INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE FÍSICA Y MATEMÁTICAS

La Cohomología de Tate y Algunas de sus Aplicaciones

T E S I S

QUE PARA OBTENER EL TÍTULO DE LICENCIADO EN FÍSICA Y MATEMÁTICAS

P R E S E N T A

RICARDO COLIN FLORES

ASESOR EXTERNO DE TESIS
DR. GABRIEL DANIEL VILLA SALVADOR

ASESOR DE TESIS
DR. PABLO LAM ESTRADA

MÉXICO, D. F. **NOVIEMBRE DE 2007**

.

A mis padres:

Baltazar y Leonides,

y a mis hermanas:

Cristina, Sandra y Hortencia.

Agradecimientos

A mis padres, hermanas y sobrinos por su apoyo incondicional.

A mis amigos por su amistad que he tenido de ellos.

A los profesores Dr. Gabriel D. Villa Salvador y Dr. Pablo Lam Estrada por el valioso apoyo que me brindaron en la realización de esta tesis.

A los integrantes del jurado: M. en C. Rubén Santos Mancio Toledo, Lic. Manuel Robles Bernal y Dra. Martha Rzedowski Calderón, por su valiosa participación en la revisión y sugerencias vertidas en esta tesis.

Al Instituto Politécnico Nacional, especialmente a la Escuela Superior de Física y Matemáticas, así como a su personal académico que fue parte de mi formación académica.

Contenido

Introducción

El objetivo de esta tesis es el de desarrollar los resultados fundamentales correspondientes a la homología y cohomología de grupos e introducir la cohomología de Tate, para que de esta última se puedan obtener algunas aplicaciones algebraicas. Para esto, se desarrollará la homología y cohomología en bajas dimensiones, así como la cohomología de Galois. Además, a través de la cohomología de Tate, abordaremos la cohomología de grupos cíclicos finitos.

La metodología aplicada a los temas abordados en esta tesis será desde el punto de vista algebraico, por lo cual se utilizarán algunas herramientas de la teoría de grupos, anillos, teoría de Galois y, sobre todo, de la teoría de módulos.

La cohomología de grupos es un tema especializado el cual tiene su desarrollo más acelerado se fundamenta en ciertas áreas de las matemáticas, como en Topología Algebraica, Teoría de Números y Geometría Algebraica, entre otras. Sus raíces provienen tanto del álgebra como de la geometría.
Podemos considerar que el lado algebraico de la teoría empezó con los trabajos de Schur (1904, 1907, 1911). Schur estudió lo que ahora se conoce como el primer y el segundo grupos de cohomología $\mathrm{H}^1(G,\, A)$ y $\mathrm{H}^2(G,\, A)$ alrededor de la Teoría de Representaciones Proyectivas de Grupos. Las ideas de Schur fueron prolíficas en la década de los años treintas y los años cuarentas del siglo veinte. Schreier en sus artículos de 1926 y Baer en 1934 trabajaron sobre la Teoría de Extensiones de Grupos y sobre la Teoría de Productos Cruzados de Álgebras, respectivamente.
El trabajo de Baer fue sumamente relevante en el desarrollo de la parte de la Teoría de Números llamada Teoría de Campos de Clases. Las bases de la teoría de campos de clases es un tema de gran interés en la teoría de números.

La forma cohomológica de la teoría de campos de clases, fue puesta de manera definitiva por Tate aproximadamente en el año 1950 usando cohomología de grupos de Galois.
Por el lado topológico, al trabajo de Hurewicz (1936) en espacios no esféricos, lo podemos considerar como la punta de lanza de esta teoría. De hecho, Hurewicz había introducido la homotopía en altas dimensiones de grupos $\pi_n X$ con $n \geq 2$ de un espacio X. Durante este tiempo se concreta el estudio de espacios X arco conexos cuyos grupos de homotopía en altas dimensiones son todos triviales, pero cuyos grupos fundamentales $\pi = \pi_1 X$ son no triviales. Estos espacios son los que se llaman esféricos.
Hurewicz probó, entre otras cosas, que el tipo de homotopía de un espacio esférico está completamente determinado por su grupo fundamental; en particular, los grupos de homología de X dependen únicamente de π. Por tanto, es razonable pensar en ellos como grupos de homología de π. Para cualquier grupo π tenemos que $\mathrm{H}_0\pi = \mathbb{Z}$ y $\mathrm{H}_1\pi = \pi_{ab}$, donde π_{ab} denota la abelianización de π, es decir π_{ab} es igual a π módulo su subgrupo conmutador. Sin embargo, para $n \geq 2$, lo anterior no es suficiente para describir $\mathrm{H}_n\pi$ algebraicamente. El primer progreso en esta ultima dirección fue hecha por Hopf en (1942) quien expresa $\mathrm{H}_2\pi$ en términos puramente algebraicos y quien dio evidencia más allá de su importancia en topología, probando el siguiente teorema:

Teorema: *Para cualquier espacio arco-conexo X con grupo fundamental π existe una sucesión exacta $\pi_2 X \to \mathrm{H}_2 X \to \mathrm{H}_2\pi \to 0$.*

Incidentalmente la descripción de Hopf de $\mathrm{H}_2\pi$, fue como sigue. Escogiendo una presentación de π como F/R, donde F es un grupo libre y R es un subgrupo normal de F, se tiene $\mathrm{H}_2\pi = R \cap [F, F]/[R, F]$, donde para $A, B \subseteq F$, $[A,\ B]$ denota el subgrupo generado por los conmutadores $[a, b] = aba^{-1}b^{-1}$, $a \in A, b \in B$.
Más o menos por la mitad de los años cuarenta del siglo pasado se tuvo una definición puramente algebraica de los grupos de homología y de cohomología. Lo anterior nos da una clara idea de que el tema fue de interés tanto para algebristas como para topólogos. Por otro lado, los grupos de cohomología en bajas dimensiones se ha visto que coinciden con grupos, que habían sido introducidos mucho antes y los cuales tienen conexión con varios problemas algebraicos.
Por ejemplo, el primer grupo de cohomología $\mathrm{H}^1(G,\ A)$ consiste de clases de

equivalencia de homomorfismos cruzados o derivaciones módulo homomorfismos cruzados principales y el segundo grupo de cohomología $\mathrm{H}^2(G,\ A)$ consiste de clases de equivalencia de conjuntos de factores de G.
Mencionamos que el presente trabajo es un estudio estrictamente algebraico de los grupos de cohomología por lo cual no se estudiará el punto de vista functorial. La construcción de los grupos de cohomología se basa en tomar un grupo abstracto G, al cual lo escribiremos multiplicativamente, y un segundo grupo A el cual es abeliano, y que escribiremos aditivamente, sobre el cual G va a actuar. Esta es la noción de **un G-módulo**.
Sea ahora una sucesión exacta de G-módulos

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

A esta sucesión le asociamos la sucesión exacta

$$0 \to \mathrm{Hom}_G(P,\ A) \xrightarrow{f^*} \mathrm{Hom}_G(P,\ B) \xrightarrow{g^*} \mathrm{Hom}_G(P,\ C) \to 0$$

donde P es un G-módulo proyectivo. Probando que el grupo $\mathrm{Hom}(A,\ B)$ tiene una estructura de G-módulo podemos demostrar ciertos teoremas importantes en relación con módulos proyectivos y sucesiones exactas que también involucran al producto tensorial y sumas directas. Otros de los resultados son los concernientes a las resoluciones proyectivas, los cuales son usados para definir los grupos de cohomología, $\mathrm{H}^n(P,\ A)$ y de homología $\mathrm{H}_n(P,\ A)$ donde P es dicha resolución y A es un G-módulo.
Por otro lado, si tenemos que A y B son dos G-módulos y $f : A \to B$ es un G-homomorfismo, se inducen de manera natural homomorfismos de grupos

$$\mathrm{H}^n(f) : \mathrm{H}^n(G,\ A) \to \mathrm{H}^n(G,\ B) \quad \text{y} \quad \mathrm{H}_n(f) : \mathrm{H}_n(G,\ A) \to \mathrm{H}_n(G,\ B)$$

lo que nos da herramientas muy poderosas para analizar la aritmética de los campos por medio de los grupos de cohomología y de homología.
Además calculamos los grupos de cohomología y de homología en dimensiones bajas, es decir, para $n = 0, 1, 2$ los cuales involucran módulos inducidos así como coinducidos. También definimos los grupos de cohomología de Tate, los cuales nos servirán para tener en un solo concepto los grupos de cohomología y de homología. Esto nos servirá para el cálculo de los grupos de cohomología de un grupo cíclico finito G. Otro concepto que veremos es el de norma de un grupo. Finalmente, tratamos algunos teoremas importantes acerca del cociente de Herbrand.

El contenido de esta tesis está conformado por cuatro capítulos. En el Capítulo 1 se desarrollan las propiedades de los G-módulos y las resoluciones proyectivas. Las resoluciones proyectivas serán parte esencial en la definición de los grupos de homología y cohomología. La homología y cohomología de grupos se abordará en el Capítulo 2; aquí se establecerán cuáles son los n-ésimos grupos de homología y cohomología, calculándose éstos en bajas dimensiones. Además, se calcularán algunos grupos de homología y cohomología, en particular para los G-módulos inducidos y coinducidos, respectivamente.
La conexión de la homología y cohomología de grupos se hará a través de la cohomología de Tate, la cual es introducida en el Capítulo 3. La aplicación de la cohomología de Tate nos permitirá calcular la cohomología de grupos cíclicos finitos. Finalmente, en el Capítulo 4 daremos algunos aplicaciones de los resultados establecidos en el Capítulo 3.

Capítulo 1

G-Módulos y Resoluciones Proyectivas

1.1 El Anillo Entero de Grupo

Definición 1.1.1. *Para un grupo G, se define* ***el anillo entero de grupo*** *por:*

$$\mathbb{Z}[G] = \left\{ \sum_{\sigma \in G} a_\sigma \sigma \mid a_\sigma \ \in \mathbb{Z} \ y \ a_\sigma = 0 \text{ para toda excepto un número finito de } \sigma \right\}$$

Las operaciones siguientes:

$$\begin{array}{ccc} \mathbb{Z}[G] \times \mathbb{Z}[G] & \longrightarrow & \mathbb{Z}[G] \\ \left(\sum_{\sigma \in G} a_\sigma \sigma, \sum_{\sigma \in G} b_\sigma \sigma \right) & \mapsto & \sum_{\sigma \in G} (a_\sigma + b_\sigma)\sigma \end{array}$$

$$\begin{array}{ccc} \mathbb{Z}[G] \times \mathbb{Z}[G] & \longrightarrow & \mathbb{Z}[G] \\ \left(\sum_{\sigma \in G} a_\sigma \sigma, \sum_{\sigma \in G} b_\sigma \sigma \right) & \mapsto & \sum_{\sigma \in G} \left(\sum_{\tau\mu = \sigma} a_\tau b_\mu \right) \sigma \end{array}$$

están bien definidas. Obsérvese que, como $a_\sigma + b_\sigma = 0$, excepto para un número finito de sigmas, se tiene que $\sum_{\sigma\in G}(a_\sigma + b_\sigma)\sigma \in \mathbb{Z}[G]$. Análogamente, la suma $\sum_{\tau\mu=\sigma} a_\tau b_\mu$ contiene solamente un número finito de sumandos $a_\tau b_\mu \in \mathbb{Z}$ diferentes de cero, por lo tanto $\sum_{\sigma\in G}\left(\sum_{\tau\mu=\sigma} a_\tau b_\mu\right)\sigma \in \mathbb{Z}[G]$.

Dicho de otra manera, podemos decir que el anillo $\mathbb{Z}[G]$ consiste en el grupo abeliano libre generado por los elementos de G como base y tal que el producto de dos está inducido por el producto de G. También, podemos concebir los elementos de $\mathbb{Z}[G]$ como funciones $u : G \to \mathbb{Z}$ que toman el valor cero para casi todo elemento de G, junto con las operaciones:

(i) $(u+v)(\sigma) = u(\sigma) + v(\sigma)$.

(ii) $(uv)(\sigma) = \sum_{\sigma=\tau\mu} u(\tau)v(\mu)$.

