \epsilon_3} & & \\ 0 & \longrightarrow & M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \longrightarrow & 0 \end{array}$$

Por el lema 1.17, ϵ_2 es un homomorfismo sobreyectivo. □

Proposición 1.33. *Sea* P *un* R*-módulo. Las siguientes afirmaciones son equivalentes:*

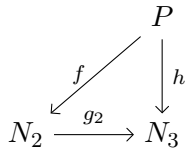
(1) P *es proyectivo.*

(2) *Para toda sucesión exacta corta* $0 \to N_1 \xrightarrow{g_1} N_2 \xrightarrow{g_2} N_3 \to 0$ *de* R*-módulos la sucesión inducida*

$$0 \to Hom_R(P, N_1) \xrightarrow{g_{1*}} Hom_R(P, N_2) \xrightarrow{g_{2*}} Hom_R(P, N_3) \to 0$$

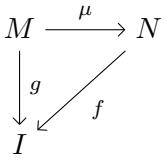
es exacta.

Demostración. (1) $\Rightarrow$ (2) Por la proposición 1.18, es suficiente probar que g_{2*} es sobreyectico. Sea $h\colon P \to N_3$ un homomorfismo de R-módulos. Dado que g_2 es un homomorfismo sobreyectivo y que P es proyectivo, existe un homomorfismo $f\colon P \to N_2$ tal que $g_2 \circ f = h$, equivalentemente $g_{2*}(f) = h$.



(2) $\Rightarrow$ (1) Sea $g\colon M \to N$ un homomorfismo de R-módulos sobreyectivo y sea $h\colon P \to N$ un homomorfismo de R-módulos. Sea $L = \ker g$ y consideremos la sucesión exacta de R-módulos $0 \to L \to M \xrightarrow{g} N \to 0$. Dado que el homomorfismo $g_*\colon Hom_R(P, M) \to Hom_R(P, N)$ es suprayectivo, existe un homomorfismo $f\colon P \to M$ tal que $g_*(f) = h$, es decir $g \circ f = h$. □

Definición 1.34. Sea I un R-módulo. Se dice que I es inyectivo si para cada homomorfismo de R-módulos $g : M \to I$ y cada homomorfismo inyectivo $\mu : M \to N$ de R-módulos, existe un homomorfismo $f : N \to I$ tal que $f \circ \mu = g$, es decir tal que el diagrama



es conmutativo.

Proposición 1.35. *Sea I un R-módulo. Las siguientes afirmaciones son equivalentes:*

(1) *I es inyectivo.*

(2) *Para toda sucesión exacta corta $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ de R-módulos la sucesión inducida*

$$0 \to \mathrm{Hom}_R(M_3, I) \xrightarrow{{f_2}^*} \mathrm{Hom}_R(M_2, I) \xrightarrow{{f_1}^*} \mathrm{Hom}_R(M_1, I) \to 0$$

es exacta.

Demostración. Es similar a la demostración de la proposición 1.33. □

1.5. Complejos de módulos

Definición 1.36. Un *complejo de cadenas* $\mathbf{C} = \{C_n, \delta_n\}$ de R-módulos es una familia $\{C_n\}_{n\in\mathbb{Z}}$ de R-módulos y una familia de homomorfismos $\{\delta_n \colon C_n \to C_{n-1}\}$ de R-módulos, tales que $\delta_n \circ \delta_{n+1} = 0$:

$$\mathbf{C}: \quad \cdots \longrightarrow C_{n+1} \xrightarrow{\delta_{n+1}} C_n \xrightarrow{\delta_n} C_{n-1} \longrightarrow \cdots$$

Sean $\mathbf{C} = \{C_n, \delta_n\}$ y $\mathbf{D} = \{D_n, \delta'_n\}$ complejos de cadenas de R-módulos. Un *morfismo* $\varphi_* \colon \mathbf{C} \to \mathbf{D}$ *de complejos de cadenas* es una familia $\{\varphi_n \colon C_n \to D_n\}$ de homomorfismos de R-módulos tal que, para cada n, el diagrama

$$\begin{array}{ccc} C_n & \xrightarrow{\delta_n} & C_{n-1} \\ {\scriptstyle\varphi_n}\downarrow & & \downarrow{\scriptstyle\varphi_{n-1}} \\ D_n & \xrightarrow{\delta'_n} & D_{n-1} \end{array}$$

es conmutativo.

Consideramos la categoría $\mathbf{Mod}_R^{\mathbb{Z}}$ de R-módulos graduados. Un objeto $\mathbf{M}$ en $\mathbf{Mod}_R^{\mathbb{Z}}$ es una familia $\{M_n\}_{n\in\mathbb{Z}}$ de R-módulos. Un *morfismo* $f_* \colon \mathbf{M} \to \mathbf{M}'$ *de R-módulos graduados de grado r* es una familia $\{f_n \colon M_n \to M'_{n+r}\}_{n\in\mathbb{Z}}$ de homomorfismos de R-módulos. Podemos decir que que un complejo de cadenas $\mathbf{C}$ es un objeto de $\mathbf{Mod}_R^{\mathbb{Z}}$ junto con un morfismo $\delta_* \colon \mathbf{C} \to \mathbf{C}$ de grado -1, tal que $\delta_* \circ \delta_* = 0$. Un morfismo de complejos de cadenas $\varphi_* : \mathbf{C} \to \mathbf{D}$ es un morfismo de grado cero en $\mathbf{Mod}_R^{\mathbb{Z}}$ tal que $\varphi_* \circ \delta_* = \delta'_* \circ \varphi_*$. Los complejos de cadenas y los morfismos de complejos de cadenas forman una categoría preaditiva que denotaremos por $\mathbf{CMod}_R$.

Definición 1.37. Sea $\mathbf{C} = \{C_n, \delta_n\}$ un complejo de cadenas de R-módulos. Se llama *n-ésimo módulo de homología* de $\mathbf{C}$ al R-módulo

$$H_n(\mathbf{C}) = \ker \delta_n / \operatorname{im} \delta_{n+1}.$$

Se llama *módulo de homología* de C_* al módulo graduado $H_*(\mathbf{C}) = \{H_n(\mathbf{C}))_{\mathbf{n}\in\mathbb{Z}}\}$.

Un morfismo de complejos de cadenas $\varphi_* \colon \mathbf{C} \to \mathbf{D}$ induce un morfismo de grado cero de módulos graduados $H_*(\varphi_*) \colon H(\mathbf{C}) \to H(\mathbf{D})$, dado por $H_n(\varphi_*)[z_n] = [\varphi_n(z_n)]$, para $z_n \in \ker \delta_n$. Se tiene un funtor covariante aditivo

$$H_*(-) \colon \mathbf{C}\mathrm{Mod}_R \to \mathrm{Mod}_R^{\mathbb{Z}},$$

dado por: $H_*(-)(\mathbf{C}) = H_*(\mathbf{C})$ y $H_*-)(\varphi_*) = H_*(\varphi_*)$, para cada morfismo $\varphi_* \colon \mathbf{C} \to \mathbf{D}$ de complejos de cadenas que se llama funtor homología.

Definición 1.38. Un *complejo de cocadenas* de R-módulos $\mathbf{C} = \{C^n, \delta^n\}$ es un objeto en $\mathbf{Mod}_R^{\mathbb{Z}}$ junto con un morfismo $\delta^*\colon \mathbf{C} \to \mathbf{C}$ de grado $+1$ tal que $\delta^* \circ \delta^* = 0$.

$$\mathbf{C}: \quad \cdots \longrightarrow C^{n-1} \overset{\delta^{n-1}}{\longrightarrow} C^n \overset{\delta^n}{\longrightarrow} C^{n+1} \longrightarrow \cdots$$

El morfismo δ^* se llama *diferencial*. Los morfismos de complejos de cocadenas se definen de forma análoga a los morfismos de complejos de cadenas. Dado un complejo de cocadenas $\mathbf{C} = \{C^n, \delta^n\}$ se define su *módulo de cohomología* $H^*(\mathbf{C}) = \{\mathbf{H^n(C)}\}_{\mathbf{n}\in\mathbb{Z}}$ por

$$H^n(\mathbf{C}) = \ker \delta^n / \operatorname{im} \delta^{n-1}, \quad n \in \mathbb{Z}.$$

Se tiene un funtor aditivo $H^*(-)$ de la categoría de complejos de cocadenas de R-módulos a la categoría de R-módulos graduados que se denomina funtor *cohomología*.

Definición 1.39. Se dice que la sucesión $0 \to \mathbf{C} \overset{\varphi_*}{\to} \mathbf{D} \overset{\psi_*}{\to} \mathbf{E} \to 0$ (resp. $0 \to \mathbf{C} \overset{\varphi_*}{\to} \mathbf{D} \overset{\psi_*}{\to} \mathbf{E} \to 0$) es una *sucesión exacta corta* de complejos de cadenas (resp. cocadenas) de R-módulos si la sucesión $0 \to C_n \overset{\varphi_n}{\to} D_n \overset{\psi_n}{\to} E_n \to 0$ a(resp. $0 \to C^n \overset{\varphi^n}{\to} D^n \overset{\psi^n}{\to} E^n \to 0$) es una sucesión exacta de R-módulos para todo $n \in \mathbb{Z}$.

Proposición 1.40. *Dada una sucesión exacta corta de complejos de cocadenas*

$$0 \to \mathbf{C} \overset{\varphi^*}{\to} \mathbf{D} \overset{\psi^*}{\to} \mathbf{E} \to 0.$$

existe un morfismo de módulos graduados $\omega\colon H(\mathbf{E}) \to H(\mathbf{C})$ *de grado* $+1$ *tal que la siguiente sucesión es exacta:*

$$\cdots \overset{\omega^{n-1}}{\longrightarrow} H^n(\mathbf{C}) \overset{H^n(\varphi^*)}{\longrightarrow} H^n(\mathbf{D}) \overset{H^n(\psi^*)}{\longrightarrow} H^n(\mathbf{E}) \overset{\omega_n}{\longrightarrow} H^{n+1}(\mathbf{C}) \to \cdots \qquad (\star)$$

Demostración. Sea $\mathbf{C} = \{C_n, \delta^n\}$ un complejo de cocadenas. Puesto que $\operatorname{im}\delta^{n-1} \subseteq \ker \delta^n$ y $\operatorname{im}\delta^n \subseteq \ker \delta^{n+1}$ el diferencial δ^n induce una aplicación $\tilde{\delta^n}$ como sigue:

$$\operatorname{coker}\delta^{n-1} = \mathbf{C_n}/\operatorname{im}\delta^{\mathbf{n-1}} \to \mathbf{C_n}/\ker\,\delta^{\mathbf{n}} \cong \operatorname{im}\delta^{\mathbf{n}} \subseteq \ker\,\delta^{\mathbf{n+1}}.$$

Se tiene

$$\ker\,\tilde{\delta^n} = \ker\,\delta^n/\operatorname{im}\delta^{n-1} = H^n(\mathbf{C}), \quad \operatorname{coker}\tilde{\delta^n} = \ker\,\delta^{n+1}/\operatorname{im}\delta^n = H^{n+1}(\mathbf{C}).$$

Consideremos la sucesión exacta corta de complejos de cocadenas

$$0 \to \mathbf{C} \overset{\varphi^*}{\to} \mathbf{D} \overset{\psi^*}{\to} \mathbf{E} \to 0.$$

y el diagrama conmutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \ker\,\delta^n & \longrightarrow & \ker\,\delta^n & \longrightarrow & \ker\,\delta^n & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbf{C^n} & \xrightarrow{\varphi^n} & \mathbf{D^n} & \xrightarrow{\psi^n} & \mathbf{E^n} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \delta^n} & & \downarrow{\scriptstyle \delta^n} & & \downarrow{\scriptstyle \delta^n} & & \\
0 & \longrightarrow & \mathbf{C^{n+1}} & \xrightarrow{\varphi^{n+1}} & \mathbf{D^{n+1}} & \xrightarrow{\psi^{n+1}} & \mathbf{E^{n+1}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \operatorname{coker}\delta^n & \longrightarrow & \operatorname{coker}\delta^n & \longrightarrow & \operatorname{coker}\delta^n & \longrightarrow & 0
\end{array}$$

Por el lema de la serpiente, la primera fila y la cuarta fila son sucesiones exactas. Se tiene el diagrama conmutativo

$$\begin{array}{ccccccccc}
 & & H^n(\mathbf{C}) & \longrightarrow & H^n(\mathbf{D}) & \longrightarrow & H^n(\mathbf{E}) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \operatorname{coker}\,\delta^{n-1} & \longrightarrow & \operatorname{coker}\,\delta^{n-1} & \longrightarrow & \operatorname{coker}\,\delta^{n-1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \bar{\delta^n}} & & \downarrow{\scriptstyle \bar{\delta^n}} & & \downarrow{\scriptstyle \bar{\delta^n}} & & \\
0 & \longrightarrow & \ker\,\delta^{n+1} & \longrightarrow & \ker\,\delta^{n+1} & \longrightarrow & \ker\,\delta^{n+1} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & H^{n+1}(\mathbf{C}) & \longrightarrow & H^{n+1}(\mathbf{D}) & \longrightarrow & H^{n+1}(\mathbf{E}) & &
\end{array}$$

Aplicando de nuevo el lema de la serpiente, deducimos la existencia de un homomorfismo

$$\omega_n \colon H^n(\mathbf{E}) \to H^{n+1}(\mathbf{C})$$

tal que la sucesión $(\star)$ es exacta. □

Definición 1.41. Sean $\mathbf{C}$ y $\mathbf{D}$ complejos de cadenas y $\varphi_*, \psi_* : \mathbf{C} \to \mathbf{D}$ morfismos de complejos. Una homotopía $\Sigma_* : \varphi_* \to \psi_*$ es un morfismo de grado $+1$ de módulos graduados $\Sigma_* \colon \mathbf{C} \to \mathbf{D}$ tal que

$$\psi_n - \varphi_n = \delta_{n+1} \circ \Sigma_n + \Sigma_{n-1} \circ \delta_n, \quad n \in \mathbb{Z}.$$

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & C_{n+1} & \xrightarrow{\delta_{n+1}} & C_n & \xrightarrow{\delta_n} & C_{n-1} & \longrightarrow & \cdots \\
 & & \Vert & \swarrow^{\Sigma_n} & \Vert{\scriptstyle \varphi_n}\ \Vert{\scriptstyle \psi_n} & \swarrow^{\Sigma_{n-1}} & \Vert & & \\
\cdots & \longrightarrow & D_{n+1} & \xrightarrow{\delta_{n+1}} & D_n & \xrightarrow{\delta_n} & D_{n-1} & \longrightarrow & \cdots
\end{array}$$

Decimos que φ_* y ψ_* son homotópicos, y escribimos $\varphi_* \simeq \psi_*$ si existe una homotopía $\Sigma^* : \varphi_* \to \psi_*$.