De hecho, si escribimos $u = \sum_{\sigma\in G} a_\sigma\sigma$, $v = \sum_{\sigma\in G} b_\sigma\sigma$, con $a_\sigma = u(\sigma)$, $b_\sigma = v(\sigma)$, $\sigma \in G$, entonces obtenemos (i) y (ii).

Proposición 1.1.1. *Para cualquier grupo G, $\mathbb{Z}[G]$ es un anillo con identidad donde el elemento identidad 1 de $\mathbb{Z}[G]$ corresponde al elemento $\sum_{\sigma\in G} a_\sigma\sigma$ con $a_e = 1$, y $a_\sigma = 0$ para toda $\sigma \neq e$. Además $\mathbb{Z}[G]$ es conmutativo $\Longleftrightarrow$ G es abeliano.*

Demostración: Es fácil verificar que $\mathbb{Z}[G]$ es un anillo con identidad 1 como está establecido en el enunciado de la proposición. Por otra parte, supongamos que G es abeliano y sean $\sum_{\sigma\in G} a_\sigma\sigma$, $\sum_{\sigma\in G} b_\sigma\sigma \in \mathbb{Z}[G]$, luego

$$\left(\sum_{\sigma\in G} a_\sigma\sigma\right)\left(\sum_{\sigma\in G} b_\sigma\sigma\right) = \sum_{\sigma\in G}\left(\sum_{\tau\mu=\sigma} a_\tau b_\mu\right)\sigma.$$

Por ser G abeliano tenemos que $\tau\mu = \sigma = \mu\tau$. Así que $\sum_{\sigma\in G}\left(\sum_{\tau\mu=\sigma} a_\tau b_\mu\right)\sigma = \sum_{\sigma\in G}\left(\sum_{\mu\tau=\sigma} b_\mu a_\tau\right)\sigma$, por tanto $\mathbb{Z}[G]$ es conmutativo.

Recíprocamente, suponga que $\mathbb{Z}[G]$ es conmutativo, es decir, para cualesquiera $\sum_{\sigma\in G} a_\sigma\sigma,\ \sum_{\sigma\in G} b_\sigma\sigma \in \mathbb{Z}[G]$, tenemos que:

$$\left(\sum_{\sigma\in G} a_\sigma\sigma\right)\left(\sum_{\sigma\in G} b_\sigma\sigma\right) = \left(\sum_{\sigma\in G} b_\sigma\sigma\right)\left(\sum_{\sigma\in G} a_\sigma\sigma\right).$$

Sean ahora $\theta, \delta \in G$, y escribámoslos como elementos de $\mathbb{Z}[G]$ de la siguiente manera, $a_\sigma = 0$ para toda $\sigma \neq \theta$ y $a_\sigma = 1$ si $\sigma = \theta$ y $b_\sigma = 0$ para toda $\sigma \neq \delta$ y $b_\sigma = 1$ si $\sigma = \delta$, luego tenemos que:

$$\theta = \sum_{\sigma\in G} a_\sigma\sigma, \quad \delta = \sum_{\sigma\in G} b_\sigma\sigma$$

pero

$$\theta\cdot\delta = \left(\sum_{\sigma\in G} a_\sigma\sigma\right)\left(\sum_{\sigma\in G} b_\sigma\sigma\right) = \left(\sum_{\sigma\in G} b_\sigma\sigma\right)\left(\sum_{\sigma\in G} a_\sigma\sigma\right) = \delta\cdot\theta$$

Por tanto G es abeliano. ■

1.2 G-módulos

Definición 1.2.1. *Sea A un grupo abeliano escrito aditivamente y sea G un grupo arbitrario escrito multiplicativamente. Decimos que A* ***es un G-módulo*** *(**izquierdo**) si existe un homomorfismo de grupos $\varphi : G \to \mathrm{Aut}(A)$, donde* Aut(A) *es el grupo de automorfismos de A.*

Esta definición es equivalente a establecer la existencia de una función $\psi : G \times A \to A$, denotada por $\psi(g, a) = g \cdot a = ga$ tal que

(*i*) $1 \cdot a = a$, para todo $a \in A$.

(*ii*) $(gh)a = g(ha)$, para todo $g, h \in G$, $a \in A$.

(*iii*) $g(a + b) = ga + gb$, para todo $g \in G$, para todo $a, b \in A$.

Notemos que si A es un G-módulo, entonces es un $\mathbb{Z}[G]$-módulo de manera natural, esto es:

$$\left(\sum_{\sigma\in G} a_\sigma\sigma\right)(x) = \sum_{\sigma\in G} a_\sigma(\sigma x) \text{ para } \sum_{\sigma\in G} a_\sigma\sigma \in \mathbb{Z}[G],\ x \in A.$$

Recíprocamente, si A es un $\mathbb{Z}[G]$-módulo, A es abeliano y consideremos la función $\varphi : G \to \mathrm{Aut}(A)$ dada de la siguiente forma.
Para $\theta \in G$, $\varphi(\theta) : A \to A$, es el automorfismo de A dado por $\varphi(\theta)a = \theta a$, donde θ es el elemento considerado en $\mathbb{Z}[G]$ expresado como:

$$\sum_{\sigma\in G} a_\sigma(\sigma), \text{ donde } a_\sigma = \begin{cases} 0 \text{ si } \sigma \neq \theta \\ 1 \text{ si } \sigma = \theta \end{cases}$$

Se tiene que $\varphi(\theta) \in \mathrm{Aut}(A)$ y que φ es un homomorfismo de grupos.

En efecto, $\varphi(\theta)$ es homomorfismo pues:

$$\varphi(\theta)(a+b) = \theta(a+b) = \theta a + \theta b = \varphi(\theta)a + \varphi(\theta)b.$$

Ahora bien, $\varphi(\theta)$ es monomorfismo ya que si $\varphi(\theta)a = \varphi(\theta)b$, entonces $\theta a = \theta b$. Puesto que $\theta \in G$, existe $\beta \in G$ tal que $\beta\theta = \theta\beta = 1$ donde 1 es la identidad de dicho grupo, luego tenemos que $\beta\theta a = \beta\theta b$, es decir, $a = 1a = 1b = b$.

Finalmente, $\varphi(\theta)$ es epimorfismo pues dado $b \in A$, existe $a := \theta^{-1}b$ tal que $\varphi(\theta)a = b$. En efecto,

$$\varphi(\theta)\theta^{-1}b = \theta(\theta^{-1}b) = 1b = b.$$

Por otro lado, $\varphi(\beta\theta)a = \beta\theta a = \beta(\theta a) = \varphi(\beta)\varphi(\theta)a$, para todo $a \in A$, es decir, $\varphi(\beta\theta) = \varphi(\beta)\varphi(\theta)$, luego φ es homomorfismo.

Así pues, tener un G-módulo es lo mismo que tener un $\mathbb{Z}[G]$-módulo.

Ejemplos

1. (**Anillo Entero de Grupo**). Si G es un grupo cíclico de orden n generado por $\sigma \in G$, entonces las potencias de σ, σ^s, $0 \leq s \leq n-1$, forman una $\mathbb{Z}$-base de $\mathbb{Z}[G]$, donde $\sigma^n = 1$. Definamos un epimorfismo $\rho : \mathbb{Z}[x] \to \mathbb{Z}[G]$, donde $\mathbb{Z}[x]$ es el anillo de polinomios con coeficientes en $\mathbb{Z}$, como sigue. Sea $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m \in \mathbb{Z}[x]$, entonces $\rho(f(x)) = a_0 + a_1\sigma + a_2\sigma^2 + \cdots + a_m\sigma^m$. Notemos que al aplicar el algoritmo de la división y el hecho de que $\sigma^n - 1 = 0$, tenemos que el núcleo de ρ es el ideal generado por el polinomio $g(x) = x^n - 1$. Ahora, por el Primer Teorema de Isomorfismo, se tiene que $\mathbb{Z}[x]/(x^n - 1) \cong \mathbb{Z}[G]$.

2. (**G-módulo**). Si A es cualquier grupo abeliano , entonces A se puede hacer un G-módulo con la acción trivial, esto es, $ga = a$ para toda $a \in A$ y toda $g \in G$. En este caso, decimos que G **actúa trivialmente sobre** A o que A **es un** G**-módulo trivial**. Que A sea un G-módulo trivial equivale, a que $\varphi : G \to \mathrm{Aut}(A)$, satisfaga que $\varphi(G) = Id$.

Definición 1.2.2. *Sean A, B G-módulos. Un G-**homomorfismo** es un homomorfismo de grupos $\varphi : A \to B$ tal que $\varphi(ga) = g\varphi(a)$, $g \in G, a \in A$.*

Notación. Para dos G-módulos A y B denotamos por:

$\mathrm{Hom}(A,\ B)$	el grupo de homomorfismos de A en B,
$\mathrm{Hom}_G(A,\ B)$	el grupo de G-homomorfismos de A en B.

Aquí $\mathrm{Hom}_G(A,\ B)$ sólo se considerará con su estructura de grupo.

Proposición 1.2.1. *El grupo* $\mathrm{Hom}\,(A,\ B)$ *tiene una estructura de G-módulo cuya acción está dada por: para cada $\varphi \in \mathrm{Hom}\,(A,\ B)$ y $g \in G$, $g \circ \varphi \in \mathrm{Hom}\,(A,\ B)$ se define por*

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

Demostración: $(1 \circ \varphi)(a) = 1\varphi(1^{-1}a) = \varphi(a)$, esto es $1 \circ \varphi = \varphi$ para toda $\varphi \in \text{Hom}\,(A,\, B)$. También,

$$\begin{aligned} g \circ (\varphi + \psi)(a) &= g \circ (\varphi + \psi)(g^{-1}a) = g(\varphi(g^{-1}a) + \psi(g^{-1}a)) \\ &= g\varphi(g^{-1}a) + g\psi(g^{-1}a), \end{aligned}$$

esto es,

$$g \circ (\varphi + \psi) = g \circ \varphi + g \circ \psi$$

para cualesquiera $g \in G$, φ, $\psi \in \text{Hom}(A,\, B)$.
Finalmente, se tiene que para cualesquiera $g, h \in G$, $\varphi \in \text{Hom}(A, B)$ y $a \in A$,

$$\begin{aligned} (g \circ h)(\varphi)(a) &= (gh)(\varphi\left((gh)^{-1}a\right)) = g \circ (\, h\,(\,\varphi\,(\,h^{-1}\,(g^{-1}a)))) \\ &= g(h \circ \varphi)(g^{-1}a) \\ &= g \circ (h \circ \varphi)(a), \end{aligned}$$

es decir, $(g \circ h)\,(\,\varphi) = g\,(\,h\,(\,\varphi))$. ■

Definición 1.2.3. *Sea A un G-módulo. Denotamos por A^G al máximo G-submódulo trivial de A, esto es, $A^G = \{a \in A \mid g \circ a = a$ para todo $g \in G\}$, el cual es llamado el G-**submódulo de A de puntos fijos**.*

Proposición 1.2.2. *Se tiene* $\text{Hom}_G(A,\, B) = (\text{Hom}\,(A,\, B))^G$. *En particular,* $\text{Hom}_G(\mathbb{Z},\, A) = (\,\text{Hom}\,(\mathbb{Z},\, A))^G \cong A^G$.

Demostración: Si $\varphi \in \text{Hom}_G(A, B)$, entonces $\varphi \in \text{Hom}(A, B)$. Ahora, para $g \in G$, $(g \circ \varphi)(a) = g \circ \varphi(g^{-1}a) = gg^{-1}\varphi(a) = \varphi(a)$.
Por tanto $g \circ \varphi = \varphi$ para $g \in G$ y, de aquí que $\varphi \in \text{Hom}(A,\, B)^G$.

Recíprocamente, si $\varphi \in \text{Hom}(A,\, B)^G$, entonces para $a \in A$ y $g \in G$ se tiene que $\varphi(ga) = (g \circ \varphi)(ga) = g\varphi(g^{-1}(ga)) = g\varphi(1a) = g\varphi(a)$, por lo tanto $\varphi \in \text{Hom}_G(A,\, B)$ y esto prueba la primera parte de la proposición.