Definición 1.42. Sean $\mathbf{C}$ y $\mathbf{D}$ complejos de cocadenas y $\varphi^*, \psi^* \colon \mathbf{C} \to \mathbf{D}$ morfismos de complejos. Una homotopía $\Sigma^* \colon \varphi^* \to \psi^*$ es un morfismo de grado -1 de módulos graduados $\Sigma^* \colon \mathbf{C} \to \mathbf{D}$ tal que

$$\psi^n - \varphi^n = \delta^{n-1} \circ \Sigma^n + \Sigma^{n+1} \circ \delta^n, \quad n \in \mathbb{Z}.$$

$$\begin{array}{ccccccccc}
\ldots & \longrightarrow & C^{n-1} & \xrightarrow{\delta^{n-1}} & C^n & \xrightarrow{\delta^n} & C^{n+1} & \longrightarrow & \ldots \\
 & & \Big\downarrow & \swarrow^{\Sigma^n} & \Big\downarrow & \swarrow^{\Sigma^{n+1}} & \Big\downarrow & & \\
\ldots & \longrightarrow & D^{n-1} & \xrightarrow{\delta^{n-1}} & D^n & \xrightarrow{\delta^{n-1}} & D^{n+1} & \longrightarrow & \ldots
\end{array}$$

Decimos que φ^* y ψ^* son homotópicos, y escribimos $\varphi^* \simeq \psi^*$ si existe una homotopía $\Sigma^* \colon \varphi^* \to \psi^*$.

El resultado mas importante sobre homotopía es el siguiente:

Proposición 1.43. *Si los dos morfismos de complejos de (co)cadenas $\varphi, \psi \colon \mathbf{C} \to \mathbf{D}$ son homotópicos, entonces $H(\varphi_*) = H(\psi_*) : H(\mathbf{C}) \to H(\mathbf{D})$.*

Demostración. Veamos el resultado para complejos de cadenas. Sea $z \in \ker \delta_n$ un ciclo en C_n. Si $\Sigma_* \colon \varphi_* \to \psi_*$ es una homotopía, entonces

$$(\psi_n - \varphi_n)z = \delta_{n+1}\Sigma_n z + \Sigma_{n-1}\delta_n z = \delta_{n+1}\Sigma_n z$$

puesto que $\delta z = 0$. Así, $\psi(z) - \varphi(z) \in \operatorname{im} \delta_{n+1}$ y se tiene

$$H_n(\varphi_*)(z + \delta_{n+1}) = H_n(\varphi_n(z) + \operatorname{im} \delta_{n+1}) = H_n(\psi_n(z) + \operatorname{im} \delta_{n+1}) = H_n(\psi_*)(z + \delta_{n+1}) \ \square.$$

La demostración en el caso de complejos de cocadenas es similar.

Lema 1.44. *La relación de homotopía $\simeq$ es una relación de equivalencia.*

Demostración. Claramente $\simeq$ es reflexiva y simétrica. Para comprobar la transitividad, si $\Sigma_* \colon \varphi_* \to \psi_*$ y $\Sigma'_* \colon \psi_* \to \chi_*$ son homotopías, entonces

$$\psi - \varphi = \delta\,\Sigma + \Sigma\,\delta, \quad \chi - \psi = \delta\,\Sigma' + \Sigma'\,\delta,$$

(suprimiendo los subíndices), de donde se sigue

$$\chi - \varphi = \delta\,(\Sigma + \Sigma') + (\Sigma + \Sigma')\,\delta.$$

$\square$

Lema 1.45. *Si* $\varphi_* \simeq \psi_* : \mathbf{C} \to \mathbf{D}$ *y* $\varphi'_* \simeq \psi'_* : \mathbf{D} \to \mathbf{E}$ *entonces* $\varphi'_* \varphi_* \simeq \psi'_* \psi_* : \mathbf{C} \to \mathbf{E}$.

Demostración. Sean $\Sigma_* \colon \varphi_* \to \psi_*$ y $\Sigma'_* \colon \varphi'_* \to \psi'_*$. Se tiene

$$\psi - \varphi = \delta\,\Sigma + \Sigma\,\delta, \quad \psi' - \varphi' = \delta\,\Sigma' + \Sigma'\,\delta,$$

y entonces

$$\varphi' \circ \psi - \varphi' \circ \varphi = \varphi'\delta\,\Sigma + \varphi'\Sigma\,\delta = \delta(\varphi'\,\Sigma) + (\varphi'\Sigma)\,\delta.$$

se tiene la homotopía $\varphi'_*\,\Sigma \colon \varphi'_*\varphi_* \to \varphi'_*\psi_*$. Dado que

$$\psi' \circ \psi - \varphi' \circ \psi = \delta\,\Sigma'\psi + \Sigma'\delta\psi = \delta\,(\Sigma'\,\psi) + (\Sigma'\psi)\,\delta.$$

El resultado sigue por transitividad. □

Lema 1.46. *Sean* $\mathcal{C}$ *y* $\mathcal{D}$ *categorías de módulos y sea* $F : \mathcal{C} \to \mathcal{D}$ *un funtor aditivo. Si* $\mathbf{C}$ *y* $\mathbf{D}$ *son complejos de (co)cadenas de módulos de* $\mathcal{C}$ *y* $\varphi_* \simeq \psi_* : \mathbf{C} \to \mathbf{D}$*, entonces* $F\varphi_* \simeq F\psi_* : F(\mathbf{C}) \to F(\mathbf{D})$.

Demostración. Sea $\Sigma_* \colon \varphi_* \to \psi_*$, entonces

$$F\psi - F\varphi = F(\psi - \varphi) = F(\delta\,\Sigma + \Sigma\,\delta) = F\delta\,F\Sigma + F\Sigma\,F\delta.$$

Luego, se tiene la homotopía $F\,\Sigma_* \colon F\varphi_* \to F\psi_*$. □

Corolario 1.47. *Si* $\varphi_* \simeq \psi_* \colon \mathbf{C} \to \mathbf{D}$ *y si* F *es un funtor aditivo, entonces* $H(F\varphi_*) = H(F\psi_*) \colon H(F(\mathbf{C})) \to H(F(\mathbf{D}))$.

Demostración. Por el lema 1.46, $F\varphi_* \simeq F\psi_*$ y por la proposición 1.43, $H(F\varphi_*) = H(F\psi_*)$. □

Definición 1.48. Una *contracción de homotopía* para un (co)complejo $\mathbf{C}$ es una homotopía $\Sigma \colon 0 \to \mathrm{id}_{\mathbf{C}}$, donde $0, \mathrm{id}_{\mathbf{C}} \colon \mathbf{C} \to \mathbf{C}$ son los morfismo de (co)complejos obvios.

Por la proposición 1.43, si existe una contracción de homotopía para $\mathbf{C}$, entonces $H(\mathbf{C}) = 0$, de donde se sigue que $\mathbf{C}$ es exacto.

Definición 1.49. Se dice que los (co)complejos $\mathbf{C}$ y $\mathbf{D}$ son del mismo tipo de homotopía, o homotópicos, si existen morfismos de (co)complejos $\varphi_* : \mathbf{C} \to \mathbf{D}$ y $\psi_* : \mathbf{D} \to \mathbf{C}$ tales que $\psi_* \circ \varphi_* \simeq \mathrm{id}_{\mathbf{C}}$ y $\varphi_* \circ \psi_* \simeq \mathrm{id}_{\mathbf{D}}$. El morfismo φ_* (o ψ_*) se dice entonces que es una equivalencia de homotopía.

1.6. Resoluciones

En esta sección vamos a definir una clase especial de complejos necesarios para definir los funtores derivados Ext^n.

Definición 1.50. Un complejo de cadenas de módulos $\mathbf{C} = \{C_n, \delta_n\}$ se dice que es positivo si $C_n = 0$, para todo $n < 0$. Un complejo de cocadenas de módulos $\mathbf{C} = \{C^n, \delta^n\}$ se dice que es positivo si $C^n = 0$, para todo $n < 0$.

Definición 1.51. Un complejo de cadenas de módulos positivo $\mathbf{C} = \{C_n, \delta_n\}$ se dice que es proyectivo si C_n es proyectivo para todo $n \geq 0$; se dice que es acíclico si $H_n(\mathbf{C}) = 0$, para $n \geq 1$.

Definición 1.52. Una resolución proyectiva de M es un complejo $\mathbf{P} = \{P_n, \delta_n\}$ de módulos proyectivos y acíclico y tal que $H_0(\mathbf{P}) = M$, es decir un complejo exacto de la forma

$$\mathbf{P} : \cdots \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0$$

Proposición 1.53. *Todo R-módulo tiene una resolución proyectiva.*

Demostración. Sea M un R-módulo. Elegimos una presentación proyectiva $0 \to R_1 \to P_0 \to M \to 0$ de M; luego una presentación proyectiva $0 \to R_2 \to P_1 \to R_1 \to 0$ de R_1, etc. Claramente el complejo

$$\mathbf{P}\colon \cdots \to P_n \xrightarrow{\delta_n} P_{n-1} \to \cdots \to P_0$$

donde $\delta_n \colon P_n \to P_{n-1}$ es la composición $P_n \twoheadrightarrow R_n \rightarrowtail P_{n-1}$ es una resolución proyectiva de M. □

Teorema 1.54. (Teorema de comparación) *Sea $\mathbf{P} = \{P_n, \delta\}$ un complejo de cadenas proyectivo y sea $\mathbf{C} = \{C_n, \delta'\}$ un complejo de cadenas positivo y acíclico. Para cada homomorfismo $\varphi \colon H_0(\mathbf{P}) \to H_0(\mathbf{C})$ existe un morfismo de complejos $\varphi_* \colon \mathbf{P} \to \mathbf{C}$ que induce φ. Además dos morfismos de complejos induciendo φ son homotópicos.*

Demostración. El morfismo de cadenas $\varphi_* \colon \mathbf{P} \to \mathbf{C}$ se define por inducción. Como $\mathbf{C}$ es acíclico, $C_0 \to H_0(\mathbf{C}) \to 0$ es exacta. Por la proyectividad de P_0 existe un homomorfismo $\varphi_0 \colon P_0 \to C_0$ que hace diagrama

$$\begin{array}{ccc} P_0 & \longrightarrow & H_0(\mathbf{P}) \\ {\scriptstyle \varphi_0}\downarrow & & \downarrow{\scriptstyle \varphi} \\ C_0 & \longrightarrow & H_0(\mathbf{C}) \end{array}$$

conmutativo. Supongamos $n \geq 1$ y que $\varphi_0, \varphi_1, ..., \varphi_{n-1}$ están definidos. Consideramos el diagrama

$$\begin{array}{ccccccc} P_n & \xrightarrow{\delta} & P_{n-1} & \xrightarrow{\delta} & P_{n-2} & \longrightarrow & \cdots \\ \downarrow{\scriptstyle \varphi_n} & & \downarrow{\scriptstyle \varphi_{n-1}} & & \downarrow{\scriptstyle \varphi_{n-2}} & & \\ C_n & \xrightarrow{\delta} & C_{n-1} & \xrightarrow{\delta} & C_{n-2} & \longrightarrow & \cdots \end{array}$$

(Si $n = 1$, ponemos $P_{-1} = H_0(\mathbf{P})$, $C_{-1} = H_0(\mathbf{C})$). Se tiene que $\delta\,\varphi_{n-1}\,\delta = \varphi_{n-2}\,\delta\,\delta = 0$ y entonces

$$\operatorname{im}(\varphi_{n-1}\,\delta) \subseteq \ker(\delta\colon C_{n-1} \to C_{n-2}).$$

Dado que $\mathbf{C}$ es acíclico, $\ker\, \delta_{n-1} = \operatorname{im}(\delta\colon C_n \to C_{n-1})$. La proyectividad de P_n nos permite encontrar $\varphi_n\colon P_n \to C_n$ tal que $\varphi_{n-1}\,\delta = \delta\,\varphi_n$. Esto completa el proceso de inducción.

Ahora sean $\varphi_* = \{\varphi_n\}$, $\psi_* = \{\psi_n\}$ dos morfismos de complejos de cadenas que inducen la aplicación $\varphi\colon H_0(\mathbf{P}) \to H_0(\mathbf{C})$. Vamos a definir una homotopía $\Sigma_*\colon \psi_* \to \varphi_*$ por inducción.

Primero consideremos el diagrama

$$\begin{array}{ccccccc} P_1 & \longrightarrow & P_0 & \longrightarrow & H_0(\mathbf{P}) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi_1}\downarrow{\scriptstyle \psi_1} & \swarrow{\scriptstyle \Sigma_0} & \downarrow{\scriptstyle \varphi_0}\downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \varphi} & & \\ C_1 & \longrightarrow & C_0 & \longrightarrow & H_0(\mathbf{C}) & \longrightarrow & 0 \end{array}$$

Dado que φ_0 y ψ_0 ambos inducen φ, se tiene que

$$\operatorname{im}(\varphi_0 - \psi_0) \subset \ker(C_0 \to H_0(C)) = \operatorname{im}(\delta\colon C_1 \to C_0)$$

y dado que P_0 es proyectivo, existe un homomorfismo $\Sigma_0\colon P_0 \to C_1$ tal que $\varphi_0 - \psi_0 = \delta\Sigma_0$.

Ahora supongamos que $n \geq 1$ y que $\Sigma_0, \ldots, \Sigma_{n-1}$ verifican

$$\varphi_r - \psi_r = \delta\,\Sigma_r + \Sigma_{r-1}\,\delta, \quad r \leq n-1,$$

(entendiendo $\Sigma_{-1}\,\delta$ como 0). Consideremos el diagrama

$$\begin{array}{ccccccc} P_{n+1} & \xrightarrow{\delta} & P_n & \xrightarrow{\delta} & P_{n-1} & & \\ \downarrow{\scriptstyle \varphi_{n+1}}\downarrow{\scriptstyle \psi_{n+1}} & \swarrow{\scriptstyle \Sigma_n} & \downarrow{\scriptstyle \varphi_n}\downarrow{\scriptstyle \psi_n} & \swarrow{\scriptstyle \Sigma_{n-1}} & \downarrow{\scriptstyle \varphi_{n-1}}\downarrow{\scriptstyle \psi_{n-1}} & & \\ C_{n+1} & \xrightarrow{\delta} & C_n & \xrightarrow{\delta} & C_{n-1} & & \end{array}$$

Se tiene

$$\delta(\varphi_{n*}-\psi_n-\Sigma_{n-1}\delta) = \varphi_{n-1*}\delta-\psi_{n-1}\delta-\delta\Sigma_{n-1}\delta = (\varphi_{n-1*}-\psi_{n-1}-\delta\Sigma_{n-1})\delta = \Sigma_{n-2}\delta\delta = 0$$

Por tanto,

$$\operatorname{im}(\varphi_n - \psi_n - \Sigma_{n-1}\delta) \subset \ker(\delta\colon C_n \to C_{n-1}) = \operatorname{im}(\delta\colon P_{n+1} \to P_n).$$

y dado que P_n es proyectivo, existe $\Sigma_n\colon P_n \to C_{n+1}$ tal que

$$\varphi_n - \psi_n - \Sigma_{n-1}\delta = \delta\Sigma_n. \qquad \square$$

Proposición 1.55. *Sea M un módulo. Dos resoluciones proyectivas de M son del mismo tipo de homotopía.*

Demostración. Sean $\mathbf{P}$ y $\mathbf{Q}$ dos resoluciones proyectivas de M. Por la proposición 1.54 existen aplicaciones de cadenas $\varphi_*\colon \mathbf{P} \to \mathbf{Q}$ y $\psi_*\colon \mathbf{Q} \to \mathbf{P}$ induciendo la identidad en $H_0(\mathbf{P}) = M = H_0(\mathbf{Q})$. La composición $\psi_* \circ \varphi_*\colon \mathbf{P} \to \mathbf{P}$ induce la aplicación identidad en M. Por el teorema 1.54, tenemos $\psi_* \circ \varphi_* \cong \mathrm{id}_*$. Análogamente, $\varphi_* \circ \psi_* \cong \mathrm{id}_*$. Por tanto, $\mathbf{P}$ y $\mathbf{Q}$ son del mismo tipo de homotopía. $\square$

Lema 1.56. *Sea $0 \to M' \to M \to M'' \to 0$ una sucesión exacta de R-módulos. Existe una sucesión exacta corta de complejos $0 \to \mathbf{P}' \rightarrowtail \mathbf{P} \twoheadrightarrow \mathbf{P}'' \to 0$ donde $\mathbf{P}$, $\mathbf{P}'$ y $\mathbf{P}''$ son resoluciones proyectivas de M', M y M'' respectivamente, y tales que el diagrama*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P_0' & \longrightarrow & P_o & \longrightarrow & P_0'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \epsilon'} & & \downarrow{\scriptstyle \epsilon} & & \downarrow{\scriptstyle \epsilon''} & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0
\end{array}$$

es conmutativo.

Demostración. Por el lema 1.32 existe una sucesión exacta corta de módulos proyectivos $0 \to P_0' \to P_0 \to P_0'' \to 0$ y homomorfismos sobreyectivos $\epsilon'\colon P_0' \to M'$, $\epsilon\colon P_0 \to M$ y $\epsilon''\colon P_0'' \to M''$, tales que el siguiente diagrama

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P_0' & \longrightarrow & P_0 & \longrightarrow & P_0'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \epsilon'} & & \downarrow{\scriptstyle \epsilon} & & \downarrow{\scriptstyle \epsilon''} & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \xrightarrow{f} & M_3 & \longrightarrow & 0
\end{array}$$

es conmutativo. Por el lema de la serpiente, la sucesión de núcleos

$$0 \to \ker\ \epsilon' \to \ker\ \epsilon \to \ker\ \epsilon'' \to 0,$$

es corta exacta. Repitiendo este procedimiento con la sucesión de núcleos en lugar de la sucesión $0 \to M' \to M \to M' \to 0'$ y luego procediendo inductivamente, construímos una sucesión exacta de complejos $0 \to \mathbf{P}' \rightarrowtail \mathbf{P} \twoheadrightarrow \mathbf{P}'' \to 0$, donde $\mathbf{P}'$, $\mathbf{P}$ y $\mathbf{P}''$ son resoluciones proyectivas de M', M, M'' respectivamente.

□

1.7. El funtor Ext

El funtor Ext es un funtor derivado. En este trabajo no vamos a estudiar los funtores derivados en general, sino que nos restrigiremos al caso de los funtor $\mathrm{Ext}^n_R(-, A)$ que son funtores derivados del funtor $\mathrm{Hom}_R(-, A)$.

Consideremos para cada módulo M una resolución proyectiva $\mathbf{P}_M$ de M y el funtor aditivo $\mathrm{Hom}_R(-, M)\colon \mathbf{Mod} \to \mathbf{Ab}$.

Definición 1.57. Para cada módulo M definimos

$$\mathrm{Ext}^n_R(M, N) = H^n(\mathrm{Hom}_R(\mathbf{P}_M, N)), \quad n \in \mathbb{N}$$

es decir $\mathrm{Ext}^n_R(M, N)$ es el n-ésimo grupo de cohomología del complejo de cocadenas

$$\mathrm{Hom}(\mathbf{P}_M, N):\ 0 \to \mathrm{Hom}(P_0, N) \to \mathrm{Hom}(P_1, N) \to \cdots \to \mathrm{Hom}(P_n, N) \to \cdots$$

Si $f\colon M' \to M$ es un homomorfismo de R-módulos, por el teorema 1.54, existe un morfismo de complejos $\bar{f}\colon P_{M'} \to P_M$ que induce f. Definimos

$$\mathrm{Ext}^n_R(f, N) = H^n(\mathrm{Hom}_R(\bar{f}, M)), \quad n \in \mathbb{N}$$

Proposición 1.58. *Se tienen funtores* $Ext^n_R(-, N)\colon \mathbf{Mod}_R \to \mathrm{Ab}$ *para todo* $n \in \mathbb{N}$.

Demostración. Veamos que $\mathrm{Ext}^n_R(-, N)$ está bien definido. Sea $h\colon \mathbf{P}_{M'} \to \mathbf{P}_M$ otro morfismo de complejos que induce f. Por el teorema 1.54, $\bar{f}$ y h son homotópicos y dado que el funtor $\mathrm{Hom}_R(-, M)\colon \mathrm{Mod} \to \mathrm{Ab}$ es un funtor aditivo, por el corolario 1.47, $H^n(\mathrm{Hom}_R(\bar{f}, N)) = H^n(\mathrm{Hom}_R(h, N))$. □

Vamos a probar que los funtores $\mathrm{Ext}^n_R(-, N)$ no dependen de las resoluciones proyectivas consideradas. Fijemos para cada módulo M otra resolución proyectiva $\mathbf{Q}_M$ de M. Tenemos funtores $\mathbf{Q}\,\mathrm{Ext}^n_R(-, N)$ definidos de forma similar a los funtores $\mathrm{Ext}^n(-, N)$.

Proposición 1.59. *Existe una equivalencia natural*

$$\Phi\colon \operatorname{Ext}^n_R(-,N) \to \mathbf{Q}\operatorname{Ext}^n_R(-,N).$$

Demostración. Por el teorema de comparación, existe un morfismo de complejos $\mathbf{i}_M\colon : \mathbf{Q}_M \to \mathbf{P}_M$ que induce id_M. Por ser el funtor $\operatorname{Hom}_R(-,M)$ aditivo se tiene que el morfismo de complejos $\operatorname{Hom}_R(\mathbf{i}_M,N)\colon \operatorname{Hom}_R(\mathbf{P}_M,N) \to \operatorname{Hom}_R(\mathbf{Q}_M,N)$ induce un morfismo

$$\Phi_M = H^n(\operatorname{Hom}_R(\mathbf{i}_M,N))\colon \operatorname{Ext}^n_R(M,N) \to \mathbf{Q}\operatorname{Ext}^n_R(M,N)$$

Veamos que Φ_M es un isomorfismo:

Por el teorema de comparación, existe un morfismo de complejos $\mathbf{j}_M\colon \mathbf{P}_M \to \mathbf{Q}_M$ que induce id_M. Por el teorema de comparación $\mathbf{j}_M \circ \mathbf{i}_M \simeq \mathbf{id}_{\mathbf{Q}_M}$. Por tanto $H^n(\operatorname{Hom}_R(\mathbf{j}_M),N)) \circ \Phi_M = \mathrm{id}$. Análogamente, $\Phi_M \circ H^n(\operatorname{Hom}_R(\mathbf{j}_M,N)) = \mathrm{id}$.

Veamos ahora que Φ es una transformación natural: Sea $f\colon M' \to M$ un morfismo de R-módulos. Tenemos que probar que el cuadrado

$$\begin{array}{ccc} \operatorname{Ext}^n_R(M,N) & \xrightarrow{\Phi_M} & \mathbf{Q}\operatorname{Ext}^n_R(M,N) \\ {\scriptstyle \operatorname{Ext}^n_R(f,N)}\downarrow & & \downarrow{\scriptstyle \mathbf{Q}\operatorname{Ext}^n_R(f,N)} \\ \operatorname{Ext}^n_R(M',N) & \xrightarrow{\Phi_{M'}} & \mathbf{Q}\operatorname{Ext}^n_R(M',N) \end{array}$$

es conmutativo. Sea $\varphi_*\colon \mathbf{Q}_M \to \mathbf{Q}_{M'}$ un morfismo de complejos que induce f, $\psi_*\colon \mathbf{P}_M \to \mathbf{P}_{M'}$ un morfismo de complejos que induce f y $\mathbf{i}_{M'}\colon \mathbf{Q}_{M'} \to \mathbf{P}_{M'}$ un morfismo de complejos que induce $\mathrm{id}_{M'}$. Los morfismos $i_{M'} \circ \varphi_*, \psi_* \circ i_M\colon \mathbf{Q}_M \to \mathbf{P}_{M'}$ son homotópicos. Por ser $\operatorname{Hom}_R(-,M)$ aditivo, $\operatorname{Hom}_R(\varphi_*,N) \circ \operatorname{Hom}_R(\mathbf{i}_{M'},N) \simeq \operatorname{Hom}_R(\mathbf{i}_M,N) \circ \operatorname{Hom}_R(\psi*,N)$, y entonces aplicando el funtor H^n se tiene que $\Phi_{M'} \circ \operatorname{Ext}^n_R(f,N) = \mathbf{Q}\operatorname{Ext}^n_R(f,N)) \circ \Phi_M$. □

Identificaremos los grupos $\operatorname{Ext}^n_R(M,N)$ y $\mathbf{Q}\operatorname{Ext}^n_R(M,N)$ vía el isomorfismo Φ_M.

Corolario 1.60. $\operatorname{Ext}^n_R(M,N)$ *no depende de la resolución proyectiva de* M *considerada.*

Definición 1.61. Un funtor contravariante $F\colon \mathbf{Mod}_R \to \mathbf{Ab}$ se dice que es *exacto a la izquierda*, si para toda sucesión exacta $0 \to M' \to M \to M'' \to 0$ se tiene que la sucesión $0 \to F(M'') \to F(M) \to F(M')$ es exacta. Se dice que F es *exacto* si, para toda sucesión exacta corta $0 \to M' \to M \to M'' \to 0$ se tiene que la sucesión $0 \to F(M'') \to F(M) \to F(M') \to 0$ es exacta corta.

Un funtor contravariante exacto a la izquierda es el funtor $\operatorname{Hom}(-,N)\colon \mathbf{Mod}_R \to \mathbf{Ab}$. Si I es un R-módulo inyectivo el funtor $\operatorname{Hom}(-,I)$ es exacto.

Proposición 1.62. *Sean* M *y* N *R-módulos a la izquierda.*

(1) *Si I es inyectivo, entonces* $\mathrm{Ext}^n_R(M, I) = 0$, *para* $n \geq 0$.

(2) *Si P es proyectivo, entonces* $\mathrm{Ext}^n_R(P, N) = 0$.

(3) *Los funtores* $\mathrm{Ext}^0(-, N)$ *y* $\mathrm{Hom}_R(-, N)$ *son naturalmente equivalentes.*

(4) *Sea* $0 \to M' \to M \to M'' \to 0$ *una sucesión exacta corta de R-módulos. Se tiene una sucesión exacta larga*

$$\cdots \to \mathrm{Ext}^n_R(M'', N) \to \mathrm{Ext}^n_R(M, N) \to \mathrm{Ext}^n_R(M', N) \to \mathrm{Ext}^{n+1}_R(M'', N) \to \cdots$$

(5) *Sea* $0 \to N' \to N \to N'' \to 0$ *una sucesión exacta corta de R-módulos: se tiene una sucesión exacta larga*

$$\cdots \to \mathrm{Ext}^n_R(M, N') \to \mathrm{Ext}^n_R(M, N) \to \mathrm{Ext}^n_R(M, N'') \to \mathrm{Ext}^{n+1}_R(M, N') \to \cdots$$

Demostración. (1) Dado que el funtor $\mathrm{Hom}_R(-, I)$ es exacto, si $\mathbf{P}$ es una resolución proyectiva de M entonces el complejo $\mathrm{Hom}_R(\mathbf{P}, I)$ es exacto; Por tanto $H^n(\mathrm{Hom}_R(\mathbf{P}, I)) = 0$ para todo $n \geq 1$.

(2) Dado que $\mathbf{P}\colon \cdots \to 0 \to P_0 \to 0$, siendo $P_0 = P$, es una resolución proyectiva de P, se tiene que $\mathrm{Ext}^n_R(P, N) = 0$, para $n \geq 1$.

(3) Si $\mathbf{P}$ es una resolución proyectiva de N, entonces la sucesión $P_1 \to P_0 \to M \to 0$ es exacta. Por tanto, la sucesión $0 \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(P_0, N) \to \mathrm{Hom}_R(P_1, N)$ es exacta. Así, $H^0(\mathrm{Hom}_R(\mathbf{P}, N)) \cong \mathrm{Hom}_R(M, N)$. Claramente, este isomorfismo es natural.

(4) Por el lema 1.56, existe una sucesión exacta corta de complejos de R-módulos proyectivos $0 \to \mathbf{P'} \to \mathbf{P} \to \mathbf{P''} \to 0$ donde $\mathbf{P}$, $\mathbf{P'}$ y $\mathbf{P''}$ son resoluciones de M, M' y M'', respectivamente, y donde $P_n = P'_n \oplus P''_n$. Si $\pi\colon P_n \to P'_n$ es la proyección y $\mu\colon P'_n \to P_n$ es la inyección, dado que $\pi\mu = 1_{P'_n}$, se tiene que la sucesión $0 \to \mathrm{Hom}_R(P''_n, N) \to \mathrm{Hom}_R(P_n, N) \to \mathrm{Hom}_R(P'_n, N) \to 0$ es exacta. Por tanto, la sucesión

$$0 \to \mathrm{Hom}_R(\mathbf{P''}, N) \to \mathrm{Hom}_R(\mathbf{P}, N) \to \mathrm{Hom}_R(\mathbf{P'}, N) \to 0,$$

es exacta corta. El resultado se sigue de la proposición 1.40.

(5) Sea $\mathbf{P}$ una resolución proyectiva de M. Se tiene la sucesión exacta corta de complejos

$$0 \to \mathrm{Hom}_R(\mathbf{P}, N') \to \mathrm{Hom}_R(\mathbf{P}, N) \to \mathrm{Hom}_R(\mathbf{P}, N'') \to 0.$$

Aplicando la proposición 1.40 se tiene el resultado.

□

Capítulo 2

Cohomología de grupos

2.1. G-módulos

Sea G un grupo. Denotaremos la operación de G con la multiplicación y por $\mathbf{1}$ el elemento neutro de G. Si A es un grupo abeliano, denotaremos por $\operatorname{Aut} A$ el grupo de automorfismos de A y por $\operatorname{End}(A)$ el anillo de endomorfismos de A.

Definición 2.1. Se *llama anillo de grupo entero* de G y se denota por $\mathbb{Z}G$, al grupo abeliano libre sobre el conjunto G, es decir el conjunto $\sum_{x\in G} m_x\, x$, $m(x) \in \mathbb{Z}$ y donde $m_x \neq 0$ solo para un número finito de elementos $x \in G$, con la operación adición dada por

$$(\sum_{x\in G} m_x\, x) \,+\, (\sum_{x\in G} m'_x\, x) = \sum_{x\in G} (m_x + m'_x)\, x.$$

y con la operación multiplicación:

$$(\sum_{x\in G} m_x\, x)\,.\,(\sum_{y\in G} m_y\, y) = \sum_{x,y\in G} (m_x\, m_y)\, xy$$

Denotaremos por $j\colon G \to \mathbb{Z}G$ la aplicación dada por $j(x) = 1\, x$, para $x \in G$.

$\mathbb{Z}G$ verifica la siguiente propiedad universal: Si R es un anillo y $f\colon G \to R$ es una aplicación verificando que $f(x\,y) = f(x)\,.\,f(y)$, entonces existe un único homomorfismo de anillos $f' : \mathbb{Z}G \to R$ tal que $f' \circ i = f$. En efecto, f' es la aplicación dada por $f'(\sum_{x\in G} m_x\, x) = \sum_{x\in G} m_x\, f(x)$.