La última parte de la proposición se sigue del hecho de que $\text{Hom}(\mathbb{Z},\, A) \cong A$ con isomorfismo de G-módulos $\theta : \text{Hom}(\mathbb{Z},\, A) \to A$, dado por $\theta(\varphi) = \varphi(1)$.
En efecto:

i) Es claro que $\varphi(1) \in A$.

ii) θ es homomorfismo pues $\theta(\psi + \zeta) = (\psi + \zeta)(1) = \psi(1) + \zeta(1) = \theta(\psi) + \theta(\zeta)$.

iii) θ es monomorfismo pues si $\theta(\varphi) = \varphi(1) = 0$ entonces para toda $n \in \mathbb{Z}$ tenemos que $\varphi(n) = \varphi(n \cdot 1) = n\varphi(1) = n \cdot 0 = 0$ por tanto $\varphi = 0$.

iv) θ es epimorfismo ya que si $x \in A$, entonces definimos $\varphi_x : \mathbb{Z} \to A$ mediante la relación $\varphi_x(m) = mx$, con $m \in \mathbb{Z}$.

Finalmente notemos que θ respeta la acción de G es decir

$$\theta(g\varphi) = (g\varphi)(1) = g\varphi(g^{-1}1) = g \circ \varphi(1) = g\theta(\varphi) \quad \blacksquare$$

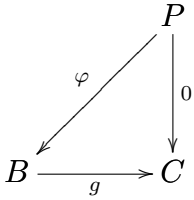
Teorema 1.2.1. *Sea* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *una sucesión exacta de* G*-módulos y sea* P *un* G*-módulo proyectivo. Entonces*

$$0 \to \mathrm{Hom}_G(P,\, A) \xrightarrow{f^*} \mathrm{Hom}_G(P,\, B) \xrightarrow{g^*} \mathrm{Hom}_G(P,\, C) \to 0$$

es una sucesión exacta de grupos, donde $f^*(\varphi) = f \circ \varphi$ *y* $g^*(\theta) = g \circ \theta$.

Demostración: Es fácil probar que f^* y g^* están bien definidas y son G-homomorfismos. Veamos que la sucesión es exacta.
Si $f^*(\varphi) = f \circ \varphi = 0$, como f es inyectiva, tenemos que $\varphi = 0$, por lo que f^* es inyectiva. Ahora, $g^* \circ f^* = (g \circ f)^* = 0^* = 0$, por lo que $\mathrm{im}(f^*) \subseteq \ker(g^*)$.

Si $\varphi \in \ker(g^*)$, $g^*(\varphi) = g \circ \varphi = 0$,



entonces $\varphi(P) \subseteq \ker(g) = \mathrm{im}(f)$, por lo que $f^{-1} \circ \varphi \in \mathrm{Hom}_G(P,\, A)$ y $f^*(f^{-1} \circ \varphi) = f \circ f^{-1} \circ \varphi = \varphi$, es decir, $\mathrm{im}(f^*) = \ker(g^*)$.
Finalmente, si $\varphi \in \mathrm{Hom}_G(P, C)$, como P es proyectivo, existe $\theta \in \mathrm{Hom}_G(P, B)$ tal que $g \circ \theta = g^*(\theta) = \varphi$, por lo tanto g^* es suprayectiva. $\blacksquare$

Nota. Si P es un G-módulo arbitrario, y $0 \to A \to B \to C$ es una sucesión G-exacta, entonces $0 \to \mathrm{Hom}_G(P, A) \to \mathrm{Hom}_G(P, B) \to \mathrm{Hom}_G(P, C)$ es exacta, como se sigue inmediatamente de la demostración anterior. De hecho, la proyectividad de P es equivalente a la exactitud de la sucesión del teorema anterior.

Teorema 1.2.2. *Sea* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *una sucesión exacta de* G*-módulos y sea* P *un* G*-módulo proyectivo. Entonces* $0 \to P \otimes A \xrightarrow{1\otimes f} P \otimes B \xrightarrow{1\otimes g} P \otimes C \to 0$ *es exacta. Aquí* $P \otimes X$ *denota al producto tensorial de los* G*-módulos* P *y* X*, esto es, para* $p \in P$, $x \in X$, $g \in G, g(p \otimes x) = gp \otimes gx$.

Demostración: Como P es proyectivo, P es sumando directo de un G-módulo libre, digamos que $P \oplus R \cong T = \bigoplus_{i\in I} \mathbb{Z}[G]$. Ahora, el producto tensorial conmuta con la suma directa y, además, para cualquier G-módulo M tenemos que $\mathbb{Z}[G] \otimes M \cong M$, por lo tanto se tiene que $(P \oplus R) \otimes M \cong (P \otimes M) \oplus (R \otimes M) \cong \bigoplus_{i\in I} M$.

Ahora bien, $f : A \to B$ es inyectiva, y la función $1_T \otimes f : T \otimes A \to T \otimes B$, está dada por $(1_T \otimes f)(e_i \otimes a) = e_i \otimes f(a)$, donde e_i es el generador de $\mathbb{Z}[G]$ de la componente i-ésima de $T = \bigoplus_{i\in I} \mathbb{Z}[G]$. De esto se sigue que $1_T \otimes f$ es inyectiva, pues f lo es. Por último, $(1_T \otimes f)|_{P\otimes A} = 1_P \otimes f$, por lo que esta última es inyectiva.

Veamos que $1_P \otimes g$ es suprayectiva. Para $p \otimes c \in P \otimes C$, existe $b \in B$ tal que $g(b) = c$, por lo que $(1_P \otimes g)(p \otimes b) = p \otimes g(b) = p \otimes c$. Ahora bien, $(1_P \otimes g)(1_P \otimes f) = 1 \otimes g \circ f = 1_P \otimes 0 = 0$, por lo que $\mathrm{im}\,(1_P \otimes f) \subseteq \ker(1_P \otimes g)$.

Sea $\varphi : (P \otimes B)/(\ker\ (1_P \otimes g)) \to P \otimes C$ el isomorfismo inducido por $(1_P \otimes g.)$ Puesto que $\mathrm{im}\,(1_P \otimes f) \subseteq \ker\ (1_P \otimes g)$, consideremos el epimorfismo inducido por φ

$$\psi : (P \otimes B)/(\mathrm{im}(1_P \otimes f)) \to P \otimes C.$$

Se tiene que $\ker(\psi) = \ker\,(1_P \otimes g)/\ \mathrm{im}\,(1_P \otimes f)$.

Sea

$$\theta : P \times C \to (P \otimes B)/(\mathrm{im}\ (1_P \otimes f))$$

dado por

$$\theta(p, c) = p \otimes b + \text{im } (1_P \otimes f),$$

para $c = g(b) \in C$. Veamos que θ está bien definida.

Si $g(b_1) = g(b_2) = c$, entonces $g(b_1 - b_2) = 0$, por lo que
$b_1 - b_2 \in \ker(g) = \text{im}(f)$, esto es, $b_1 - b_2 = f(a)$ para algún $a \in A$. Por tanto

$$p \otimes b_1 = p \otimes b_2 + p \otimes f(a),$$

con $p \otimes f(a) \in \text{im } (1_P \otimes f)$.

De aquí que

$$p \otimes b_1 \bmod (\text{ im } (1_P \otimes f)\ ) = p \otimes b_2 \bmod (\text{ im } (1_P \otimes f)\ ).$$

Así pues, θ está bien definida y claramente es G-bilineal. Entonces, existe $\overline{\theta} : P \otimes C \to (P \otimes B)/(\text{im } (1_P \otimes f))$ el G-homomorfismo inducido. Además, se tiene que $\overline{\theta} \circ \psi = \text{Id}$, $\psi \circ \overline{\theta} = \text{Id}$ por lo que ψ es un isomorfismo, probando que $\ker (1_P \otimes g) = \text{im } (1_P \otimes f)$. ■

Observación 1.2.1. En el único lugar en que usamos la proyectividad de P en el Teorema 1.2.2 fue en la inyectividad de $1_P \otimes f$. Todo módulo que satisface esta propiedad se llama **plano.**

Teorema 1.2.3. (Lema de la Serpiente) *Sea*

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

un diagrama conmutativo de G-módulos, donde las filas son exactas. Entonces, existe un homomorfismo de conexión $\delta : \ker \gamma \to \text{coker } \alpha$ tal que la sucesión

$$\ker\ \alpha \xrightarrow{\tilde{f}} \ker\ \beta \xrightarrow{\tilde{g}} \ker\ \gamma \xrightarrow{\delta} \operatorname{coker}\ \alpha \xrightarrow{\tilde{f'}} \operatorname{coker}\ \beta \xrightarrow{\tilde{g'}} \operatorname{coker}\ \gamma$$

es exacta, donde $\tilde{f}'$ *y* $\tilde{g}'$ *son los homomorfismos inducidos por* f' *y* g', *respectivamente, y* $\tilde{f}$ *y* $\tilde{g}$ *son las restricciones de* f *y* g, *respectivamente. Además, si* f *es inyectiva, entonces* $\tilde{f}$ *es inyectiva, y si* g' *es suprayectiva,* $\tilde{g'}$ *es suprayectiva.*

Demostración: Sea f inyectiva. Si $x \in \ker\alpha$, $(\beta \circ f)(x) = (f' \circ \alpha)(x) = 0$, esto es, $\tilde{f}(x) \in \ker\beta$ y, como f es inyectiva , $\tilde{f} = f_{|\ker\ \alpha} : \ker\alpha \to \ker\beta$ es inyectiva.
Ahora, si $y \in \ker\beta$, $(\gamma \circ g)(y) = (g' \circ \beta)(y) = 0$, esto es, $g(y) \in \ker\gamma$ con $y = f(x)$ para algún $x \in A$, pero además sabemos que $g \circ f = 0$, esto implica que $\operatorname{im}\tilde{f} \subseteq \ker\tilde{g}$, ya que ambas son restricciones.

Si $y \in \ker\tilde{g}$, $y = f(x)$, $x \in A$, entonces $(f' \circ \alpha)(x) = (\beta \circ f)(x) = \beta(f(x)) = \beta(y) = 0$, lo cual implica que $\alpha(x) \in \ker f' = \{0\}$. Por lo tanto $x \in \ker\alpha$, así que $\tilde{f}(x) = y$ luego $\operatorname{im}\tilde{f} = \ker\tilde{g}$ y la sucesión es exacta en $\ker\beta$.

Ahora, sea $\tilde{f'} : \operatorname{coker}\alpha = \mathrm{A}'/\operatorname{im}\alpha \to \mathrm{B}'/\operatorname{im}\beta = \operatorname{coker}\beta$ dada por:

$$\tilde{f'}(a + \operatorname{im}\alpha) = f'(a) + \operatorname{im}\beta.$$

Veamos que esta función está bien definida.

Si $a \equiv a_1 \bmod \operatorname{im}\alpha$, entonces $a - a_1 \in \operatorname{im}\alpha$, es decir $a - a_1 = \alpha(x)$, para algún $x \in A$; luego, $f'(a - a_1) = (f'\alpha)(x) = \beta(f(x)) \in \operatorname{im}\beta$, es decir, $\tilde{f'}$ está bien definida.

Sea, ahora, $\tilde{g'} : \operatorname{coker}\beta = B'/\operatorname{im}\beta \to C'/\operatorname{im}\gamma = \operatorname{coker}\gamma$ dada por:

$$\tilde{g'}(b + \operatorname{im}\beta) = g'(b) + \operatorname{im}\gamma.$$

Veamos que la función está bien definida.

Si $b \equiv b_1 \bmod \operatorname{im}\beta$, entonces $b - b_1 \in \operatorname{im}\beta$, es decir $b - b_1 = \beta(y)$, $y \in B$; así $(\tilde{g} \circ \beta)(y) = \gamma(g(y)) \in \operatorname{im}\gamma$, es decir, $\tilde{g'}$ está bien definida.