Definición 2.2. Se llama *ideal aumentación* de G y se denota por IG al núcleo del homomorfismo de anillos $\epsilon : \mathbb{Z}G \to \mathbb{Z}$, dado por $\epsilon(\sum_{x\in G} m_x\, x) = \sum_{x\in G} m_x$. la aplicación ϵ se llama *aplicación aumentación.*

Lema 2.3. (1) *IG es un grupo abeliano libre sobre el conjunto $T = \{x-\mathbf{1} \mid \mathbf{1} \neq x \in G\}$.*

(2) *Si el grupo G está generado por el conjunto S, entonces IG está generado por $S-\mathbf{1} = \{s-\mathbf{1} \mid s \in S\}$.*

Demostración. (1) Veamos que T es linealmente independiente. En efecto

$$\sum_{x\in G} m_x\,(x-\mathbf{1}) = 0 \iff \sum_{x\in G} m_x\,x - \sum_{x\in G} m_x\,\mathbf{1} = 0 \;\Rightarrow\; m_x = 0, \forall\, x \in G.$$

T genera IG, puesto que si $\sum_{x\in G} m_x\,x \in IG$, entonces $\sum_{x\in G} m_x = 0$ y se tiene

$$\sum_{x\in G} m_x\,x = \sum_{x\in G} m_x\,x - \sum_{x\in G} m_x\,\mathbf{1} = \sum_{x\in G} m_x\,(x-\mathbf{1}).$$

(2) Los elenmentos de G son producto finito de elementos de S o de inversos de elementos de S, es decir de la foma $x = s_1^{\pm 1}s_2^{\pm 1}\cdots s_r^{\pm 1}$. Por (1) es suficiente probar que $x-\mathbf{1}$ está en el $\mathbb{Z}G$-módulo generado por $S-\{\mathbf{1}\}$. El resultado se sigue se sigue de las igualdades:

$$s_1\,s_2-\mathbf{1} = s_1\,(s_2-\mathbf{1}) + (s_1-\mathbf{1}), \quad s^{-1}-\mathbf{1} = -s^{-1}(s-\mathbf{1}), \quad s, s_1, s_2 \in S. \qquad \square$$

Definición 2.4. Un *G-módulo a la izquierda* es un grupo abeliano A junto con un homomorfismo de grupos $\sigma\colon G \to \mathrm{Aut}(A)$. Denotaremos $\sigma(x)(a)$ por $x\circ a$ o simplemente por $x\,a$. Por la propiedad universal de $\mathbb{Z}G$ la existencia del homomorfismo de grupos $\sigma\colon G \to \mathrm{Aut}(A)$ es equivalente a la existencia de un homomorfismo de anillos $\bar{\sigma}\colon \mathbb{Z}G \to \mathrm{End}(A)$, es decir, A es un $\mathbb{Z}G$-módulo a la izquierda. La estructura de $\mathbb{Z}G$-módulo de A está dada por

$$(\sum_{x\in G} m_x\,x)\,a = \bar{\sigma}(\sum_{x\in G} m_x\,x)(a) = \sum_{x\in G} m_x(x\circ a).$$

Decimos que un G-módulo a la izquierda A es *trivial* si, $x\circ a = a$, para todo $x \in G$ y $a \in A$.

2.2. La cohomología de un grupo

Si A, A' son G-módulos a la izquierda, denotaremos los grupos abelianos $\mathrm{Hom}_{\mathbb{Z}G}(A, A')$ y $\mathrm{Ext}^n_{\mathbb{Z}G}(A, A')$ por $\mathrm{Hom}_G(A, A')$ y $\mathrm{Ext}^n_G(A, A')$, respectivamente.

Definición 2.5. Se llama *n-ésimo grupo de cohomología* de G con coeficientes en el G-módulo a la izquierda A al grupo abeliano

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

donde $\mathbb{Z}$ se considera un G-módulo trivial.

El funtor $H^n(G,-)$ es covariante. Podemos calcularlo tomando una resolución proyectiva $\mathbf{P}$ de $\mathbb{Z}$, formando el complejo $\mathrm{Hom}_G(\mathbf{P},A)$ y calculando su homología.

Si A es un G-módulo denotaremos por A^G el siguiente subconjunto de A:

$$A^G = \{a \in A \mid x \circ a = a,\ \forall\, x \in G\}.$$

A^G es el mayor submódulo de A sobre el cual G actúa trivialmente y llama *subgrupo de elementos G-invariantes* de A.

Proposición 2.6. *Sea A un G-módulo a la izquierda. Se tiene que $H^0(G,A) \cong A^G$ y si A es un G-módulo trivial, entonces $H^0(G,A) \cong A$.*

Demostración. Se tiene que $H^0(G,A) \cong \mathrm{Hom}_G(\mathbb{Z},A)$. La aplicación $\phi\colon \mathrm{Hom}_G(\mathbb{Z},A) \to A$, dada por $\phi(\varphi) = \varphi(1)$ es un homomorfismo de grupos abelianos inyectivo cuya imagen es A^G. □

Denotaremos por $[G,G]$ el subgrupo conmutador de G, es decir el subgrupo de G generado por todos los elementos de la forma $x\,y\,x^{-1}\,y^{-1}$, $x,y \in G$. El subgrupo $[G,G]$ es normal y denotaremos por G_{ab} el grupo abeliano cociente G/G', donde $G' = [G,G]$. Denotaremos por $q\colon G \to G_{\mathrm{ab}}$ la aplicación dada por $q(x) = xG'$.

Lema 2.7. *Los grupos abelianos G_{ab} y $IG/(IG)^2$ son isomorfos.*

Demostración. Por el Lema 2.3, el grupo abeliano IG es libre en $T = \{x-\mathbf{1} \mid e \neq x \in G\}$. La función $\psi\colon T \to G/G'$ definido por

$$\psi(x-\mathbf{1}) = xG'$$

se extiende de forma única a $\psi'\colon IG \to G/G'$. Dado que

$$(x-\mathbf{1})(y-\mathbf{1}) = (xy-\mathbf{1}) - (x-\mathbf{1}) - (y-\mathbf{1}),$$

se tiene que

$$\psi((x-\mathbf{1})(y-\mathbf{1})) = xyx^{-1}y^{-1}\,G' = G'$$

y entonces ψ' se factoriza a través de $\psi''\colon IG/(IG)^2 \to G/G'$.

Por otro lado, la aplicación $\varphi(x) = (x-\mathbf{1}) + (IG)^2$ es (mediante el mismo cálculo anterior) un homomorfismo de grupos. Puesto que

$$\varphi(xyx^{-1}y^{-1}) = \varphi(xy) - \varphi(yx) = (x-\mathbf{1}) + (y-\mathbf{1}) - (x-\mathbf{1}) - (y-\mathbf{1}) + (IG)^2 = (IG)^2,$$

φ' induce un homomorfismo de grupos $\varphi'\colon G/G' \to IG/(IG)^2$. Es trivial que φ' y ψ'' son inversas la una de la otra. □

Proposición 2.8. *Sea A un G-módulo trivial. Se tiene que $H^1(G,A) \cong \mathrm{Hom}_{\mathbb{Z}}(G_{ab}, A)$.*

Demostración. De nuevo, por definición tenemos

$$H^1(G,A) = \mathrm{Ext}^1_G(\mathbb{Z}, A),$$

La sucesión exacta

$$0 \longrightarrow IG \xrightarrow{i} \mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0,$$

induce por la proposición 1.62 (2) y (3), la sucesión exacta

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}, A) \xrightarrow{\epsilon^*} \mathrm{Hom}_G(\mathbb{Z}G, A) \xrightarrow{i^*} \mathrm{Hom}_G(IG, A) \longrightarrow H^1(G,A) \longrightarrow 0.$$

Para cada G-módulo A se tiene,

$$H^1(G,A) = \mathrm{coker}(i^* \colon A \to \mathrm{Hom}_G(IG, A)) \tag{2,8,1}$$

donde $i^*(a)(x-1) = xa - a, a \in A, x \in G$. Observemos que para cada G-módulo trivial A, i^* es el homomorfismo cero y entonces en este caso

$$H^1(G,A) \cong \mathrm{Hom}_G(IG, A).$$

Además, $\varphi \colon IG \to A$ es un homomorfismo de G-módulos si, y solo si, $\varphi(x(y-\mathbf{1})) = x \circ \varphi(y-\mathbf{1}) = \varphi(y-\mathbf{1})$, para $x, y \in G$, equivalentemente

$$\varphi((x-\mathbf{1})(y-\mathbf{1})) = 0, \quad x, y \in G.$$

Usando el lema anterior, se obtiene para cada G-módulo trivial A

$$H^1(G,A) \cong \mathrm{Hom}_{\mathbb{Z}}(IG/(IG)^2, A) \cong \mathrm{Hom}_{\mathbb{Z}}(G_{ab}, A). \qquad \square$$

Vamos a dar una interpretación de $H^1(G,A)$ para cualquier G-módulo A.

2.3. Derivaciones y producto semidirecto

Definición 2.9. Sea A un G-módulo a la izquierda. Una aplicación $d \colon G \to A$ se dice que es una *derivación* de G en A o un *homomorfismo cruzado* si verifica

$$d(x\,y) = d(x) + x \circ d(y), \quad x, y \in G$$

Si d es una derivación, entonces $d(1) = 0$. Denotaremos por $\mathrm{Der}(G,A)$ al conjunto de las derivaciones de G en A. El conjunto $\mathrm{Der}(G,A)$ con la operación adición

$$(d + d')(x) = d(x) + d'(x), \quad d, d' \in \mathrm{Der}(G,A),\ x \in G$$

es un grupo abeliano. Se tiene un funtor $\mathrm{Der}(G,-) : \mathrm{Gr} \to \mathrm{Ab}$.

Teorema 2.10. *Sea A un G-módulo. La aplicación $\Phi_A\colon \mathrm{Der}(G,A) \to \mathrm{Hom}_G(IG,A)$, dada por $(\Phi_A)(d)(x-\mathbf{1}) = d(x)$, para $x \in G$, es un isomorfismo de grupos abelianos.*

Demostración. Dada una derivación $d\colon G \to A$, el homomorfismo de grupos $\Phi_A(d) = \varphi_d\colon IG \to A$ definido por $\varphi_d(x-\mathbf{1}) = dx, x \in G$, es un homomorfismo de G-módulos. En efecto,

$$\varphi_d(y(x-\mathbf{1})) = \varphi_d((yx-\mathbf{1}) - (y-\mathbf{1})) = d(yx) - dy = dy + y \circ dx - dy = y \circ \varphi_d(x-\mathbf{1}).$$

Reciprocamente, dado un homomorfismo de G-módulos $\varphi\colon IG \to A$, definimos la aplicación $d_\varphi\colon G \to A$ con $d_\varphi(x) = \varphi(x-\mathbf{1})$. Veamos que d_φ es una derivación:

$$d_\varphi(xy) = \varphi(xy-\mathbf{1}) = \varphi(x(y-\mathbf{1}) + (x-\mathbf{1})) = x \circ \varphi(y-\mathbf{1}) + \varphi(x-\mathbf{1}) = x \circ d_\varphi(y) + d_\varphi(x).$$

Es obvio que Φ_A es un homomorfismo de grupos abelianos y que la aplicación que lleva φ a d_φ es inversa de Φ_A. □

Proposición 2.11. *Se tiene una equivalencia natural $\Phi : \mathrm{Der}(G,-) \to \mathrm{Hom}(IG,-)$, dada por $\Phi(M) = \Phi_M$.*

Demostración. Hay que probar que si $f\colon A \to B$ es un homomorfismo de G-módulos entonces el cuadrado

$$\begin{array}{ccc} \mathrm{Der}(G,A) & \xrightarrow{\Phi_A} & \mathrm{Hom}_G(IG,A) \\ {\scriptstyle \mathrm{Der}(G,f)}\downarrow & & \downarrow{\scriptstyle \mathrm{Hom}_G(IG,f)} \\ \mathrm{Der}(G,B) & \xrightarrow{\Phi_B} & \mathrm{Hom}_G(IG,B) \end{array}$$

es conmutativo. En efecto, sea $d \in \mathrm{Der}(G,A)$. Se tiene

$$((\Phi_B \circ \mathrm{Der}(G,f))(d))(x-\mathbf{1}) = (\Phi_B(f\,d))(x-\mathbf{1}) = (f\,d)(x) = f(d((x)),$$

Analogamente,

$$(\mathrm{Hom}_G(IG,f) \circ \Phi_A)(x-\mathbf{1}) = (f\,\Phi_A(d))(x-\mathbf{1}) = f(\Phi_A(d)(x-\mathbf{1})) = f(d(x)).$$

Por tanto se tiene que $\Phi_B \circ \mathrm{Der}(G,f) = \mathrm{Hom}_G(IG,f) \circ \Phi_A$. □

Se dice que el ideal aumentación IG representa el funtor $\mathrm{Der}(G,-)$.

Definición 2.12. Sea $a \in A$. Se dice que la aplicación $d_a\colon G \to A$ es una *derivación interior* o *homomorfismo cruzado principal* si $d_a(x) = (x-\mathbf{1})\,a$, para cada $x \in G$.

Toda derivación interior es una derivación. Denotaremos por $\mathrm{IDer}(G, A)$ el conjunto de derivaciones interiores de G en A. El conjunto $\mathrm{IDer}(G, A)$ es un subgrupo de $\mathrm{Der}(G, A)$.

Proposición 2.13. *Se tiene*

$$H^1(G, A) \cong \frac{\mathrm{Der}(G, A)}{\mathrm{IDer}(G, A)}.$$

Demostración. El teorema 2.10 ahora nos permite dar una descripción del primer grupo de cohomología en términos de derivaciones. Por (2.8.1), $H^1(G, A)$ es el cociente de $\mathrm{Hom}_G(IG, A)$ por el subgrupo de homomorfismos $\varphi\colon IG \to A$ de la forma $\varphi(x-1) = xa-a$ para algún $a \in A$. La derivación $d_\varphi\colon G \to A$ asociada a φ es una derivación interior, es decir

$$d_\varphi(x) = (x-1)a$$

para algún $a \in A$. Por tanto,

$$H^1(G, A) \cong \frac{\mathrm{Der}(G, A)}{\mathrm{IDer}(G, A)}.$$

□

Definición 2.14. Sean $i\colon N \to E$ y $p\colon E \to G$ homomorfismos de grupos. Se dice que

$$1 \to N \xrightarrow{i} E \xrightarrow{p} G \to 1. \qquad (\star)$$

es una *sucesión exacta corta de grupos* si i es una aplicación inyectiva, $\ker p = i(N)$ y p es una aplicación suprayectiva. Se dice que la sucesión exacta corta $(\star)$ *rompe* o que $(\star)$ es una *sucesión exacta corta rota*, si existe un homomorfismo de grupos $s\colon G \to E$ tal que $p \circ s = 1$.

Dado que $(\star)$ es una sucesión exacta corta, N es isomorfo a un subgrupo normal de E y p induce un isomorfismo de grupos $E/i(N) \cong G$.

Definición 2.15. Sea G un grupo y A un G-módulo. Se llama *producto semidirecto* $A \rtimes G$ al conjunto $A \times G$ con la siguiente operación multiplicación:

$$(a, x)\,.\,(a', x') = (a + x \circ a', x\,x')$$

Con esta operación el producto semidirecto $A \rtimes G$ es un grupo. El elemento neutro es $(0, \mathbf{1})$ y $(a, x)^{-1} = (-x^{-1} \circ a, x^{-1})$. La aplicación $\iota\colon A \to A \rtimes G$, dada por $\iota(a) = (a, \mathbf{1})$, es un homomorfismo de grupos inyectivo. La aplicación $\pi\colon A \rtimes G \to G$, dada por $\pi(a, x) = x$, es un homomorfismo de grupos sobreyectivo. Se tiene la sucesión exacta corta rota de grupos

$$0 \to A \xrightarrow{\iota} A \rtimes G \xrightarrow{\pi} G \to 1. \qquad (\star\star)$$

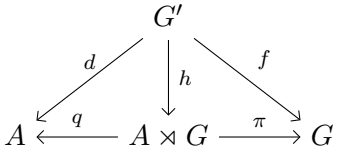
La sucesión exacta corta ($\star\star$) rompe puesto que la aplicación $\tilde{s}\colon G \to A \rtimes G$, dada por $\tilde{s}(x) = (0, x)$, es un homomorfismo de grupos y $\pi \circ \tilde{s} = 1_G$. El G-módulo A es un $A \rtimes G$-módulo con la acción

$$(a', x) \circ a = x \circ a, \quad x \in G, a, a' \in A,$$

es decir, con la acción vía p. La aplicación $q\colon A \rtimes G \to A$, $q(a, x) = a$, es una derivación. En efecto,

$$q((a, x)\,.\,(a', x')) = q(a + x\,a', x\,x') = a + x\,a' = q(a, x) + (a, x)\,q(a', x').$$

Proposición 2.16. *Sean G un grupo y A un G-módulo. Para cada homomorfismo $f\colon G' \to G$ de grupos y cada f-derivación $g\colon G' \to A$ (es decir, d es una derivación donde A se considera un G-módulo con la acción $x \circ a = f(x) \circ a$), existe un único homomorfismo $h\colon G' \to A \rtimes G$ de grupos que hace conmutativo el siguiente diagrama*



Recíprocamente, cada homomorfismo $h\colon G' \to A \rtimes G$ de grupos determina un homomorfismo $f = \pi\,h\colon G' \to G$ de grupos y una f-derivación $q\,h\colon G' \to A$.

Demostración. La aplicación h está definida por $hx = (dx, fx), x \in G$, y es sencillo comprobar que h es un homomorfismo.

□

Corolario 2.17. *Existe una aplicación biyectiva entre el conjunto de derivaciones de G en A y el conjunto de homomorfismos de grupos $f\colon G \to A \rtimes G$ tales que $p \circ f = 1_G$.*

Demostración. Basta tomar $f = 1_G$. □

Teorema 2.18. *Si F es un grupo libre sobre el conjunto S, entonces el ideal aumentación IF es un $\mathbb{Z}F$-módulo libre sobre el conjunto $S - \mathbf{1} = \{s - \mathbf{1} \mid s \in S\}$.*

Demostración. Veamos que cualquier aplicación f del conjunto $\{s - \mathbf{1} \mid s \in S\}$ en un F-módulo M puede extenderse de forma única a un homomorfismo de F-módulos $f'\colon IF \to M$. En primer lugar, observemos que la unicidad es clara, ya que $\{s - \mathbf{1} \mid s \in S\}$ genera IF como F-módulo, por el lema 2.3. Como F es libre en S, existe un homomorfismo de grupos $\bar{f}\colon F \to M \rtimes F$ tal que $\bar{f}(s) = (f(s - \mathbf{1}), s)$. Por el Corolario 2.17, $\bar{f}$ se tiene una derivación $d\colon F \to M$ con $d(s) = f(s - \mathbf{1})$. Por la proposición 2.10 a d le corresponde un homomorfismo de F-módulos $f'\colon IF \to M$ con $f'(s - \mathbf{1}) = f(s - \mathbf{1})$. □

Corolario 2.19. *Para todo grupo libre F y todo G-módulo A, se tiene*

$$H^0(F,\mathbb{Z}) \cong \mathbb{Z}, \quad H^1(F,\mathbb{Z}) \cong \prod_{s\in S} \mathbb{Z}, \quad H^n(F,A) = 0, \quad n \geq 2.$$

Demostración. Se tiene la siguiente resolución de $\mathbb{Z}$:

$$\mathbf{P}\colon \cdots \longrightarrow 0 \longrightarrow \cdots \longrightarrow 0 \longrightarrow IF \longrightarrow \mathbb{Z}F \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

formada por F-módulos libres y $H^n(F,A) = H^n(\mathrm{Hom}_F(\mathbf{P},A))$. Así, $H^n(F,M) = 0$, para $n \geq 2$ y $H^0(F,\mathbb{Z}) \cong \mathbb{Z}$. Como F es un grupo libre sobre S, $F/[F,F]$ es un grupo abeliano libre sobre S. Luego,

$$H^1(F,\mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(F/[F,F],\mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(\bigoplus_{s\in S}\mathbb{Z},\mathbb{Z}) \cong \prod_{s\in S}\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}) \cong \prod_{s\in S}\mathbb{Z}. \qquad \square$$

2.4. La cohomología de los grupos cíclicos

En esta sección se calculan los grupos de cohomología de un grupos cíclico finito C_k con coeficientes en un C_k módulo. Se prueba que la cohomología de los grupos cíclicos finitos es periódica.

Sea C_k un grupo cíclico de orden k con generador τ.

Definición 2.20. Se llama norma en $\mathbb{Z}C_k$ al elemento $N = \mathbf{1} + \tau + \tau^2 + \ldots + \tau^{k-1}$.

Proposición 2.21. *El C_k-módulo trivial $\mathbb{Z}$ tiene la siguiente resolución formada por C_k-módulos libres:*

$$\ldots \xrightarrow{N} \mathbb{Z}C_k \xrightarrow{\tau-\mathbf{1}} \mathbb{Z}C_k \xrightarrow{N} \mathbb{Z}C_k \xrightarrow{\tau-\mathbf{1}} \mathbb{Z}C_k \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0, \qquad (2{,}21{,}1)$$

donde por N y $\tau - \mathbf{1}$ denotamos la multiplicación por N y $\tau - \mathbf{1}$, respectivamente.

Demostración. Dado que

$$N(\tau-\mathbf{1}) = (\mathbf{1}+\tau+\ldots+\tau^{k-1})(\tau-\mathbf{1}) = \tau+\tau^2+\ldots+\tau^{k-1}+\tau^k-(\mathbf{1}+\tau+\ldots+\tau^{k-1}) = \tau^k-1 = 0,$$

y $\epsilon(\tau - \mathbf{1}) = \epsilon(\tau) - \mathbf{1} = 0$, entonces $\mathbf{C}$ es un complejo de cadenas de $\mathbb{Z}C_k$-módulos libres positivo. Veamos que la sucesión:

$$0 \longrightarrow IC_k \to \mathbb{Z}C_k \xrightarrow{N} N\,\mathbb{Z} \longleftrightarrow 0$$

es exacta: Dado que $N\,\tau^i = N$, para todo $i \in \mathbb{N}$,

$$N(\sum_{i=0}^{k-1} m_{\tau^i}\,\tau^i) = \sum_i m_{\tau^i}\,N \in N\,\mathbb{Z}.$$

Se tiene que $IC_k \subset \ker N$:

$$N(\sum_i m_{\tau^i}\,(\tau^i - \mathbf{1})) = \sum_i m_{\tau^i}\,N(\tau^i - \mathbf{1}) = \sum_i m_{\tau^i}\,0 = 0.$$

Recíprocamente, si $\sum_i m_{\tau^i}\,\tau^i \in \operatorname{Ker} N$, entonces

$$N(\sum_i m_{\tau^i}\,\tau^i) = \sum_i m_{\tau^i}\,N = 0.$$

Aplicando ϵ se tiene

$$\epsilon(\sum_i m_{\tau^i}\,N) = \sum_i m_{\tau^i}\,k = 0,$$

y entonces $\sum_i m_{\tau^i} = 0$, con lo cual $\sum_i m_{\tau^i}\tau^i \in IG$. Veamos que la sucesión

$$0 \longrightarrow N\,\mathbb{Z} \longrightarrow \mathbb{Z}C_k \xrightarrow{\tau-\mathbf{1}} IC_k \longrightarrow 0,$$

es exacta. La aplicación $\tau - \mathbf{1}\colon \mathbb{Z}C_k \to IC_k$ es sobre puesto que

$$\sum_i m_{\tau^i}(\tau^i - 1) = \sum_i m_{\tau^i}(\tau - \mathbf{1})(\tau^{i-1} + \ldots + \tau + \mathbf{1}) \in (\tau - \mathbf{1})(\mathbb{Z}C_k).$$

Además, $\ker(\tau - \mathbf{1}) = N\,\mathbb{Z}$. En efecto,

$$\begin{aligned}(\tau - \mathbf{1})(\sum_i m_{\tau^i}\tau^i) = 0 &\iff \sum_i m_{\tau^i}\tau^{i+1} = \sum_i m_{\tau^i}\tau^i \\ &\iff m_1 = m_\tau = m_{\tau^2} = \ldots = m_{\tau^{i-1}}\end{aligned}$$

y entonces

$$\sum_i m_{\tau^i}\tau^i = \sum_i m_1\tau^i = m_1\,N \in \mathbb{N}\,\mathbb{Z}.$$

□

Teorema 2.22. *Si A es un C_k-módulo y $m \geq 1$ entonces*

$$H^n(C_k, A) \cong \begin{cases} \{a \in A \mid x \circ a = a\}, \text{ para } n = 0 \\ \{a \in A \mid N\,a = 0\}/(\tau - \mathbf{1})\,A, \text{ para } n = 2m-1 \\ \{a \in A \mid x \circ a = a\}/NA, \text{ para } n = 2m \end{cases}$$

Demostración. Aplicando el funtor $\operatorname{Hom}_{C_k}(-, A)$ a la resolución (2.21,1) de $\mathbb{Z}$ y teniendo en cuenta que $\operatorname{Hom}_{C_k}(\mathbb{Z}C_k, A) \cong A$, se tiene el complejo

$$0 \longrightarrow \operatorname{Hom}_{C_k}(\mathbb{Z}, A) \longrightarrow A \xrightarrow{N} A \xrightarrow{\tau-\mathbf{1}} A \xrightarrow{N} A \xrightarrow{\tau-\mathbf{1}} \cdots$$

y calculando su cohomología se tiene el resultado. □

Corolario 2.23. *Si $G = \{\mathbf{1}\}$, entonces $H^n(G, A) = 0$, para todo G-módulo A y para todo $n > 0$.*

Demostración. Es trivial. □

Corolario 2.24. *Si A es un C_K-módulo trivial y $m \geq 1$, entonces*

$$H^n(C_k, A) \cong \begin{cases} A, \text{ para } n = 0 \\ \{a \in A \mid k\,a = 0\}, \text{ para } n = 2m-1 \\ A/k\,A, \text{ para } n = 2m \end{cases}$$

En particular,

$$H^0(C_k, \mathbb{Z}) \cong \mathbb{Z}, \quad H^{2m-1}(C_k, \mathbb{Z}) = 0, \quad H^{2m}(C_k, \mathbb{Z}) \cong \mathbb{Z}/k\mathbb{Z}.$$

Demostración. Es trivial. □

Teorema 2.25. *Si $C = \langle \tau \rangle$ es un grupo cíclico infinito y M un C-módulo, se tiene*

$$\begin{aligned} H^0(C, A) &\cong \{a \in A \mid a\,\tau = a\}, \\ H^1(C, A) &\cong A/A(\tau - 1) \\ H^n(C, A) &= 0, \text{ para } n \geq 2 \end{aligned}$$

Demostración. Dado que C es un grupo libre con base $\{\tau\}$, por el lema 2.3, IC es un C-módulo libre sobre el conjunto $\{\tau - 1\}$ y entonces la aplicación $h\colon \mathbb{Z}C \to IC$, dada por $h(a) = (\tau - 1)\,a$, para $a \in \mathbb{Z}C$ es un isomorfismo de C-módulos. Se tiene la resolución C-libre de $\mathbb{Z}$

$$\mathbf{P}\colon \cdots \longrightarrow 0 \longrightarrow \mathbb{Z}C \xrightarrow{\tau-1} \mathbb{Z}C \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0.$$

y $H^n(C, A) = H^n(\mathrm{Hom}_C(\mathbf{P}, A))$. El complejo $\mathrm{Hom}_C(\mathbf{P}, A)$ es isomorfo al complejo

$$\mathbf{P}'\colon\ 0 \longrightarrow A \xrightarrow{\tau-1} A \longrightarrow 0 \longrightarrow \cdots.$$

Calculando sus grupos de cohomologia se obtiene el resultado. □

2.5. La resolución estándar

En esta sección se introduce la resolución estándar o barra normalizada de $\mathbb{Z}$ y a partir de ella se obtienen propiedades fundamentales de los grupos de cohomología $H^n(G, A)$. Si G es un grupo denotaremos po G^* el conjunto $G - \{\mathbf{1}\}$.

Notación 2.26. *Denotaremos por B_0 el G-módulo libre con base el símbolo $[\ ]$. Así, $B_0 \simeq \mathbb{Z}G$, Para $n \geq 1$, sea B_n el G-módulo libre con base $(G^*)^n$, el producto cartesiano de n copias de G^*. Escribiremos*

$$[x_1|x_2|\dots|x_n] = \begin{cases} (x_1,\dots,x_n), \text{ si } x_i \neq 1,\ i = 1,\dots n \\ 0, \text{ si existe } i \in \{1,\dots,n\} \text{ tal que } x_i = \mathbf{1}. \end{cases}$$

Proposición 2.27. *La sucesión*

$$\mathbf{B}\colon\ \dots \longrightarrow B_n \xrightarrow{d_n} \dots \longrightarrow B_1 \xrightarrow{d_1} B_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

es una resolución de $\mathbb{Z}$ donde la diferencial d_n es el homomorfismo de G-módulos dado por

$$d_n[x_1|x_2|\dots|x_n] = x_1[x_2|\dots x_n] + \sum_{i=1}^{n-1}(-1)^i[x_1|x_2|\dots|x_ix_{i+1}|\dots x_n] + (-1)^n[x_1|x_2|\dots|x_{n-1}]$$

para $n \geq 1$, siendo $d_1[x_1] = x_1[\ ] - [\ ]$, y donde $\epsilon\colon B_0 \to \mathbb{Z}$, dado por $\epsilon[\ ] = 1$, es la aumentación.