Puesto que $g' \circ f' = 0$, se tiene que $\tilde{g'} \circ \tilde{f'} = 0$, de donde im $\tilde{f'} \subseteq \ker \tilde{g'}$. Sea, ahora, $z + \operatorname{im}\beta \in \ker \tilde{g'}$, $\tilde{g'}(z + \operatorname{im}\beta) = g'(z) + \operatorname{im}\gamma = 0$, es decir $g'(z) = \gamma(t)$, $t \in C$. Sea $t = g(u)$, $u \in B$, luego $g'(z) = (\gamma \circ g)(u) = g'(\beta(u))$ con lo cual $g'(z - \beta(u)) = 0$, de aquí que $z - \beta(u) \in \ker g' = \operatorname{im} f'$. Sea $z - \beta(u) = f'(x)$, $x \in A'$. Entonces $f'(x) + \operatorname{im}\beta = z - \beta(u) + \operatorname{im}\beta = z + \operatorname{im}\beta = f'(x + \operatorname{im}\alpha)$. Por lo tanto im $\tilde{f'} = \ker \tilde{g'}$ y la sucesión es exacta en coker β.

Ahora si g' es suprayectiva, veamos que $\tilde{g'}$ es suprayectiva.

Sea $c + \operatorname{im}\gamma \in \operatorname{coker}\gamma$, y sea $b \in B$ tal que $g(b) = c$. Entonces, $\tilde{g'}(b + \operatorname{im}\beta) = g'(b) + \operatorname{im}\gamma = c + \operatorname{im}\gamma$.

Resta definir δ: $\ker\gamma \to \operatorname{coker}\alpha$ y probar que $\operatorname{im}\tilde{g} = \ker\delta$, $\operatorname{im}\delta = \ker\tilde{f'}$. Para esto, sea $z \in \ker\gamma$ con $z = g(y)$, $y \in B$. Entonces, $\gamma(z) = \gamma(g(y)) = g'\beta(y) = 0$. Por tanto se tiene que $\beta(y) \in \ker g' = \operatorname{im} f'$, esto es, $\beta(y) = f'(a)$, $a \in A'$. Sea $\delta(z) = a + \operatorname{im}\alpha$. Veamos que δ está bien definida. Si $z = g(y) = g(y_1)$, entonces $z = g(y - y_1) = 0$, es decir, $y - y_1 \in \ker g = \operatorname{im} f$, por tanto $y = y_1 + f(x)$, con $x \in A$. Ahora $\beta(y_1) = f'(a_1)$, por tanto

$$\beta(y) = f'(a) = \beta(y_1) + \beta(f(x)) = f'(a_1) + \beta(f(x)) = f'(a_1) + f'(\alpha(x)).$$

Como f' es inyectiva, tendremos que $a = a_1 + \alpha(x)$, por lo que $a + \operatorname{im}\alpha = a_1 + \operatorname{im}\alpha$.

Claramente δ es un G-homomorfismo.

Si $z \in \ker\gamma$, $z \in \operatorname{im}\tilde{g}$, entonces $g(y) = z$, $y \in \ker\beta$. Luego, $\beta(y) = 0 = f'(0)$, esto es, $(\delta\tilde{g})(y) = \delta(z) = 0 + \operatorname{im}\alpha$, por lo tanto $\operatorname{im}\tilde{g} \subseteq \ker\delta$. Si $z \in \ker\delta$, esto es, $\delta(z) = 0$, tenemos que $z = g(y)$, $y \in B$, $\beta(y) = f'(x)$, $x \in \operatorname{im}\alpha$, o sea, $x = \alpha(a)$, $a \in A$ y $\beta(y) = (f'\alpha)(a) = \beta(f(a))$, por tanto $\beta(y - f(a)) = 0$, es decir, $y - f(a) \in \ker\beta$ y $\tilde{g}(y - f(a)) = g(y) - (gf)(a) = g(y) = z$. Por lo que la sucesión es exacta en $\ker\gamma$.

Finalmente, $(\tilde{f'} \circ \delta)(z) = \tilde{f'}(a + \operatorname{im}\alpha) = f'(a) + \operatorname{im}\beta$, donde $z = g(y)$, $\beta(y) = f'(a)$. Por tanto $(\tilde{f'} \circ \delta)(z) = \beta(y) + \operatorname{im}\beta = 0$, esto es, $\operatorname{im}\delta \subseteq \ker\tilde{f'}$. Si $a + \operatorname{im}\alpha \in \ker\tilde{f'}$, $f'(a) \in \operatorname{im}\beta$, es decir, $f'(a) = \beta(y)$, entonces $z = g(y)$, y $\delta(z) = a + \operatorname{im}\alpha$. Por tanto, la sucesión es exacta en $\operatorname{coker}\alpha$. ■

1.3 Resoluciones Proyectivas

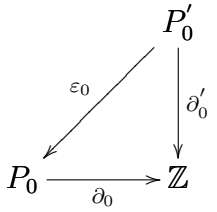
Definición 1.3.1. *Una* ***resolución proyectiva*** P *de* $\mathbb{Z}$ *es una sucesión exacta de* G*-módulos*

$P:\qquad \cdots \to P_n \xrightarrow{\partial_n} P_{n-1} \to \cdots \to P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathbb{Z} \to 0$

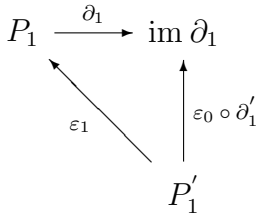
donde $\mathbb{Z}$ *es el* G*-módulo trivial y cada* P_i *es proyectivo. En particular,* $\partial_n \circ \partial_{n+1} = 0$ *para toda* n*.*

Proposición 1.3.1. *Si* P, P' *son dos resoluciones proyectivas de* $\mathbb{Z}$*, entonces existen* $\varepsilon_i : P_i' \to P_i$ *tales que* $\partial_i \circ \varepsilon_i = \varepsilon_{i-1} \circ \partial_i'$*, para todo* i*, donde* $\varepsilon_{-1} = \mathrm{Id}_{\mathbb{Z}}$*.*

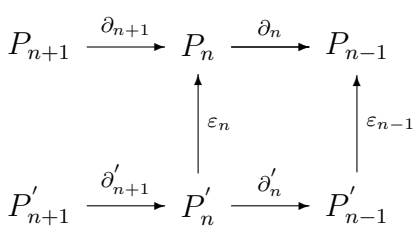
Demostración: Se hará la demostración por inducción. Sea $\varepsilon_{-1} = \mathrm{Id}_{\mathbb{Z}}$. Como P_0' es proyectivo, existe $\varepsilon_0 : P_0' \to P_0$ tal que $\partial_0' = \partial_0 \circ \varepsilon_0 = \mathrm{Id}_{\mathbb{Z}} \circ \partial_0' = \varepsilon_{-1} \circ \partial_0'$, como se puede observar del diagrama

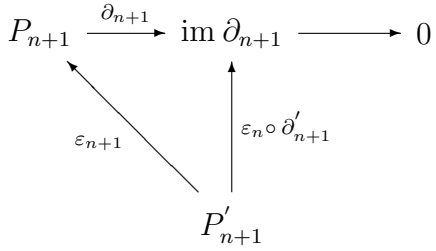


Veamos como se construye ε_1. Sea $x \in P_1'$. Tenemos que $(\varepsilon_0 \circ \partial_1')(x) \in P_0$, puesto que $\partial_0 \circ (\varepsilon_0 \circ \partial_1')(x) = (\partial_0 \circ \varepsilon_0) \circ \partial_1'(x) = \varepsilon_{-1} \circ (\partial_0' \circ \partial_1')(x) = 0$. Luego, se tiene que $(\varepsilon_0 \circ \partial_1')(P_1') \subseteq \ker \partial_0 = \operatorname{im} \partial_1$ y, como P_1' es proyectivo, tenemos que existe $\varepsilon_1 : P_1' \to P_1$ tal que $\partial_1 \circ \varepsilon_1 = \varepsilon_0 \circ \partial_1'$.



Supongamos construidos $\varepsilon_0, \varepsilon_1, ..., \varepsilon_n$ tales que los $\varepsilon_i : P_i' \to P_i$ satisfacen $\partial_i \circ \varepsilon_i = \varepsilon_{i-1} \circ \partial_i'$, $i = 0, 1, ..., n$.





Sea $x \in P'_{n+1}$, $(\varepsilon_n \circ \partial'_{n+1})(x) \in P_n$. Puesto que

$$\partial_n \circ (\varepsilon_n \circ \partial'_{n+1})(x) = (\partial_n \circ \varepsilon_n) \circ \partial'_{n+1}(x) = \varepsilon_{n-1} \circ (\partial'_n \circ \partial'_{n+1})(x) = 0,$$

se tiene que $(\varepsilon_n \circ \partial'_{n+1})(P'_{n+1}) \subseteq \ker \partial_n = \operatorname{im} \partial_{n+1}$ y, como P'_{n+1} es proyectivo, tenemos que existe $\varepsilon_{n+1} : P'_{n+1} \to P_{n+1}$ tal que $\partial_{n+1} \circ \varepsilon_{n+1} = \varepsilon_n \circ \partial'_{n+1}$. ■

Capítulo 2

Cohomología de Grupos

2.1 El n-ésimo Grupo de Cohomología

Sea $P: \quad \cdots \to P_n \xrightarrow{\partial_n} P_{n-1} \to \cdots \to P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathbb{Z} \to 0$ una resolución proyectiva sobre $\mathbb{Z}$ de G-módulos proyectivos P_i. Sea $K_i = \mathrm{Hom}_G(P_i,\ A)$ y $R_i = P_i \otimes_G A = P_i \otimes_{\mathbb{Z}[G]} A$, donde P_i se hace G-módulo derecho con la acción: $x \circ g = g^{-1}x,\ g \in G,\ x \in P_i$. Entonces, se tienen las sucesiones

$$0 \to K_0 \xrightarrow{\partial_1^*} K_1 \xrightarrow{\partial_2^*} \cdots \to K_{n-1} \xrightarrow{\partial_n^*} K_n \to \cdots$$

$$\cdots \to R_n \xrightarrow{\partial_n^+} R_{n-1} \to \cdots \to R_1 \xrightarrow{\partial_1^+} R_0 \to 0$$

donde $\partial_n^*(\varphi) = \varphi \circ \partial_n,\ \partial_n^+(x \otimes a) = \partial_n x \otimes a$. Además,

$$\partial_{n+1}^* \circ \partial_n^* = (\partial_n \circ \partial_{n+1})^* = 0^* = 0$$

y

$$\partial_n^+ \circ \partial_{n+1}^+ = (\partial_n \circ \partial_{n+1})^+ = 0^+ = 0,$$

esto es, $\mathrm{im}\,\partial_n^* \subseteq \ker \partial_{n+1}^*$ e $\mathrm{im}\,\partial_{n+1}^+ \subseteq \ker \partial_n^+$.