Demostración. Para probar la exactitud de $\mathbf{B}$ definimos una sucesión $\{s_n\}$ de homomorfismos de grupos abelianos que forman una contracción de homotopía,

$$\mathbb{Z} \xrightarrow{s_{-1}} B_0 \xrightarrow{s_0} B_1 \xrightarrow{s_1} B_2 \longrightarrow \dots$$

es decir, tales que

$$\epsilon \circ s_{-1} = \mathrm{id}_{\mathbb{Z}}, \quad d_1s_0 + s_{-1}\epsilon = \mathrm{id}_{C_0}, \quad d_{n+1}s_n + s_{n-1}d_n = \mathrm{id}_{C_n},\ n \geq 1.$$

Obsérvese que $\{1\}$ es una $\mathbb{Z}$-base $\mathbb{Z}$, $\{x[\ ] \mid x \in G\}$ es una $\mathbb{Z}$-base para $\mathbb{Z}G$ y $\{x_0[x_1|x_2|\dots|x_n], \mid x_i \in G, i = 1,\dots,n\}$ es una $\mathbb{Z}$ base para B_n. Por tanto tenemos homorfismos de grupos abelianos $s_{-1}\colon \mathbb{Z} \to C_0$, $s_n\colon C_n \to C_{n+1}$ tales que

$$s_{-1}(1) = [\ ], \quad s_0(x_0[\ ]) = [x_0], \quad s_n(x_0[x_1|\dots|x_n]) = [x_0|x_1|\dots|x_n],\ n \geq 1.$$

Veamos que $\{s_n\}$ es una contracción de homotopía:

$$\epsilon(s_{-1})(1) = \epsilon([\ ]) = 1, \quad (d_1s_0 + s_{-1}\epsilon)(x_0[\ ]) = x_0[\ ] - [\ ] + [\ ] = x_0[\ ].$$

Si $n > 0$, tenemos

$$\begin{aligned} d_{n+1}s_n(x_0[x_1|\dots|x_n]) =& d_{n+1}[x_0|x_1|\dots|x_n] \\ &= x_0[x_1|\dots|x_n] + \sum_{i=0}^{n-1}(-1)^{i+1}[x_0|\dots|x_i|x_{i+1}|\dots|x_n], \\ &+ (-1)^{n+1}[x_0|\dots|x_{n-1}] \end{aligned}$$

$$\begin{aligned}
s_{n-1}d_n(x_0[x_1|\dots|x_n]) =& s_{n-1}(x_0\, d_n[x_1|\dots|x_n]) \\
&= s_{n-1}(x_0\, x_1[x_2|\dots|x_n]) + \sum_{i=1}^{n-1}(-1)^i s_{n-1}(x_0[x_1|\dots|x_i|x_{i+1}|\dots|x_n]) \\
&+ (-1)^n s_{n-1}(x_0[x_1|\dots|x_{n-1}]) \\
&= [x_0\, x_1|x_2|\dots|x_n] + \sum_{i=1}^{n-1}(-1)^i[x_0|x_1|\dots|x_i\, x_{i+1}|\dots|x_n] \\
&+ (-1)^n[x_0|x_1|\dots|x_{n-1}].
\end{aligned}$$

y entonces $d_{n+1}s_n(x_0[x_1|\dots|x_n] + s_{n-1}d_n(x_0[x_1|\dots|x_n]) = x_0[x_1|\dots|x_n]$.

Veamos que $\mathbf{B}$ es un complejo de cadenas, es decir que $\epsilon\, d_1 = 0$ y que $d_n\, d_{n+1} = 0$.Dado que B_1 es un G-módulo libre sobre G es suficiente probar que $(\epsilon\, d_1)[x] = 0$, lo cual es cierto, puesto que

$$\epsilon\, d_1[x] = \epsilon(x[\,] - [\,]) = x\,1 - 1 = 0$$

Dado que $s_n(B_n)$ para $n > 0$ contiene el conjunto de generadores

$$\{[x_0|\dots|x_n] \mid x_i \in G, i = 0, \dots, n\},$$

es suficiente probar que $d_n\, d_{n+1}\, s_n = 0$. Razonando por inducción sobre n, podemos suponer que $d_{n-1}\, d_n = 0$. Se tiene

$$d_n\, d_{n+1}\, s_n = d_n(1 - s_{n-1}\, d_n) = d_n - (1 - s_{n-1}\, d_{n-1})d_n = s_{n-1}\, d_{n-1}\, d_n = 0. \qquad \square$$

Definición 2.28. La resolución $\mathbf{B}$ de $\mathbb{Z}$ de la proposición 2.27 se llama *resolución estándar* o *resolución barra* normalizada de $\mathbb{Z}$.

Proposición 2.29. *Sea A un G-módulo y sea $\mathbf{B}$ la resolución estándar normalizada de $\mathbb{Z}$ y consideremos el complejo de grupos abelianos*

$$\mathrm{Hom}_G(\mathbf{B}, A)\colon 0 \to \mathrm{Hom}_G(B_0, A) \xrightarrow{d_0^*} \mathrm{Hom}_G(B_1, A) \xrightarrow{d_1^*} \dots$$

La diferencial d^* de este complejo, al restringirnos a la base $\{[x_1|\dots|x_n] \mid x_i \in G^*\}$ de B_n como G-módulo, está dada por

$$\begin{aligned}
d_n^*(f)[x_1|\dots|x_n] =& x_1 \circ f[x_2|\dots|x_n] + \sum_{i=1}^{n}(-1)^i f[x_1|\dots|x_i x_{i+1}|\dots|x_{n+1}] \\
&+(-1)^{n+1} f[x_1|\dots|x_{n-1}]
\end{aligned}$$

para todo $f \in \mathrm{Hom}_G(B_n, A)$.

Demostración.

$$\begin{aligned} d_n^*(f)[x_1,\dots,x_n] =& f[x_1(x_2|\dots|x_n] + \sum_{i=1}^{n}(-1)^i[x_1|\dots|x_ix_{i+1}|\dots|x_{n+1}] \\ &+(-1)^{n+1}[x_1|\dots|x_n]) \\ =& x_1 \circ f[x_2|\dots|x_n] + \sum_{i=1}^{n}(-1)^i f[x_1|\dots|x_ix_{i+1}|\dots|x_{n+1}] \\ &+(-1)^{n+1}f(x_1|\dots|x_{n-1})) \end{aligned} \tag{$\star$}$$

□

Sea A un G-módulo, denotaremos por $C^0(G,A)$ el grupo abeliano A y por $n>0$ por $C^n(G,A)$ para $n>0$ el conjunto

$$C^n(G,A) = \{f\colon G\times \overset{n}{\dots} \times G \to A \mid f(x_1,\dots,x_n) = 0, \text{si algún } x_i = \mathbf{1}\}.$$

Proposición 2.30. *El conjunto $C^n(G,A)$ es un grupo abeliano con la operación adición usual, es decir si $f, f' \in C^n(G,A)$ y $n>0$,*

$$(f+f')(x_1,\dots,x_n) = f(x_1,\dots,x_n) + f'(x_1,\dots,x_n), \quad (x_1,\dots,x_n) \in G\times \overset{n}{\dots} \times G.$$

La aplicación $\delta^n\colon C^n(G,A) \to C^{n+1}(G,A)$, dada por

$$\begin{aligned} \delta^n(f)(x_1,\dots,x_{n+1}) =& x_1 \circ f(x_2,\dots,x_n) + \sum_{i=1}^{n}(-1)^i f(x_1,\dots,x_{i-1},x_i\,x_{i+1},\dots,x_{n+1}) \\ &+(-1)^{n+1}f(x_1,\dots,x_{n-1}). \end{aligned}$$

para $n>0$ y $\delta^0(a)(x_1) = x_1\circ a - a$, es un homomorfismo de grupos abelianos.

Demostración. La demostración es elemental. □

Obsérvese que para $n=1$, tenemos

$$\delta^1(f)(x_1,x_2) = x_1 \circ f(x_2) - f(x_1x_2) + f(x_1),$$

y para $n=2$ tenemos

$$\delta^2(f)(x_1,x_2,x_3) = x_1 \circ f(x_2,x_3) - f(x_1x_2,x_3) + f(x_1,x_2\,x_3) - f(x_1,x_2).$$

Veamos que

$$C^*(G,A):\ 0 \to C^0(G,A) \xrightarrow{\delta^0} C^1(G,A) \xrightarrow{\delta^1} \dots$$

es un complejo de grupos abelianos.

Notación 2.31. *Denotaremos por* $Z^n(G,A) = \ker \delta^n$ *y por* $D^n(G,A) = \delta^{n-1}(C^n(G,A))$. *los conjuntos* $Z^n(G,A)$ *y* $D^n(G,A)$ *son subgrupos de* $C^n(G,A)$.

Proposición 2.32. *Sea* A *un* G*-módulo a la izquierda. Se tienen isomorfismos de grupos abelianos*

$$\Psi_n \colon C^n(G,A) \longrightarrow \mathrm{Hom}_G(B_n, A), \quad n \geq 0,$$

que hacen conmutativo el siguiente cuadrado

$$\begin{array}{ccc} C^{n-1}(G,A) & \xrightarrow{\Psi_{n-1}} & \mathrm{Hom}_G(B_{n-1}, A) \\ \downarrow{\scriptstyle \delta^{n-1}} & & \downarrow{\scriptstyle d_n^*} \\ C^n(G,A) & \xrightarrow{\Psi_n} & \mathrm{Hom}_G(B_n, A) \end{array}$$

Demostración. Puesto que B_n es el G-módulo libre sobre el conjunto

$$\{(x_1, \ldots, , x_n) \mid x_i \in G^*, i = 1, \ldots, n\}$$

para cada $f \in C^n(G,A)$, existe un único $\Psi_n(f) \in \mathrm{Hom}_G(B_n, A)$ que extiende a $f_{|_{(G^*)^n}}$, es decir tal que el triángulo

$$\begin{array}{ccc} G^* \times \overset{n}{\times} \ldots G^* & \xrightarrow{\ i\ } & B_n \\ & {\scriptstyle f_{|_{(G^*)^n}}} \searrow & \downarrow{\scriptstyle \Psi_n(f)} \\ & & A \end{array}$$

es conmutativo. Recíprocamente, dado $g \in \mathrm{Hom}_G(B_n, A)$ se tiene una aplicación $f \in C^n(G,A)$ poniendo

$$f(x_1, \ldots, x_n) = \begin{cases} g\, i(x_1, \ldots, x_n), \text{ si } (x_1, \ldots, x_n) \in (G^*)^n \\ 0, \text{ si algún } x_i = 1 \end{cases}$$

Claramente Ψ_n es una aplicación biyectiva y se comprueba fácilmente que Ψ_n es un isomorfismo de grupos y que el cuadrado es conmutativo. □

Corolario 2.33. *Se tiene que*

$$C^*(G,A) : \ 0 \to C^0(G,A) \xrightarrow{\delta^0} C^1(G,A) \xrightarrow{\delta^1} \ldots$$

es un complejo de grupos abelianos.

Demostración. Se tiene

$$\Psi_{n+1}\,\delta^n\,\delta^{n-1} = d^*_{n+1}\,\Psi_n\,\delta^{n-1} = d^*_{n+1}\,d^*_n\,\Psi_{n-1} = 0 \iff \delta^n\,\delta^{n-1} = 0.$$

□

Corolario 2.34. *Sea G un grupo y A un G-módulo. El isomorfismo de complejos $\Psi^* = (\Psi_n)_{n\geq 0}$ induce un isomorfismo de grupos abelianos*

$$H^n(\Psi^*):\ H^n(C^*(G,A)) \to H^n(G,A), \quad n \geq 0.$$

Demostración. Se tiene que

$$H^n(G,A) = H^n(\mathrm{Hom}_G(\mathbf{B},A)).$$

El resultado se sigue de que $H^n(-)$ es un funtor, Ψ^* es un isomorfimo y los funtores llevan isomorfismos a isomorfismos. □

Teorema 2.35. *Si G es un grupo finito y A es un G-módulo, entonces todo elemento de $H^n(G,A)$, para $n>0$, tiene orden finito que es un divisor del orden de G.*

Demostración. Sea $f \in C^n(G,A)$ y pongamos

$$u(x_1,\ldots,x_{n-1}) = \sum_{x\in G} f(x_1,\ldots,x_{n-1},x).$$

Se tiene que $u \in C^{n-1}(G,A)$. Si sumamos las fórmulas de la proposición 2.30 para $\delta^n(f)$ y para todo $x \in G$, se tiene

$$\begin{aligned}\sum_{x\in G}\delta^n(f)(x_1,\ldots,x_n,x) =& x_1 \circ u(x_2,\ldots,x_n) + \sum_{i=1}^{n-1}(-1)^i u(x_1,\ldots,x_{i-1},x_i\,x_{i+1},\ldots,x_n)\\ &+(-1)^n u(x_1,\ldots,x_{n-1}) + (-1)^{n+1}|G|f(x_1,\ldots,x_n)\\ =&\delta^{n-1}(u)(x_1,\ldots,x_n) + (-1)^{n+1}|G|f(x_1,\ldots,x_n)\end{aligned}$$

puesto que

$$\sum_{x\in G} f(x_1,\ldots,x_{n-1},x_n x) = u(x_1,\ldots,x_{n-1}),$$

Si $\delta_n(f) = 0$ entonces

$$|G|f(x_1,\ldots,x_n) = \pm\delta^{n-1}(u)(x_1,\ldots,x_n) \in D^n(G,A).$$

Por tanto, si $f \in Z^n(G,A)$ entonces $|G|f = \pm\delta^{n-1}(u) \in B^n(G,A)$. Así,

$$|G|\,\mathbb{Z}^n(G,A) \subset B^n(G,A).$$

y $|G|\,H^n(G,A) = 0$, lo que demuestra el teorema. □

Corolario 2.36. *Sea G un grupo finito y A un G-módulo finito y tal que* m.c.d.$(|G|, |A|) = 1$. *Se tiene que $H^n(G, A) = 0$, para todo $n > 0$.*

Demostración. Se tiene que $|A| f = 0$, para todo $f \in C^n(G, A)$ y entonces $|A| H^n(G, A)$, para todo $n \geq 0$. Por el teorema 2.35, $|G| H^n(G, A) = 0$. Dado que m.c.d.$(|G|, |A|) = 1$, existen $r, s \in Z$ tales que $r|G| + s|A| = 1$. Se tiene:

$$H^n(G, A) = r|G| H^n(G, A) + s|A| H^n(G, A) = 0.$$

□

2.6. $H^2(G, M)$ y Extensiones

En esta sección vamos a dar la interpretación clásica de $H^2(G, A)$ en términos de extensiones de G por A.

Sea $0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 0$ una sucesión exacta corta de grupos con A abeliano. Denotaremos la operación de los grupos A y E como la adición y la de G como la multiplicación.

Lema 2.37. *Sea $0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ una sucesión exacta corta de grupos con A abeliano. Sea $s\colon G \to E$ una sección de p, es decir una aplicacion tal que $p \circ s = 1_G$. Se tiene que s induce una estructura de G-módulo en A con la acción*

$$i(x \circ a) = s(x) + i(a) - s(x), \;\; x \in G,\, a \in A$$

Demostración. La aplicación $\mu\colon G \to \mathrm{Aut}(A)$, dada por $i(\mu(x)(a)) = s(x) + i(a) - s(x)$ es un homomorfismo de grupos. En efecto, si denotamos $\mu(x)(a)$ por $x \circ a$, entonces $i((x\,y) \circ ia) = s(x\,y) + i(a) - s(x\,y)$. Dado que $p(s(x\,y) - s(y) - s(x) = 0$, existe $b \in A$ tal que $s(x\,y) = s(x) + s(y) + i(b)$. Así, por ser $i(A)$ un grupo abeliano

$$\begin{aligned} i((x\,y) \circ a) =& s(x\,y) + i(a) - s(x\,y) = s(x) + s(y) + +i(b) + i(a) - i(b) - s(y) - s(x) \\ =& s(x) + s(y) + i(a) - s(y) - s(x) = s(x) + i(y \circ a) - s(x) = i(x \circ (y \circ a)) \end{aligned}$$

□

Observación 2.38. Si $s' : G \to E$ es otra sección de p, entonces la acción inducida por s' coincide con la acción inducida por s. En efecto, dado que $p(s(x)) = p(s'(x)) = \mathbf{1}$, existe $a' \in A$ tal que $s(x) = s'(x) + i(a')$. Así, $s(x) + i(a) - s(x) = s'(x) + i(a') + i(a) + i(a') - s'(x) = s'(x) + i(a) - s(x')$.

Definición 2.39. Una *extensión de un grupo G por un G-módulo A* es una sucesión exacta corta de grupos $0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ donde la estructura de G-módulo de A coincide con la inducida por una sección de p, es decir

$$i(x \circ a) = s(x) + i(a) - s(x), \quad x \in G,\, a \in A.$$

siendo $s\colon G \to E$ una sección cualquiera de p.

Se dice que las extensiones $0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ y $0 \to A \xrightarrow{i} E' \xrightarrow{p} G \to 1$ son *equivalentes* si existe un homomorfismo de grupos $h\colon E \to E'$ tal que el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle h} & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

es conmutativo. Razonando como en el lema de los tres f, se prueba que h es un isomorfismo. Denotaremos por $\mathrm{M}(G,A)$ el conjunto de clases de equivalencia de extensiones de G por A y la clase que contiene a la extensión $0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ por $[E]$.

Ejemplo 2.40. Si G es un grupo y A es un G-módulo, la sucesión exacta corta

$$0 \to A \xrightarrow{\iota} A \rtimes G \xrightarrow{\pi} G \to 1,$$

donde $A \rtimes G$ es el producto semidirecto de A por G es una extensión de G por A. En efecto, sea $s\colon G \to A \rtimes G$ la sección de π dada por $s(x) = (0,x)$. Se tiene

$$s(x)\, i(a)\, s(x)^{-1} = (0,x)\cdot(a,\mathbf{1})\cdot(0,x^{-1}) = (x \circ a, \mathbf{1}) = i(x \circ a).$$

Proposición 2.41. *Si la extensión $0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ rompe, es decir , si existe un homomorfismo de grupos $s\colon G \to E$ tal que $p\,s = 1_G$, entonces es equivalente a la extensión $0 \to A \xrightarrow{\iota} A \rtimes G \xrightarrow{\pi} G \to 1$.*

Demostración. La aplicación $f\colon E \to A \rtimes G$ dada por $f(e) = (i^{-1}(e - sp(e)), p(e))$ es un homomorfismo de grupos que hace conmutativo el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle f} & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{\iota} & A \rtimes G & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

□

Definición 2.42. Sea G un grupo y A un G-módulo. Se dice que $f\colon G \times G \to A$ es un *factor set* de $G \times G$ en A si verifica

$$x \circ f(y,z) + f(x,yz) = f(x,y) + f(xy,z), \quad f(x,\mathbf{1}) = f(\mathbf{1},y) = 0.$$

para todo $x, y, z \in G$.

El conjunto de todos los factor sets de $G \times G$ en A es el grupo abeliano $Z^2(G, A)$ de 2.31.

Ejemplo 2.43. Dada una aplicación $g\colon G \to A$ verificando que $g(\mathbf{1}) = 0$, la aplicación $d_g\colon G \times G \to A$ dada por

$$d_g(x, y) = x \circ g(y) - g(xy) + g(x), \quad \forall\, x, y \in G,$$

es un factor set. Se tiene que $\{d_g \mid g\colon G \to A\} = D^2(G, A)$ es el grupo abeliano de 2.31; $D^2(G, A) \subset Z^2(G, A)$.

Definición 2.44. Sea E la extensión $0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ de G por A. Sea $s\colon G \to E$ una sección de p tal que $s(\mathbf{1}) = 0$. Se llama *factor set* de E asociado a s, a la aplicación $f_s\colon G \times G \to A$ dada por:

$$i(f_s(x, y)) = s(x) + s(y) - s(xy), \quad \forall x, y \in G.$$

Lema 2.45. *Se tiene que $f_s \in Z(G, A)$.*

Demostración. Se tiene que $i(f_s(x, y)) = s(x) + s(y) - s(xy)$. Dado que

$$\begin{aligned}(s(x) + s(y)) + s(z) =& i(f_s(x, y)) + s(xy) + s(z) = i(f_s(x, y) + f_s(xy, z)) + s(xyz)\\ s(x) + (s(y) + s(z)) =& s(x) + i(f_s(y, z)) + s(yz) = i(x \circ f_s(y, z)) + s(x) + s(yz)\\ =& i(x \circ f_s(y, z) + f_s(x, yz)) + s(xyz),\end{aligned}$$

por la asociatividad en E se tiene

$$x \circ f_s(y, z) + f_s(x, yz) = f_s(x, y) + f_s(xy, z).$$

Además,

$$f_s(x, \mathbf{1}) = s(x) + s(\mathbf{1}) - s(x) = 0, \quad f(\mathbf{1}, y) = s(\mathbf{1}) + s(y) - s(y) = 0.$$

□

Proposición 2.46. *Sean s y s' secciones de p tales que $s(\mathbf{1}) = s'(\mathbf{1}) = 0$ y sea $g\colon G \to A$ la aplicación dada por $i(g(x)) = s'(x) - s(x)$. Se tiene que $d_g = f_{s'} - f_s$.*

Demostración. Se tiene

$$\begin{aligned}s'(x) + s'(y) =& i(g(x)) + s(x) + i(g(y)) + s(y) = i(g(x) + x \circ g(y)) + s(x) + s(y)\\ =& i(g(x) + x \circ g(y) + f_s(x, y)) + s(xy)\\ =& i(g(x) + x \circ g(y) + f_s(x, y) - g(xy)) + s'(xy)\\ =& i(g(x) + x \circ g(y) - g(xy) + f_s(x, y)) + s'(x, y)\\ =& i(d_g(x, y) + f_s(x, y)) + s'(x, y).\end{aligned}$$

y entonces

$$i(f_{s'}(x,y)) = s'(x) + s'(y) - s'(xy) = i(d_g)(x,y) + f_s(x,y)), \quad \forall\, x,y \in G.$$

con lo cual

$$f_{s'}(x,y) = d_g(x,y) + f_s(x,y), \quad \forall\, x,y \in G. \qquad \square$$

Definición 2.47. Sea E la extensión $0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ de G por A se llama *factor set* de E a cualquier factor set de E asociado a una sección s de p tal que $s(\mathbf{1}) = 0$.

Lema 2.48. *Sea $0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ una extensión de G por A. La adición en E está dada por un factor set y por la acción de G en A.*

Demostración. Sea s una sección de p y $e \in E$. Dado que $p(e - sp(e)) = 0$ entonces existe un único $a_e \in A$ tal que $e = i(a_e) + sp(e)$. Se tiene

$$\begin{aligned} e + e' =& i(a_e) + sp(e) + i(a_{e'}) + sp(e') = i(a_e) + i(p(e) \circ a_{e'}) + sp(e) + sp(e') \\ =& i(a_e + p(e) \circ a_{e'}) + f_s(p(e), p(e')) + s(p(e)\, p(e')). \quad \square \end{aligned}$$

Lema 2.49. *Sea G un conjunto no vacío con una operación $*\colon G \times G \to G$ asociativa y que verifica*

(1) *Existe un elemento $\mathbf{1} \in G$ tal que $\mathbf{1} * x = x$, para todo $x \in G$.*

(2) *Para cada $x \in G$ existe un elemento $y \in G$ tal que $y * x = \mathbf{1}$.*

Prueba que G con la operación $\cdot$ es un grupo.

Demostración. Sea x e y tales que $x * y = \mathbf{1}$. Veamos que $y * x = \mathbf{1}$. Sea z tal que $z * x = \mathbf{1}$. Se tiene

$$z * \mathbf{1} = z\,(x * y) = (z * x) * y = \mathbf{1} * y = y,$$

y entonces

$$\mathbf{1} = z * x = z * (\mathbf{1} * x) = (z * \mathbf{1}) * x = y \cdot x.$$

Veamos que $\mathbf{1}$ es el elemento neutro, es decir que $x * \mathbf{1} = x$ para todo $x \in G$. Sea y tal que $y * x = \mathbf{1} = x * y$. Se tiene

$$x * \mathbf{1} = x * (y * x) = (x \cdot y) * x = \mathbf{1} * x = x. \qquad \square$$

Teorema 2.50. *La aplicación*

$$\Delta\colon M(G,A) \longrightarrow Z^2(G,A)/D^1(G,A)$$

dada por $\Delta(E) = [f]$, siendo f un factor set asociado a E, es biyectiva.

Demostración. La correspondencia Δ está bien definida, puesto que extensiones equivalentes tienen un mismo factor set. En efecto,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle h} & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{i'} & E' & \xrightarrow{p'} & G & \longrightarrow & 1 \end{array}$$

Si s es una sección de p tal que $s(\mathbf{1}) = 0$, entonces hs es una sección de p' y se tiene

$$i'(f_{hs}(x,y)) = hs(x)+hs(y)-hs(xy) = h(s(x)+s(y)-s(xy)) = h(if_s(x,y)) = i'(f_s(x,y)).$$

La extensión $0 \to A \xrightarrow{i} A \rtimes G \xrightarrow{p} G \to 1$, tiene la aplicación cero $0\colon G \times G \to A$, $0(x,y) = 0$, como uno de sus factor sets; en efecto, si consideramos la sección s de p dada por $s(x) = (0,x)$, entonces

$$i(f_s(x,y)) = s(x)+s(y)-s(xy) = (0,x)+(0,y)-(0,xy) = (0,xy)-(0,xy) = (0,0) = i(0).$$

Veamos que Δ es inyectiva:

Sean $0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ y $0 \to A \xrightarrow{i} E' \xrightarrow{p'} G \to 1$ extensiones con factor sets f y f', respectivamente y tales que $[f] = [f']$, es decir existe $g \in B(G,A)$ tal que $f = f' + d_g$. Sea s una sección de p tal que $s(\mathbf{1}) = 0$, $f = f_s$ y s' una sección de p' tal que $s'(\mathbf{1}) = 0$, $f' = f_{s'}$. Se tiene

$$s(x) + s(y) = i(f(x,y)) + s(xy), \quad s'(x) + s'(y) = i(f'(x,y)) + s'(xy)$$

Por el lema 2.48 si $e, e' \in E$,

$$e + e' = i(a_e + p(e) \circ a_{e'} + f(p(e), p(e')) + s(p(e)\, p(e')).$$

La aplicación $h\colon E \to E'$ dada por $h(e) = i'(a_e + g\, p(e)) + s'p(e)$ es un homomorfismo de grupos y hace conmutativo el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle h} & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{i'} & E' & \xrightarrow{p'} & G & \longrightarrow & 1 \end{array}$$

En efecto,

$$h\, i(a) = i'(a)+s'(p\, i(a)) = i'(a)+s'(\mathbf{1}) = i'(a),\ p'\, h(e) = p'(a_e+g\, p(e))+s'p(e)) = p's'p(e) = p(e).$$

Veamos que h es un homomorfismo de grupos. Se tiene

$$\begin{aligned} h(e+e') =& h(i(a_e + p(e) \circ a_{e'} + f(p(e),p(e')) + s\,p(e+e')) \\ =& i'(a_e + p(e) \circ a_{e'} + f(p(e),p(e')) + g(p(e+e') + s'\,p(e+e'). \end{aligned}$$

$$\begin{aligned} h(e)+h(e') =& i'(a_e + g\,p(e)) + s'p(e) + i'(a_{e'} + g\,p(e')) + s'p(e') \\ =& i'(a_e + g\,p(e) + p(e) \circ (a_{e'} + g\,p(e')) + f'(p(e),p(e')) + s'(p(e)\,p(e')) \\ =& i'(a_e + p(e) \circ a_{e'} + g\,p(e) + p(e) \circ g\,p(e') + f'(p(e),p(e')) + s'(p(e)\,p(e')), \end{aligned}$$

y dado que $f = f' + d_g$, entonces $h(e,e') = h(e) + h(e')$.

La aplicación Δ es sobreyectiva. En efecto, sea $f \in Z(G,A)$. Consideremos en $A \times G$ la siguiente operación:

$$(a,x) * (b,y) = (a + x \circ b + f(x,y), xy).$$

Veamos que con esta operación $A \times G$ es un grupo. La operación $*$ es asociativa:

$$\begin{aligned} ((a,x) * (b,y)) * (c,z) =& ((a + x \circ b + f(x,y), xy)) * (c,z) \\ =& (a + x \circ b + f(x,y) + xy \circ c + f(xy,z), xyz) \\ =& (a + x \circ b + xy \circ c + x \circ f(y,z) + f(x,yz), xyz) \\ =& (a,x) * ((b + y \circ c + f(y,z), yz)) \\ =& (a,x) * ((b,y) * (c,z)). \end{aligned}$$

El elemento neutro por la izquierda es $(0,\mathbf{1})$:

$$(0,\mathbf{1}) * (a,x) = (\mathbf{1} \circ a + f(\mathbf{1},x), x) = (a,x), \quad \forall\, x \in G.$$

El inverso de (a,x) por la izquierda es $(-f(x^{-1},x) - x^{-1} \circ a\,,\, x^{-1})$. En efecto,

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

Por el lema 2.49, $A \times G$ es un grupo con la operación $*$. El elemento $(0,\mathbf{1})$ es el elemento neutro de $A \times G$ y $(-f(x^{-1},x) - x^{-1} \circ a, x^{-1})$ es el inverso de (a,x).

La sucesión de grupos $0 \to A \xrightarrow{i} A \times G \xrightarrow{p} G \to 1$, donde $i(a) = (a,\mathbf{1})$ y $p(a,x) = x$, es una sucesión exacta. En efecto, $p \circ i = 0$ y si $(a,x) \in \ker p$, entonces $x = \mathbf{1}$ y se tiene

$$(a,\mathbf{1}) = i(a) \in \operatorname{im} i.$$

Para probar que es una extensión de G por A hay que ver que la estructura de G-módulo de A coincide con la dada por una sección s de p. Sea s la sección de p dada por s(x)=(0,x). Se tiene

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

puesto que

$$-x\circ f(x^{-1},x)+f(x,x^{-1})=0$$

por ser f un factor set. Falta comprobar que un factor set inducido por esta extensión es f. En efecto, consideremos la sección s de p dada por $s(x)=(0,x)$. Se tiene:

$$\begin{aligned}s(x)+s(y)-s(xy) =&(0,x)+(0,y)-(0,xy)\\ =&(f(x,y),xy)+(-f((xy)^{-1},xy),(xy)^{-1})\\ =&((f(x,y)-(xy)\circ f((xy)^{-1},xy)+f(xy,(xy)^{-1},\mathbf{1})\\ =&(f(x,y),\mathbf{1})=i(f(x,y)).\quad\square\end{aligned}$$

La aplicación biyectiva Δ induce una estructura de grupo en $M(G,A)$; el elemento neutro es la clase de la extensión $0\to A\xrightarrow{\iota} A\rtimes G\xrightarrow{\pi} G\to 1$. Con esta estructura de grupo en $M(G,A)$, Δ es un isomorfismo de grupos.

Corolario 2.51. *Se tiene el isomorfismo de grupos*

$$\Delta\, H_2(\Psi^*)\colon M(G,A)\to H^2(G,A).$$

Demostración. Se sigue del teorema 2.50 y del corolario 2.34. □

2.7. Teorema de Schur-Zassenhaus

Si G es un grupo finito, denotaremos por $|G|$ el orden del grupo G.