Definición 2.1.1. *Se define el* n***-ésimo grupo de cohomología de*** A ***con respecto a*** P*, para* $n = 0, 1, \ldots,$ *como el grupo*

$$\mathrm{H}^n(P,\ A) = \ker\ \partial^*_{n+1}/\ \mathrm{im}\ \partial^*_n,$$

y el n***-ésimo grupo de homología con respecto a*** P *por*

$$\mathrm{H}_n(P,\ A) = \ \ker \partial^+_n /\ \mathrm{im}\ \ \partial^+_{n+1}.$$

Aquí se define $\partial^*_0 = 0;\ \ \partial^+_0 = 0.$

Teorema 2.1.1. *Si* P *y* $P^{'}$ *son dos resoluciones proyectivas de* $\mathbb{Z}$*, entonces*

$$\mathrm{H}^n(P,\ A) \cong \mathrm{H}^n(P^{'},\ A)$$

y

$$\mathrm{H}_n(P,\ A) \cong \mathrm{H}_n(P^{'},\ A)$$

para todo $n = 0, 1, ...$

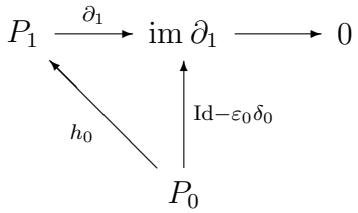
Demostración: Sean $\varepsilon_n : P^{'}_n \to P_n$ y $\delta_n : P_n \to P^{'}_n$ dadas en la Proposición 1.3.1, esto es, $\partial_n \circ \varepsilon_n = \varepsilon_{n-1} \circ \partial^{'}_n$, $\partial^{'}_n \circ \delta_n = \delta_{n-1} \circ \partial_n$. Se construirán homomorfismos $h_n : P_n \to P_{n+1}$ tales que

$$\partial_{n+1}h_n + h_{n-1}\partial_n = \ \mathrm{Id}\ - \varepsilon_{\mathrm{n}}\delta_{\mathrm{n}} \tag{2.1}$$

y, similarmente, homomorfismos $f_n : P^{'}_n \to P^{'}_{n+1}$ tales que

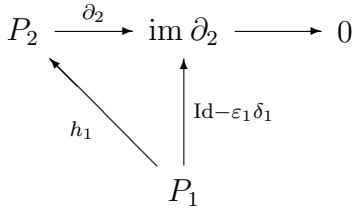
$$\partial^{'}_{n+1}f_n + f_{n-1}\partial^{'}_n = \ \mathrm{Id}\ - \delta_{\mathrm{n}}\varepsilon_{\mathrm{n}} \tag{2.2}$$

Sea $h_{-1} : \mathbb{Z} \to P_0,\ \ h_{-1} = 0$. Ahora se quiere $h_0 : P_0 \to P_1$ tal que $\partial_1 h_0 + h_{-1}\partial_0 = \partial_1 h_0 = \ \mathrm{Id}\ - \varepsilon_0\delta_0$, como se muestra en el siguiente diagrama:



Si $x \in P_0$, $\partial_0(\mathrm{Id}-\varepsilon_0\delta_0)(x) = \partial_0(x)-\partial_0\varepsilon_0\delta_0(x) = \partial_0(x)-\varepsilon_{-1}\partial_0'\delta_0(x) = \partial_0(x)-\delta_{-1}\partial_0(x) = \partial_0(x)-\partial_0(x) = 0$, por lo tanto $(\mathrm{Id}-\varepsilon_0\delta_0)(x) \in \ker\ \partial_0 = \mathrm{im}\ \partial_1$. Como P_0 es proyectivo, existe $h_0 : P_0 \to P_1$ tal que $\partial_1 \circ h_0 = \mathrm{Id} - \varepsilon_0\delta_0$.

Ahora, construiremos h_1, es decir, se quiere $h_1 : P_1 \to P_2$ tal que $\partial_2 h_1 + h_0\partial_1 = \mathrm{Id} - \varepsilon_1\delta_1$, como lo muestra el siguiente diagrama:

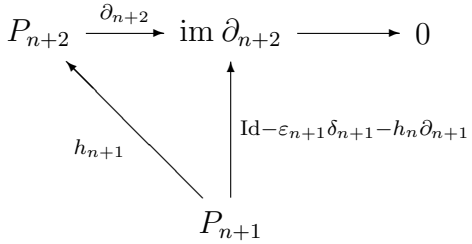


Si $x \in P_1$, entonces

$$\begin{aligned}
\partial_1(\mathrm{Id} - \varepsilon_1\delta_1 - h_0\partial_1)(x) &= \partial_1(x) - \partial_1\varepsilon_1\delta_1(x) - \partial_1 h_0\partial_1(x) \\
&= \partial_1(x) - \varepsilon_0\partial_1'\delta_1(x) - \partial_1 h_0\partial_1(x) \\
&= \partial_1(x) - \varepsilon_0\delta_0\partial_1(x) - \partial_1 h_0\partial_1(x) \\
&= (\mathrm{Id} - \varepsilon_0\delta_0)\partial_1(x) - \partial_1 h_0\partial_1(x) \\
&= (\partial_1 h_0 + h_{-1}\partial_0)\partial_1(x) - \partial_1 h_0\partial_1(x) \\
&= \partial_1 h_0\partial_1(x) + h_{-1}\partial_0\partial_1(x) - \partial_1 h_0\partial_1(x) \\
&= \partial_1 h_0\partial_1(x) - \partial_1 h_0\partial_1(x) \\
&= 0.
\end{aligned}$$

Por tanto, $(\mathrm{Id} - \varepsilon_1\delta_1 - h_0\partial_1)(x) \in \ker\ \partial_1 = \ \mathrm{im}\ \partial_2$. Como P_1 es proyectivo, existe $h_1 : P_1 \to P_2$ tal que $\partial_2 h_1 + h_0\partial_1 = \ \mathrm{Id} - \varepsilon_1\delta_1$.

Supongamos ahora construidos, $h_0, h_1, \ldots, h_n$ con la propiedad (2.1). Tenemos el diagrama:



Si $x \in P_{n+1}$, entonces tenemos

$$\begin{aligned}
\partial_{n+1}(\mathrm{Id} - \varepsilon_{n+1}\delta_{n+1} - h_n\partial_{n+1})(x) &= \partial_{n+1}(x) - \partial_{n+1}\varepsilon_{n+1}\delta_{n+1}(x) \\
&\quad -\partial_{n+1}h_n\partial_{n+1}(x) \\
&= \partial_{n+1}(x) - \varepsilon_n\partial'_{n+1}\delta_{n+1}(x) \\
&\quad -\partial_{n+1}h_n\partial_{n+1}(x) \\
&= \partial_{n+1}(x) - \varepsilon_n\delta_n\partial_{n+1}(x) \\
&\quad -\partial_{n+1}h_n\partial_{n+1}(x) \\
&= (\mathrm{Id} - \varepsilon_n\delta_n)(\partial_{n+1}(x)) - \partial_{n+1}h_n\partial_{n+1}(x) \\
&= (\partial_{n+1}h_n + h_{n-1}\partial_n)\partial_{n+1}(x) \\
&\quad -\partial_{n+1}h_n\partial_{n+1}(x) \\
&= \partial_{n+1}h_n\partial_{n+1}(x) + h_{n-1}\partial_n\partial_{n+1}(x) \\
&\quad -\partial_{n+1}h_n\partial_{n+1}(x) \\
&= \partial_{n+1}h_n\partial_{n+1}(x) - \partial_{n+1}h_n\partial_{n+1}(x) \\
&= 0.
\end{aligned}$$

Por tanto, $(\mathrm{Id} - \varepsilon_{n+1}\delta_{n+1} - h_n\partial_{n+1})(x) \in \ker\partial_{n+1} = \mathrm{im}\,\partial_{n+2}$. Como P_{n+1} es proyectivo, existe $h_{n+1} : P_{n+1} \to P_{n+2}$ tal que $\partial_{n+2}h_{n+1} = \mathrm{Id} - \varepsilon_{n+1}\delta_{n+1} - h_n\partial_{n+1}$.

Similarmente, para la contrucción de las $f_n : P'_n \to P'_{n+1}$, procedamos como sigue.
Para $\varepsilon_n : P'_n \to P_n$, sea $\varepsilon_n^* : \mathrm{Hom}_G(P_n, A) \to \mathrm{Hom}_G(P'_n, A)$ y $\varepsilon_n^+ = \varepsilon_n \otimes \mathrm{Id}_A : P'_n \otimes A \to P_n \otimes A$ dadas por $\varepsilon_n^*(\varphi) = \varphi \circ \varepsilon_n$ y $\varepsilon_n^+(x \otimes a) = \varepsilon_n(x) \otimes a$, respectivamente.
Por otro lado, si $\varphi \in \ker\partial_{n+1}^*$,

$$\partial'^*_{n+1}(\varepsilon_n^*(\varphi)) = \varphi \circ \varepsilon_n \circ \partial'_{n+1} = \varphi \circ \partial_{n+1} \circ \varepsilon_{n+1} = \varepsilon_{n+1}^*(\partial_{n+1}^* \circ \varphi) = 0,$$

es decir, $\varepsilon_n^*(\ker\partial_{n+1}^*) \subseteq \ker\partial'^*_{n+1}$. Pero también, $\varepsilon_n^*(\mathrm{im}\,\partial_n^*) \subseteq \mathrm{im}\,\partial'^*_n$; $\varepsilon_n^+(\ker\partial'^+_n) \subseteq \ker\partial_n^+$; $\varepsilon_n^+(\mathrm{im}\,\partial'^+_{n+1}) \subseteq \mathrm{im}\,\partial_{n+1}^+$, pues si $\theta \in \mathrm{im}\,\partial_n^*$, entonces

$$\varepsilon_n^*(\partial_n^*(\theta)) = \varepsilon_n^*(\theta \circ \partial_n) = \theta \circ \partial_n \circ \varepsilon_n = \theta \circ \varepsilon_{n-1} \circ \partial'_n = \partial'^*_n(\varepsilon_{n-1}^*(\theta))$$

es decir, $\varepsilon_n^*(\mathrm{im}\,\partial_n^*) \subseteq \mathrm{im}\,\partial'^*_n$.

Ahora, sea $x \otimes a \in \ker {\partial'}_n^+$, tenemos que

$$\begin{aligned} \partial_n^+(\varepsilon_n^+(x \otimes a)) &= \partial_n^+(\varepsilon_n(x) \otimes a) = \partial_n \circ \ \varepsilon_n(x) \otimes a \\ &= \varepsilon_{n-1} \circ \ \partial_n'(x) \otimes a = \varepsilon_{n-1}^*({\partial'}_n^+(x \otimes a)) \\ &= 0, \end{aligned}$$

es decir, $\varepsilon_n^+(\ker {\partial'}_n^+) \subseteq \ker \partial_n^+$.

Finalmente, sea $y \otimes a \in \operatorname{im} {\partial'}_{n+1}^+$, entonces existe $x \otimes a \in P'_{n+1} \otimes_{\mathbb{Z}[G]} A$ tal que ${\partial'}_{n+1}^+(x \otimes a) = y \otimes a$, pero ${\partial'}_{n+1}^+(x \otimes a) = \partial'_{n+1}(x) \otimes a$, luego

$$\begin{aligned} \varepsilon_n^+(y \otimes a) &= \varepsilon_n^+({\partial'}_{n+1}^+(x \otimes a)) = \varepsilon_n^+(\partial'_{n+1}(x) \otimes a) \\ &= \varepsilon_n \circ \partial'_{n+1}((x) \otimes a) = \partial_{n+1} \circ \varepsilon_{n+1}((x) \otimes a) \\ &= \partial_{n+1}^+(\varepsilon_{n+1}((x) \otimes a), \end{aligned}$$

es decir $\varepsilon_n^+(\operatorname{im} {\partial'}_{n+1}^+) \subseteq \operatorname{im} \partial_{n+1}^+$.
Por lo tanto, tenemos homomorfismos inducidos:

$$\tilde{\varepsilon}_n^* : \mathrm{H}^n(P,\ A) \to \mathrm{H}^n(P',\ A)\ ,\ \tilde{\varepsilon}_n^+ : \mathrm{H}_n(P',\ A) \to \mathrm{H}_n(P,\ A).$$

Similarmente tenemos homomorfismos inducidos para $\tilde{\delta}_n^*$ y $\tilde{\delta}_n^+$.
Ahora, si $\varphi \in \ker \partial_{n+1}^*$, $(\partial_{n+1}h_n + h_{n-1}\partial_n)^*\ \varphi = \varphi\partial_{n+1}h_n + \varphi h_{n-1}\partial_n = \underline{0 + \varphi h_{n-1}\partial_n} = \partial_n^*(\varphi h_{n-1}) \in \operatorname{im} \partial_n^*$, por lo tanto $\overline{(\partial_{n+1}h_n + h_{n-1}\partial_n)^*} = 0 = \overline{(\ \mathrm{Id}\ - \varepsilon_n\delta_n)^*}$.
Por otro lado, si $\varphi \in \mathrm{Hom}_G(P_{n+1},\ A)$ tenemos que:

$$\begin{aligned} \overline{(\ \mathrm{Id}\ - \varepsilon_n\delta_n)^*}(\varphi) &= \overline{\varphi \circ\ \mathrm{Id}\ - \varphi \circ \varepsilon_n \circ \delta_n} \\ &= (\varphi \circ\ \mathrm{Id}\ - \varphi \circ \varepsilon_n \circ \delta_n) + \operatorname{im} {\partial'}_n^* \\ &= (\varphi \circ\ \mathrm{Id}\ + \operatorname{im} {\partial'}_n^*) - (\varphi \circ \varepsilon_n \circ \delta_n + \operatorname{im} {\partial'}_n^*) \\ &= \overline{\varphi \circ\ \mathrm{Id}} - \overline{\varphi \circ \varepsilon_n \circ \delta_n} \\ &= \overline{\mathrm{Id}^*}(\varphi) - \overline{(\varepsilon_n\delta_n)^*}(\varphi) \\ &= (\overline{\mathrm{Id}^*} - \overline{(\varepsilon_n\delta_n)^*})(\varphi), \end{aligned}$$

de donde $\overline{\mathrm{Id}^*} = \mathrm{Id} = \bar{\delta}_n^* \bar{\varepsilon}_n^*$. Similarmente se tiene $\mathrm{Id} = \bar{\varepsilon}_n^* \bar{\delta}_n^*$.
Análogamente $\bar{\varepsilon}_n^+ \bar{\delta}_n^+ = \mathrm{Id}$, $\bar{\delta}_n^+ \bar{\varepsilon}_n^+ = \mathrm{Id}$. ■

Definición 2.1.2. *Para un G-módulo A y $n = 0, 1, \ldots$, se definen los grupos de cohomología $\mathrm{H}^n(G, A)$ por $\mathrm{H}^n(P, A)$, y los grupos de homología $\mathrm{H}_n(G, A)$ por $\mathrm{H}_n(P, A)$, donde P es cualquier resolución proyectiva de $\mathbb{Z}$.*

Debido al Teorema 2.1.1, la definición anterior sólo depende de G y de A y no de la resolución. Por otro lado, para ver que en la Definición 2.1.2 los grupos de cohomología y homología se pueden construir, debemos dar al menos una resolución proyectiva de $\mathbb{Z}$.

Sea $G^{n+1} = G \times \cdots \times G$ ($n+1$ copias), y sea $A_n = \mathbb{Z}[G^{n+1}]$ el anillo de grupo. Entonces, A_n es un grupo abeliano y G actúa en A_n como sigue:

$$x \circ (g_0, \ldots, g_n) = (xg_0, \ldots, xg_n),$$

para $x \in G$, y $(g_0, \ldots, g_n) \in G^{n+1}$. Además, A_n es un $\mathbb{Z}-$módulo libre con base $\{(g_0, \ldots, g_n) \mid g_i \in G\}$.

Proposición 2.1.1. *Para $n \geq 0$, A_n es un $\mathbb{Z}[G]$-módulo libre con base $\{(1, x_1, \ldots, x_n) \mid x_i \in G\}$.*

Demostración: Sea $x \in A_n$. Entonces,

$$\begin{aligned} x &= \sum_{(g_0,\ldots,g_n) \in G^{n+1}} a_{(g_0,\ldots,g_n)}(g_0, \ldots, g_n) \\ &= \sum_{(g_0,\ldots,g_n) \in G^{n+1}} a_{(g_0,\ldots,g_n)} g_0 (1, g_0^{-1}g_1, \ldots, g_0^{-1}g_n) \\ &= \sum_{(g_1,\ldots,g_n) \in G^{n}} \left(\sum_{g_0 \in G} a_{(g_0,\ldots,g_n)} g_0 \right) (1, g_0^{-1}g_1, \ldots, g_0^{-1}g_n), \end{aligned}$$

es decir, $\{(1, g_0^{-1}g_1, \ldots, g_0^{-1}g_n) \mid g_i \in G\} = \{(1, x_1, \ldots, x_n) \mid x_i \in G\}$ generan A_n como un $\mathbb{Z}[G]$-módulo.

Sean $\alpha_{(x_1,\ldots,x_n)} \in \mathbb{Z}[G]$, $\alpha_{(x_1,\ldots,x_n)} = \sum_{x_0\in G} \alpha_{(x_0,x_1,\ldots,x_n)}x_0$, $\alpha_{(x_0,x_1,\ldots,x_n)}x_0 \in \mathbb{Z}$ tales que $\sum_{(x_1,\ldots,x_n)\in G^n} \alpha_{(x_1,\ldots,x_n)}(1,x_1,\ldots,x_n) = 0$. Entonces, se tiene:

$$\begin{aligned}
&\sum_{(x_1,\ldots,x_n)\in G^n} \alpha_{(x_1,\ldots,x_n)}(1,x_1,\ldots,x_n) \\
&\quad = \sum_{(x_1,\ldots,x_n)\in G^n} \left(\sum_{x_0\in G} \alpha_{(x_0,x_1,\ldots,x_n)}x_0\right)(1,x_1,\ldots,x_n) \\
&\quad = \sum_{(x_0,\ldots,x_n)\in G^{n+1}} \alpha_{(x_0,x_1,\ldots,x_n)}(x_0,x_0x_1,\ldots,x_0x_n) \\
&\quad = \sum_{(y_0,\ldots,y_n)\in G^{n+1}} \alpha_{(y_0,y_1,\ldots,y_n)}(y_0,y_1,\ldots,y_n) \\
&\quad = 0,
\end{aligned}$$

con $y_0 = x_0$, $y_i = x_0x_i$, $1 \leq i \leq n$; $\alpha_{(y_0,\ldots,y_n)} = \alpha_{(x_0,\ldots,x_n)}$. Como A_n es el $\mathbb{Z}$-módulo libre generado por $(y_0,y_1,\ldots,y_n) \in G^{n+1}$, $\alpha_{(y_0,\ldots,y_n)} = 0$ para todo $(y_0,y_1,\ldots,y_n) \in G^{n+1}$ y, por tanto, $\alpha_{(x_0,\ldots,x_n)} = 0$, probando lo afirmado. ■

Ahora escribamos $P_i = A_i$ y sea $\partial_n : P_n \to P_{n-1}$ dada por:

$$\partial_n(g_0,g_1,\ldots,g_n) = \sum_{i=0}^{n}(-1)^i(g_0,g_1,\ldots,\hat{g}_i,\ldots,g_n),$$

donde el símbolo $\hat{g}_i$ significa que el elemento g_i no aparece, esto es,

$$(g_0,g_1,\ldots,\hat{g}_i,\ldots,g_n) = (g_0,g_1,\ldots,g_{i-1},g_{i+1},\ldots,g_n).$$

Si $g \in G$, entonces

$$\begin{aligned}
g\circ(\partial_n(g_0,g_1,...,g_n)) &= g\circ\sum_{i=0}^{n}(-1)^i(g_0,g_1,\ldots,\hat{g}_i,\ldots,g_n) \\
&= \sum_{i=0}^{n}(-1)^i(gg_0,gg_1,\ldots,\widehat{gg_i},\ldots,gg_n) \\
&= \partial_n(gg_0,gg_1,\ldots,gg_n) \\
&= \partial_n(g\circ(g_0,g_1,\ldots,g_n)),
\end{aligned}$$

esto es, ∂_n es un G-homomorfismo.

Ahora, $\partial_0 : P_0 = A_0 = \mathbb{Z}[G] \to \mathbb{Z}$ está dada por $\partial_0(g) = 1$ para toda $g \in G$.

Proposición 2.1.2. *La sucesión de G-módulos*

$$\cdots \to P_n \xrightarrow{\partial_n} P_{n-1} \to \cdots \to P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathbb{Z} \to 0$$

es G-exacta.

Demostración: Para $n = 0, 1, \ldots$ se tiene

$$\partial_{n-1} \circ \partial_n(g_0, g_1, \ldots, g_n) = \partial_{n-1}\left(\sum_{i=0}^{n}(-1)^i(g_0, g_1, \ldots, \hat{g}_i, \ldots, g_n)\right)$$

$$= \sum_{i=0}^{n}(-1)^i\left(\sum_{j=0}^{i-1}(-1)^j(g_0, g_1, \ldots, \hat{g}_j, \ldots, \hat{g}_i, \ldots, g_n) + \sum_{j=i+1}^{n}(-1)^{j-1}(g_0, g_1, \ldots, \hat{g}_i, \ldots, \hat{g}_j, \ldots, g_n)\right)$$

Para cualesquiera 2 índices $0 \leq r < s \leq n$, el elemento $(g_0, ..., \hat{g}_r, \ldots, \hat{g}_s, \ldots, g_n)$ aparece exactamente 2 veces en la expresión anterior y su coeficiente es $(-1)^{r+s} + (-1)^{r+s-1} = 0$, lo cual prueba que $\partial_{n-1} \circ \partial_n = 0$. Por tanto $\operatorname{im} \partial_n \subseteq \ker \partial_{n-1}$.

Ahora sea $h_n : P_{n-1} \to P_n$, dada por:

$$h_n(g_0, \ldots, g_{n-1}) = (1, g_0, \ldots, g_{n-1}),$$

$n = 1, 2, \ldots$ Definimos también $h_0 : P_{-1} = \mathbb{Z} \to P_0$, $h_0(1) = 1 \in \mathbb{Z}[G] = P_0$.

Se tiene que

$$
\begin{aligned}
&(\partial_n h_n + h_{n-1}\partial_{n-1})(g_0, \ldots, g_{n-1}) \\
&= \partial_n(1, g_0, ..., g_{n-1}) + h_{n-1}\left(\sum_{i=0}^{n-1}(-1)^i(g_0, g_1, \ldots, \hat{g}_i, \ldots, g_{n-1})\right) \\
&= (g_0, \ldots, g_{n-1}) + \sum_{i=0}^{n-1}(-1)^{i+1}(1, g_0, \ldots, \hat{g}_i, \ldots, g_{n-1}) + \\
&\quad + \sum_{i=0}^{n-1}(-1)^i(1, g_0, \ldots, \hat{g}_i, \ldots, g_{n-1}) \\
&= (g_0, \ldots, g_{n-1})
\end{aligned}
$$

esto es, $\partial_n h_n + h_{n-1}\partial_{n-1} = \mathrm{Id}_{P_{n-1}},\ n = 1, 2, \ldots$

Notemos que h_n se ha definido como $\mathbb{Z}$-homomorfismo pero no como G-homomorfismo.

Ahora si $x \in \ker \partial_{n-1}$, $x = \mathrm{Id}_{P_{n-1}}(x) = \partial_n h_n(x) + h_{n-1}\partial_{n-1}(x) = \partial_n(h_n(x)) + h_{n-1}(0) = \partial_n(h_n(x))$, esto es, $x = \partial_n(h_n(x)) \in \mathrm{im}\,\partial_n$, lo cual prueba la exactitud de la sucesión.■

Siempre que se hable de una resolución, si no se indica lo contrario, entenderemos la resolución dada en la Proposición 2.1.2, la cual recibe el nombre de la **resolución canónica ó resolución barra**.

Hemos probado la existencia de los grupos de homología y de cohomología para cualquier G-módulo A. Ahora si A y B son dos G-módulos y $f : A \to B$ es un G-homomorfismo, se definirán de manera natural homomorfismos de grupos:

$$\mathrm{H}^n(f) : \mathrm{H}^n(G,\ A) \to \mathrm{H}^n(G,\ B) \quad \text{y} \quad \mathrm{H}_n(f) : \mathrm{H}_n(G,\ A) \to \mathrm{H}_n(G,\ B).$$

Sea $P : \quad \cdots \to P_n \xrightarrow{\partial_n} P_{n-1} \to \cdots \to P_1 \xrightarrow{\partial_1} \mathrm{P}_0 \xrightarrow{\partial_0} \mathbb{Z} \to 0$ una resolución proyectiva. Entonces, se tiene la sucesión exacta

$$P \otimes_G A : \ \cdots \to P_n \otimes A \xrightarrow{\partial_n \otimes 1_A} P_{n-1} \otimes A \to \cdots \to P_1 \otimes A \xrightarrow{\partial_1 \otimes 1_A} P_0 \otimes A \to 0,$$

donde $P_i \otimes A$ significa $P_i \otimes_{\mathbb{Z}[G]} A$.