Lema 2.52. *Sea G un grupo finito de orden n y A un grupo abeliano de orden m. Si* m.c.d.$(m,n)=1$*, entonces toda sucesión exacta de grupos $0\to A\xrightarrow{i} E\xrightarrow{p} G\to 0$ rompe.*

Demostración. Si consideremos en A la estructura de G-módulo dada por una sección s de p, entonces $0\to A\xrightarrow{i} E\xrightarrow{p} G\to 0$ es una extensión de G por A. Por el corolario 2.36, $H^2(G,A)=0$, y por el corolario 2.51, toda extensión de G por A es equivalente

a la extensión $0 \to A \xrightarrow{\iota} A \rtimes G \xrightarrow{\pi} G \to G \to 1$. Se tiene un isomorfismo de grupos $h\colon A \rtimes G \xrightarrow{\sim} E$ que hace conmutativo el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\iota} & A \rtimes G & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \| & & \downarrow h & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \end{array}$$

La extensión $0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 0$ rompe, puesto que homomorfismo $h\,\tilde{s}\colon G \to E$ es una sección de p, siendo $\tilde{s}\colon G \to A \rtimes G,\ \tilde{s}(x) = (0, x)$. □

Si H es un grupo, denotaremos por $\mathrm{Aut}(H)$ el grupo de automorfismos de H con la operación composición.

Definición 2.53. Sean G y H dos grupos y $\sigma\colon G \to \mathrm{Aut}(H)$ un homomorfismo de grupos. Denotemos por $x \circ n$ el elemento $\sigma(x)(n)$, $n \in H$. Se llama *producto semidirecto* de H por G al conjunto producto cartesiano $H \times G$ con la siguiente operación:

$$(n_1, x_1)\,(n_2, x_2) = (n_1\,(x_1 \circ n_2), x_1\,x_2), \quad \forall\, n_1, n_2 \in H,\ \forall\, x_1, x_2 \in G.$$

Denotaremos el conjunto $H \times G$ con esta operación por $H \rtimes_\sigma G$.

Con esta definición, $H \rtimes_\sigma G$ es un grupo. El elemento neutro es el par $(\mathbf{1}, \mathbf{1})$ y el inverso de (n, x) es $(x^{-1} \circ n^{-1}, x^{-1})$. Se tiene la sucesión exacta corta rota de grupos

$$1 \to H \xrightarrow{\iota} H \rtimes_\sigma G \xrightarrow{\pi} G \to 1$$

donde $\iota(n) = (n, \mathbf{1})$ y $\pi(n, x) = x$. La aplicación $\tilde{s}\colon G \to H \rtimes_\sigma G$, $\tilde{s}(x) = (\mathbf{1}, x)$ es un homomorfismo de grupos y verifica que $\pi \circ \tilde{s} = 1_G$.

Proposición 2.54. *Si $1 \to H \xrightarrow{i} E \xrightarrow{p} G \to 1$ es una sucesión exacta corta rota de grupos y $s\colon G \to E$ es un homomorfismo de grupos tal que $p\,s = \mathrm{id}_G$, entonces los grupos E y $H \rtimes_\sigma G$ son isomorfos, siendo $\sigma\colon G \to \mathrm{Aut}(H)$ el homomorfismo de grupos dado por*

$$i(\sigma(x)(n)) = s(x)\,i(n)\,s(x^{-1}),\ x \in G,\ n \in H.$$

Demostración. La aplicación $f\colon E \to H \rtimes_\sigma G$ dada por $f(e) = (i^{-1}(e\,sp(e^{-1})), p(e))$ es un homorfismo de grupos. En efecto,

$$\begin{aligned} f(e_1)\,f(e_2) =& ((i^{-1}(e_1\,sp(e_1^{-1})),\, p(e_1))\ (i^{-1}(e_2\,sp(e_2^{-1})),\, p(e_2)) \\ =& ((i^{-1}(e_1\,sp(e_1^{-1}))\,pe_1 \circ (i^{-1}(e_2\,sp(e_2^{-1})),\, p(e_1)\,p(e_2)) \\ =& (((i^{-1}(e_1\,sp(e_1^{-1}))\,i^{-1}(sp(e_1)\,e_2\,sp(e_2^{-1})\,sp(e_1^{-1})),\, p(e_1)\,p(e_2)) \\ =& (i^{-1}(e_1\,e_2\,sp((e_1\,e_2)^{-1},\, p(e_1\,e_2)) = f(e_1\,e_2) \end{aligned}$$

Además, f es un isomorfismo de grupos. Su inverso es el homomorfismo $g\colon H \rtimes_\sigma G \to E$ dado por $g(h,x) = i(h)\,s(x)$. □

Teorema 2.55. (Teorema de Schur-Zassenhaus) *Si H es un grupo de orden m y G es un grupo de orden n y* m.c.d.$(m,n) = 1$, *entonces toda sucesión exacta corta de grupos $1 \to H \xrightarrow{i} E \xrightarrow{p} G \to 1$ rompe; equivalentemente, si H es un subgrupo normal de un grupo finito E y* m.c.d.$(|H|, |E/H|) = 1$, *entonces el grupo E es isomorfo al producto semidirecto de H por E/H.*

Demostración. Vamos a probar que si $1 \to H \xrightarrow{i} E \xrightarrow{p} G \to 1$ es una sucesión exacta de grupos, entonces rompe, es decir, existe un homomorfismo de grupos $s\colon G \to E$ tal que $s \circ p = 1_G$.

Probar que la sucesión exacta corta $1 \to H \xrightarrow{i} E \xrightarrow{p} G \to 1$ rompe, es equivalente a probar que E contiene un subgrupo de orden n. En efecto, si $s\colon G \to E$ es un homomorfismo de grupos tal que $p \circ s = 1_G$, entonces $s(G)$ es un subgrupo de E de orden n. Recíprocamente, si W es un subgrupo de E de orden n y $j\colon W \to E$ es la inclusión, la aplicación $p\,j\colon W \to G$ es un homomorfismo inyectivo. En efecto, dado que $j(\ker(p\,j)) \subset i(H)$, $|\ker(p\,j)|$ divide a n y a m y como m.c.d.$(n,m) = 1$, se tiene que $\ker(p\,j) = \{1\}$. Además, $p\,j$ es un isomorfismo, puesto que el orden de W es igual al orden de G. El homomorfismo de grupos $s = j\,(p\,j)^{-1}\colon G \to E$ verifica que $p\,s = 1_G$.

Si H es abeliano, entonces por el lema 2.52, la extensión $1 \to H \xrightarrow{i} E \xrightarrow{p} G \to 1$ rompe.

Si H no es abeliano, razonaremos por inducción sobre el orden m de H. Sea p un primo que divide a m y sea P un p-subgrupo de Sylow de E y N el normalizador de P en E, es decir

$$N = \{x \in E \,|\, x\,P\,x^{-1} = P\}.$$

Se tiene que $(E : N)$ es el número subgrupos p-Sylow de E. Veamos que todos los p-subgrupos de Sylow de E están contenidos en H. En efecto, si P' es un p-Sylow de H, entonces P' es un p-Sylow de E, puesto que el orden de E es mn y m.c.d.$(n,m) = 1$. Dado que todos los p-Sylows de E son conjugados, todo p-Sylow P'' de E es de la forma $xP'x^{-1}$ para algún $x \in E$ y entonces

$$p(P'') = p(x)\,p(P')\,p(x^{-1}) = \{\mathbf{1}\}.$$

con lo cual $P'' \subset H$.

El normalizador de P en H es $H \cap N$ y el número de p-subgrupos de Sylow de H es $(H : H \cap N) = (E : N)$. Dado que

$$(E : H)\,(H : H \cap N) = (E : N)\,(N : H \cap N),$$

se tiene que $n = (E : H) = (N : H \cap N)$. Claramente, P es un subgrupo normal de N y dado que H es un subgrupo normal de E, se tiene que $H \cap N$ es un subgrupo normal de N. Consideremos la sucesión exacta corta de grupos

$$1 \longrightarrow (H \cap N)/P \longrightarrow N/P \to N/(H \cap N) \longrightarrow 1.$$

El orden del grupo $(H \cap N)/P$ divide a m. Como $n = |N/(H \cap N)|$, por hipótesis de inducción, N/P contiene un subgrupo T/P de orden n, donde T es un subgrupo de N y P es un subgrupo normal de T.

Sea C el centro de P, es decir $C = \{x \in P \mid xy = yx, \forall\, y \in P\}$. Se tiene que C es un subgrupo normal de T. En efecto, veamos que $t\,c\,t^{-1} \in C$ para todo $t \in T$. Sea $x \in P$ y $c \in C$. Dado que P es un subgrupo normal de T, $xt = tx'$ para algún $x' \in P$ y se tiene

$$x\,t\,c\,t^{-1} = t\,x'\,c\,t^{-1} = t\,c\,x'\,t^{-1} = t\,c\,t^{-1}\,x.$$

Consideremos la sucesión exacta corta de grupos

$$1 \longrightarrow P/C \longrightarrow T/C \longrightarrow T/P \longrightarrow 1.$$

Por ser P un p-grupo, $C \neq \{1\}$ y entonces $|P/C| < |P|$. El grupo P/C es un p-grupo y p no es un divisor de $n = |T/P|$. Por hipótesis de inducción existe un subgrupo K/C de T/C, $|K/C| = n$, donde K es un subgrupo de T y C es un subgrupo normal de K. Consideremos la extensión de grupos

$$0 \longrightarrow C \longrightarrow K \longrightarrow K/C \longrightarrow 1,$$

donde $|K/C| = n$. Dado que C es un grupo abeliano, por el lema 2.52, existe un subgrupo L de K de orden n. Se tiene la cadena de subgrupos

$$L \subset K \subset T \subset N \subset E.$$

Luego, L es un subgrupo de E de orden n. □

2.8. Módulos coinducidos.

Sabemos que $H^n(G, A) = 0$, para $n \geq 1$, cuando A es un G-módulo inyectivo. Otra clase de G-módulos para los cuales la cohomología es cero es la clase de los módulos coinducidos.

Definición 2.56. Un R-módulo a la izquierda M se dice que es coinducido si existe un grupo abeliano A tal que $M \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)$.

Observación 2.57. El grupo abeliano $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)$ es un G-módulo a la izquierda con la acción $(y \circ f)(x) = f(x\,y)$, para $y \in G$, $f \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)$.

Proposición 2.58. *Todo R-módulo a la derecha es isomorfo a un submódulo de un módulo coinducido.*

Demostración. Sea A un $\mathbb{Z}G$-módulo a la izquierda y A_0 el grupo abeliano de A. La aplicación $\psi\colon A \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A_0)$, dada por $\psi(a)(x) = x\,a$, es un homomorfismo inyectivo de R-módulos. □

Proposición 2.59. *Si M es un G-módulo coinducido, entonces $H^n(G, M) = 0$, para $n \geq 0$.*

Demostración. Sea $M \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)$, con A un grupo abeliano. Se tiene

$$H^n(G, M) \cong H^n(\mathrm{Hom}_G(\mathbf{P}, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)).$$

donde $\mathbf{P}$ es una resolución proyectiva de $\mathbb{Z}$. Se tiene una equivalencia natural

$$\varphi\colon \mathrm{Hom}_G(-, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(-, A).$$

En efecto, para todo G-módulo N se tiene el isomorfismo de grupos abelianos

$$\varphi_N\colon \mathrm{Hom}_G(N, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(N, A),$$

donde $((\varphi_N(f))(n)) = f(n)(\mathbf{1})$, para $f \in \mathrm{Hom}_G(N, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A))$, $n \in N$. Su inverso φ_N^{-1} está dado por $((\varphi_N^{-1}(g))(n))(\sum_{x\in G} m_x x) = g(\sum_{x\in G} m_x x\, n)$, para $g \in \mathrm{Hom}_{\mathbb{Z}}(N, A)$, $\sum_{x\in G} m_x x \in \mathbb{Z}G$, $n \in N$. Si $h\colon N' \to N$ es un homomorfismo de G-módulos se tiene el siguiente cuadrado conmutativo de grupos abelianos

$$\begin{array}{ccc} \mathrm{Hom}_G(N, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)) & \xrightarrow{\varphi_N} & \mathrm{Hom}_{\mathbb{Z}}(N, A) \\ \Big\downarrow{\scriptstyle h^*} & & \Big\downarrow{\scriptstyle h^*} \\ \mathrm{Hom}_G(N', \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)) & \xrightarrow{\varphi_{N'}} & \mathrm{Hom}_{\mathbb{Z}}(N', A) \end{array}$$

Por tanto,

$$H^n(G, M) \cong H^n(\mathrm{Hom}_G(\mathbf{P}, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A))) \cong H^n(\mathrm{Hom}_{\mathbb{Z}}(\mathbf{P}, A)) \cong \mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z}, A) = 0. \quad \square$$

Lema 2.60. *Sea A_1 y A_2 G-módulos a la izquierda. Se tiene que* $\mathrm{Hom}_{\mathbb{Z}}(A_1, A_2)$ *es un G-módulo a la izquierda con la acción, que llamaremos* acción diagonal, *siguiente*

$$(x \circ f)(a_1) = x \circ f(x^{-1} \circ a_1), \quad x \in G,\ a_1 \in A_1.$$

Lema 2.61. *Sea A un G-módulo a la izquierda. El G-módulo* $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)$ *con la acción diagonal es un G-módulo coinducido.*

Demostración. La aplicación ψ: $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A_0)$, dada por $\psi(f)(x) = x^{-1}(f(x))$, para $f \in \mathrm{Hom}_G(\mathbb{Z}G, M)$, $x \in G$, es un isomorfismo de G-módulos. □

Teorema 2.62. (Teorema de reducción.) *Sea G un grupo y A un G-módulo. Se tiene*

$$H^n(G, A) \cong H^{n-1}(G, \mathrm{Hom}_{\mathbb{Z}}(IG, A)), \quad n \geq 2.$$

donde $\mathrm{Hom}_{\mathbb{Z}}(IG, A)$ *es un G-módulo por acción diagonal.*

Demostración. Consideremos la sucesión exacta corta de G-módulos

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(IG, A) \longrightarrow 0$$

Se tiene que $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) \cong A$ y por el lema 2.61, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)$ es un módulo coinducido. Aplicando a esta sucesión exacta de G-módulos la proposición 1.62 (5) y teniendo en cuenta la proposición 2.59, se tiene el resultado. □

Bibliografía

[1] Bourbaki H. *Algèbre Homologique* Ch. X of Algèbre, Mason Publ., Paris, 1980.

[2] Cartan, H. and Eilenberg S., *Homological Algebra*, Princenton University Press, Princenton, 1956.

[3] Hilton, P. J. and Stammbach, U. A., *A course in homological algebra*, 2nd ed., Graduate Texts in Mathematics, 4, Springer-Verlag, New York, 1997.

[4] MacLane, S. *Homology*, Springer-Verlag, New York, 1963.

[5] Rotman, J. J. *An introduction to homological algebra*, Academic Press, New York, 1979.

[6] Rotman, J. J. *An introduction to the theory of groups*, Springer-Verlag, New York, 1995.

[7] Weibel, C. A. *An introduction to homological algebra*, Cambridge University Press, New York, 1994.