El G-morfismo $f : A \to B$ induce $f_n : P_n \otimes A \to P_n \otimes B$, dada por $f_n(x \otimes a) = x \otimes f(a) = (1_{P_n} \otimes f)(a)$. Ahora,

$$f_{n-1} \circ (\partial_n \otimes 1_A) = \partial_n \otimes f = (\partial_n \otimes 1_B) \circ (1_{P_n} \otimes f) = (\partial_n \otimes 1_B) \circ f_n.$$

Si $\alpha \in \ker(\partial_n \otimes 1_A)$, entonces

$$f_{n-1} \circ (\partial_n \otimes 1_A)(\alpha) = 0 = (\partial_n \otimes 1_B) \circ (1_{P_n} \otimes f)(\alpha) = (\partial_n \otimes 1_B) \circ f_n(\alpha),$$

por lo cual

$$f_n(\alpha) \in \ker(\partial_n \otimes 1_B).$$

Si $\alpha \in \operatorname{im}(\partial_{n+1} \otimes 1_A)$, $\alpha = (\partial_{n+1} \otimes 1_A)(\beta)$, por lo cual $f_n(\alpha) = f_n \circ (\partial_{n+1} \otimes 1_A)(\beta) = ((\partial_{n+1} \otimes 1_B) \circ f_{n+1})(\beta) \in \operatorname{im}(\partial_{n+1} \otimes 1_B)$.

Así pues, f_n induce de manera natural los homomorfismos de grupos:

$$\mathrm{H}_n(f) : \mathrm{H}_n(G,\, A) \to \mathrm{H}_n(G,\, B),\ \ n = 0, 1, \ldots$$

Consideremos ahora la sucesión

$$\begin{aligned} \mathrm{Hom}_G(P,\, A): \quad 0 \ &\to \mathrm{Hom}_G(P_0,\, A) \xrightarrow{\partial_1^*} \mathrm{Hom}_G(P_1,\, A) \xrightarrow{\partial_2^*} \cdots \\ &\to \mathrm{Hom}_G(P_{n-1},\, A) \xrightarrow{\partial_n^*} \mathrm{Hom}_G(P_n,\, A) \to \cdots \end{aligned}$$

Para B tenemos de forma similar:

$$\begin{aligned} \mathrm{Hom}_G(P,\, B): \quad 0 \ &\to \mathrm{Hom}_G(P_0,\, B) \xrightarrow{\partial_1^*} \mathrm{Hom}_G(P_1,\, B) \xrightarrow{\partial_2^*} \cdots \\ &\to \mathrm{Hom}_G(P_{n-1},\, B) \xrightarrow{\partial_n^*} \mathrm{Hom}_G(P_n,\, B) \to \cdots \end{aligned}$$

Sean $f_n^* : \mathrm{Hom}_G(P_n,\, A) \to \mathrm{Hom}_G(P_n,\, B)$ dadas por : $f_n^*(\varphi) = f \circ \varphi$. Se tiene

$$\begin{aligned} (f_n^* \circ \partial_n^*)(\varphi) &= f \circ \varphi \circ \partial_n \\ (\partial_n^* \circ f_{n-1}^*)(\varphi) &= f \circ \varphi \circ \partial_n. \end{aligned}$$

Lo cual implica que :

$$(f_n^* \circ \partial_n^*) = (\partial_n^* \circ f_{n-1}^*)$$

Si $\varphi \in \ker \partial_{n+1}^*$, $(\partial_{n+1}^* \circ f_n^*)(\varphi) = (f_{n+1}^* \circ \partial_{n+1}^*)(\varphi) = 0$, por lo tanto $f_n^*(\varphi) \in \ker \partial_{n+1}^*$.

Si $\varphi \in \operatorname{im} \partial_n^*$ entonces existe $\theta \in \operatorname{Hom}_G(P_{n-1},\ B)$ o $\operatorname{Hom}_G(P_{n-1},\ A)$ tal que $\partial_n^*(\theta) = \theta \circ \partial_n = \varphi$, y por lo tanto $f_n^*(\varphi) = (f_n^* \circ \partial_n^*)(\theta) = (\partial_n^* \circ f_{n-1}^*)(\theta) \in \operatorname{im} \partial_n^*$.

Así pues, f_n^* induce de manera natural un homomorfismo de grupos:

$$\mathrm{H}^n(f) : \mathrm{H}^n(G,\ A) \to \mathrm{H}^n(G,\ B),\ \ n = 0, 1, \ldots$$

El siguiente resultado nos da una poderosa herramienta para poder estudiar la aritmética de los campos por medio de los grupos de cohomología y de homología.

Teorema 2.1.2. *Sea* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *una sucesión exacta de G-módulos. Entonces, existen homomorfismos de grupos*

$$\varepsilon_n : \mathrm{H}_{n+1}(G,\ C) \to \mathrm{H}_n(G,\ A) \ \text{ y } \ \delta_n : \mathrm{H}^n(G,\ C) \to \mathrm{H}^{n+1}(G,\ A),$$

$n = 0, 1, \ldots$, *tales que las sucesiones de homología*

$$\to \mathrm{H}_{n+1}(G,\ B) \xrightarrow{\mathrm{H}_{n+1}(g)} \mathrm{H}_{n+1}(G,\ C) \xrightarrow{\varepsilon_n} \mathrm{H}_n(G,\ A) \xrightarrow{\mathrm{H}_n(f)} \mathrm{H}_n(G,\ B) \to$$
$$\cdots \xrightarrow{\varepsilon_0} \mathrm{H}_0(G,\ A) \xrightarrow{\mathrm{H}_0(f)} \mathrm{H}_0(G,\ B) \xrightarrow{\mathrm{H}_0(g)} \mathrm{H}_0(G,\ C) \to 0 \cdots$$

y de cohomología

$$0 \to \mathrm{H}^0(G,\ A) \xrightarrow{\mathrm{H}^0(f)} \mathrm{H}^0(G,\ B) \xrightarrow{\mathrm{H}^0(g)} \mathrm{H}^0(G,\ C) \xrightarrow{\delta_0} \mathrm{H}^1(G,\ A) \to \cdots$$
$$\xrightarrow{\delta_{n-1}} \mathrm{H}^n(G, A) \xrightarrow{\mathrm{H}^n(f)} \mathrm{H}^n(G, B) \xrightarrow{\mathrm{H}^n(g)} \mathrm{H}^n(G, C) \xrightarrow{\delta_n} \mathrm{H}^{n+1}(G, A) \to \cdots$$

son sucesiones exactas de grupos.

Demostración: Sea

$$P: \quad \cdots \to P_n \xrightarrow{\partial_n} P_{n-1} \to \cdots \to P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathbb{Z} \to 0$$

una resolución proyectiva.

Denotemos por:

$$X_n = P_n \otimes X \quad \text{y}$$

$$X^n = \mathrm{Hom}_G(P_n, X),$$

donde $X = A, \quad B \quad \text{o} \quad C$.

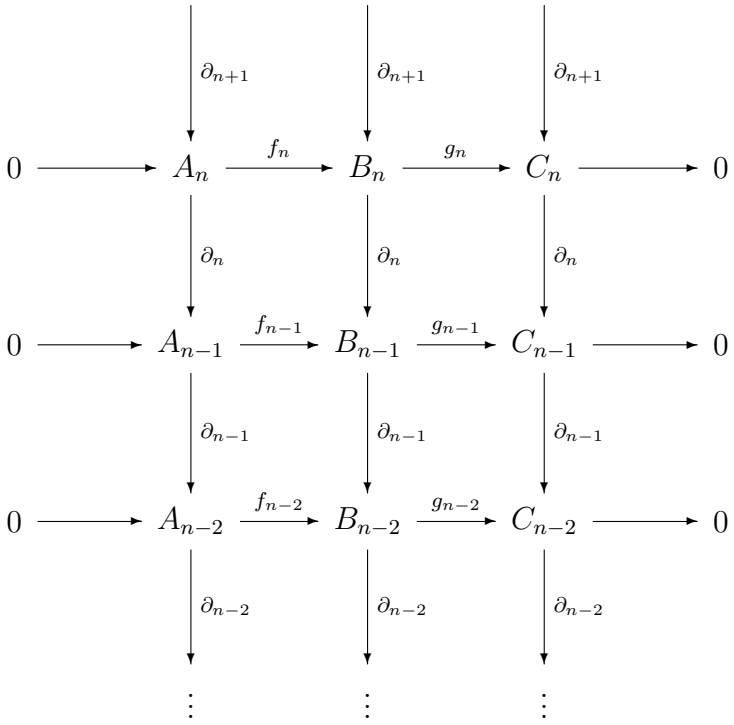
También denotamos por:

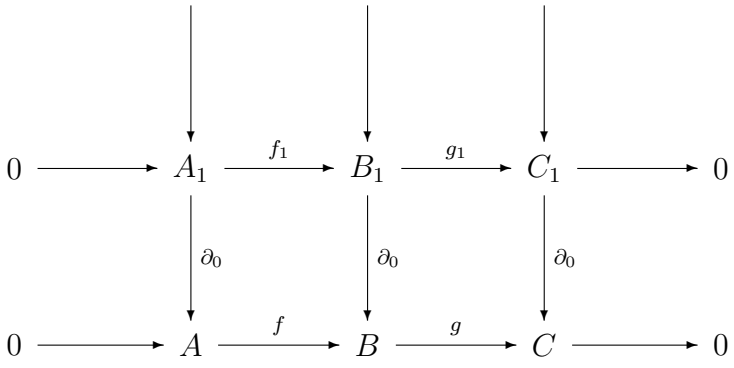
$$k_n = \mathrm{H}_n(k) \quad \text{y}$$

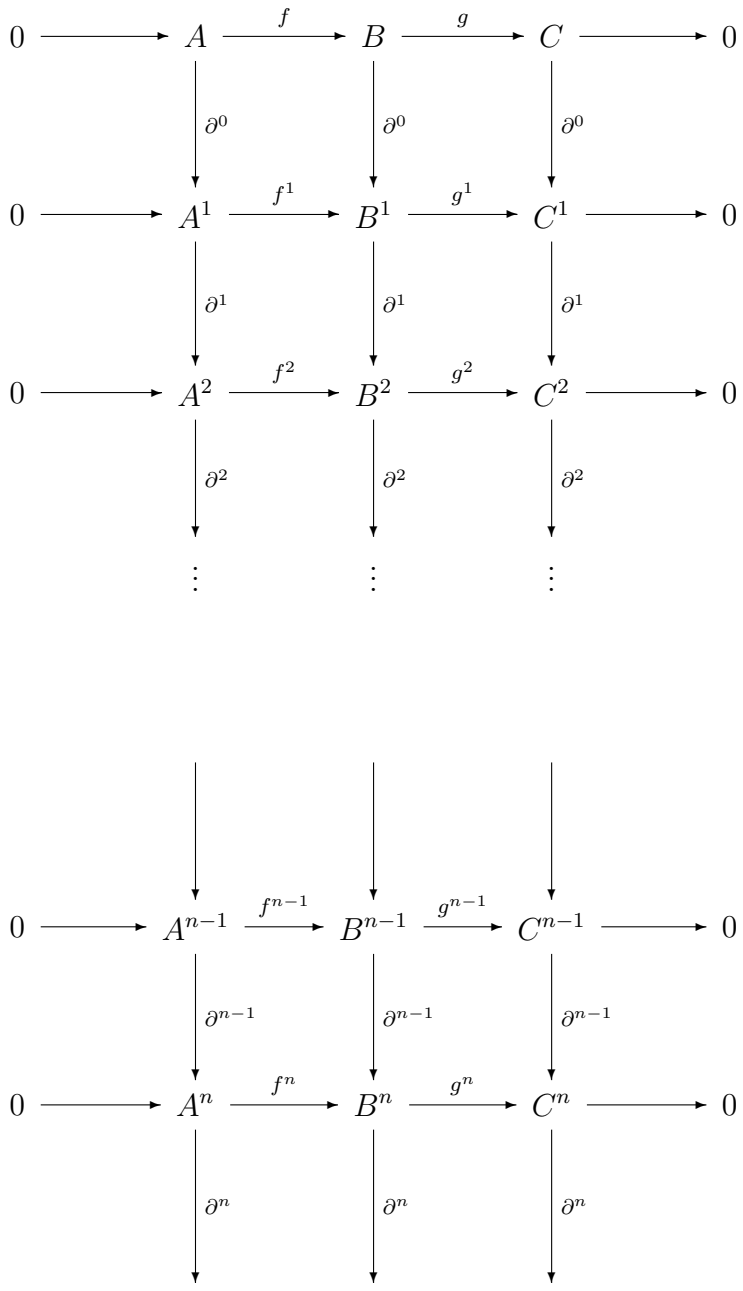
$$k^n = \mathrm{H}^n(k),$$

donde $k = f \quad \text{o} \quad g$.

Entonces, se tiene que los diagramas


∂_{n+1}
∂_{n+1}
∂_{n+1}
0
A_n
f_n
B_n
g_n
C_n
0
∂_n
∂_n
∂_n
0
A_{n-1}
f_{n-1}
B_{n-1}
g_{n-1}
C_{n-1}
0
∂_{n-1}
∂_{n-1}
∂_{n-1}
0
A_{n-2}
f_{n-2}
B_{n-2}
g_{n-2}
C_{n-2}
0
∂_{n-2}
∂_{n-2}
∂_{n-2}
$\vdots$
$\vdots$
$\vdots$


0
A_1
f_1
B_1
g_1
C_1
0
∂_0
∂_0
∂_0
0
A
f
B
g
C
0



de grupos de homología y cohomología, respectivamente, son conmutativos.

Ahora bien,

$$\partial_n : X_n \to X_{n-1}$$

induce

$$\tilde{\partial_n} : \text{coker } \partial_{n+1} \to \ker \partial_{n-1}$$

ya que : $\text{im } \partial_{n+1} \subseteq \ker \partial_n$, con lo cual

$$\text{coker } \partial_{n+1} = X_n/\text{ im } \partial_{n+1} \xrightarrow{\tilde{\partial_n}} X_n/\ker\ \partial_n \cong\ \text{im}\partial_n \subseteq \ker \partial_{n-1}.$$

Luego,

$$\ker \tilde{\partial_n} = \ker \partial_n/\text{ im } \partial_{n+1} = \text{H}_n(G,\ X) \quad \text{y}$$

$$\text{coker } \tilde{\partial_n} = \ker \partial_{n-1}/\text{ im } \partial_n = \text{H}_{n-1}(G,\ X).$$

Similarmente,

$$\partial^n : X^{n-1} \to X^n$$

induce

$$\tilde{\partial^n} : \text{coker } \partial^{n-1} \to \ker \partial^{n+1}$$

pues como $\text{im } \partial^{n-1} \subseteq \ker \partial^n$, se tiene

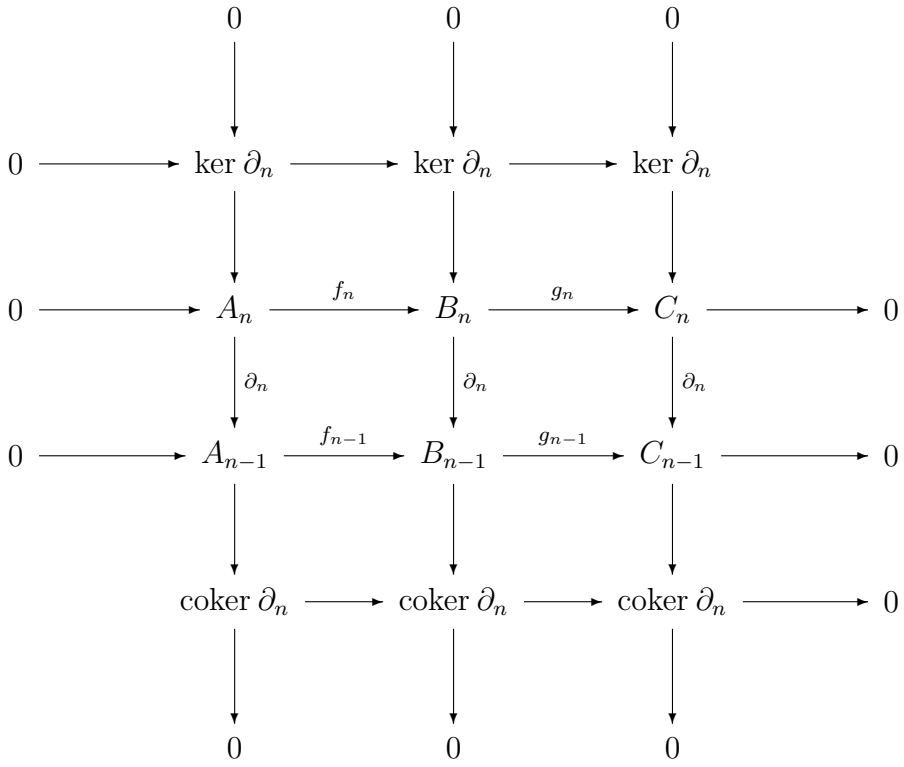
$$\text{coker } \partial^{n-1} = X^{n-1}/\text{ im } \partial^{n-1} \xrightarrow{\tilde{\partial^n}} X^{n-1}/\ker \partial^n \cong\ \text{im } \partial^n \subseteq \ker \partial^{n+1}.$$

Luego,

$$\ker \tilde{\partial^n} =\ \ker \partial^n/\text{ im } \partial^{n-1} = \text{H}^{n-1}(G,\ X) \quad \text{y}$$

$$\text{coker } \tilde{\partial^n} =\ \ker \partial^{n+1}/\text{ im } \partial^n = \text{H}^n(G,\ X).$$

Así pues, se tiene el diagrama conmutativo



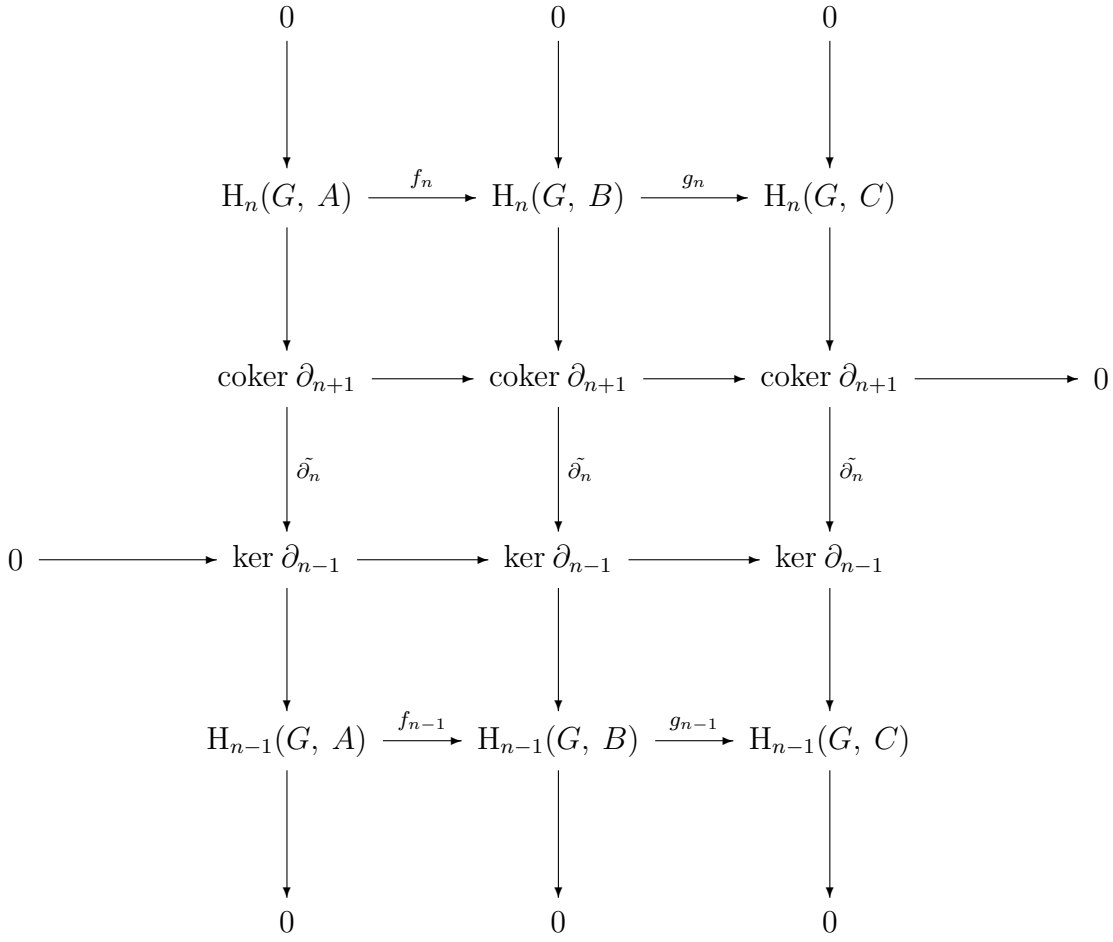
Por el Lema de la Serpiente (Teorema 1.2.3), las filas del diagrama anterior son exactas.

Ahora bien, $\partial_n : X_n \to X_{n-1}$ induce

$$0 \to \mathrm{H}_n(G,\, X) = \ker \tilde{\partial}_n \to \operatorname{coker} \partial_{n+1} \xrightarrow{\tilde{\partial}_n}$$

$$\xrightarrow{\tilde{\partial}_n} \ker \partial_{n-1} \to \operatorname{coker} \tilde{\partial}_n = \mathrm{H}_{n-1}(G,\, X).$$

De aquí que, obtenemos el diagrama

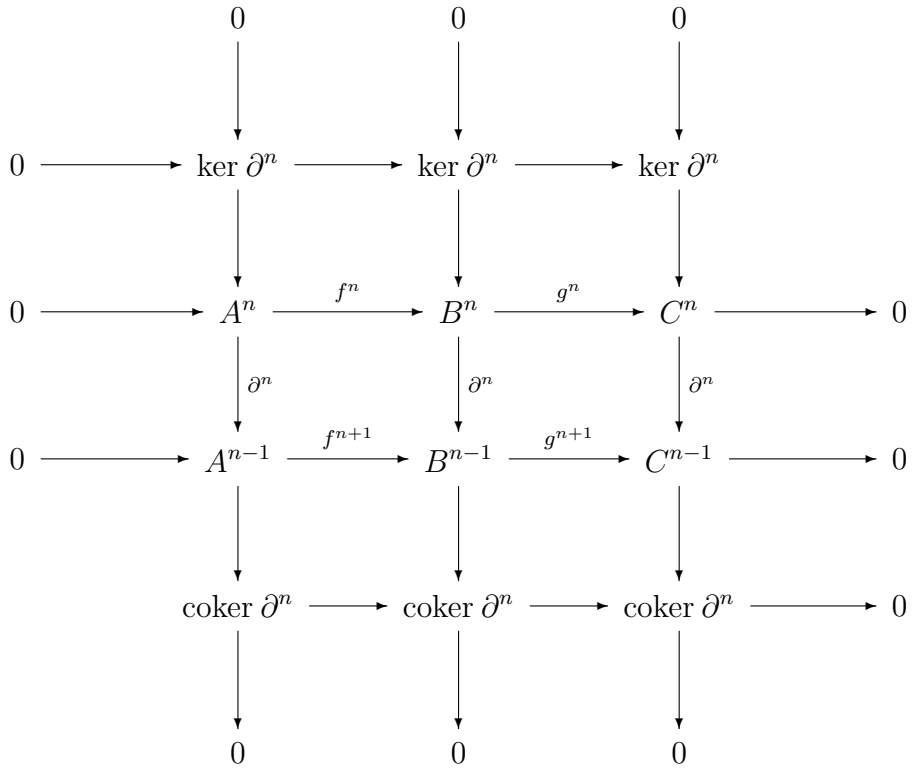


Nuevamente, por el Lema de la Serpiente, se tiene que existe un homomorfismo de grupos $\varepsilon_{n-1} : \mathrm{H}_n(G,\ C) \to \mathrm{H}_{n-1}(G,\ A)$ tal que

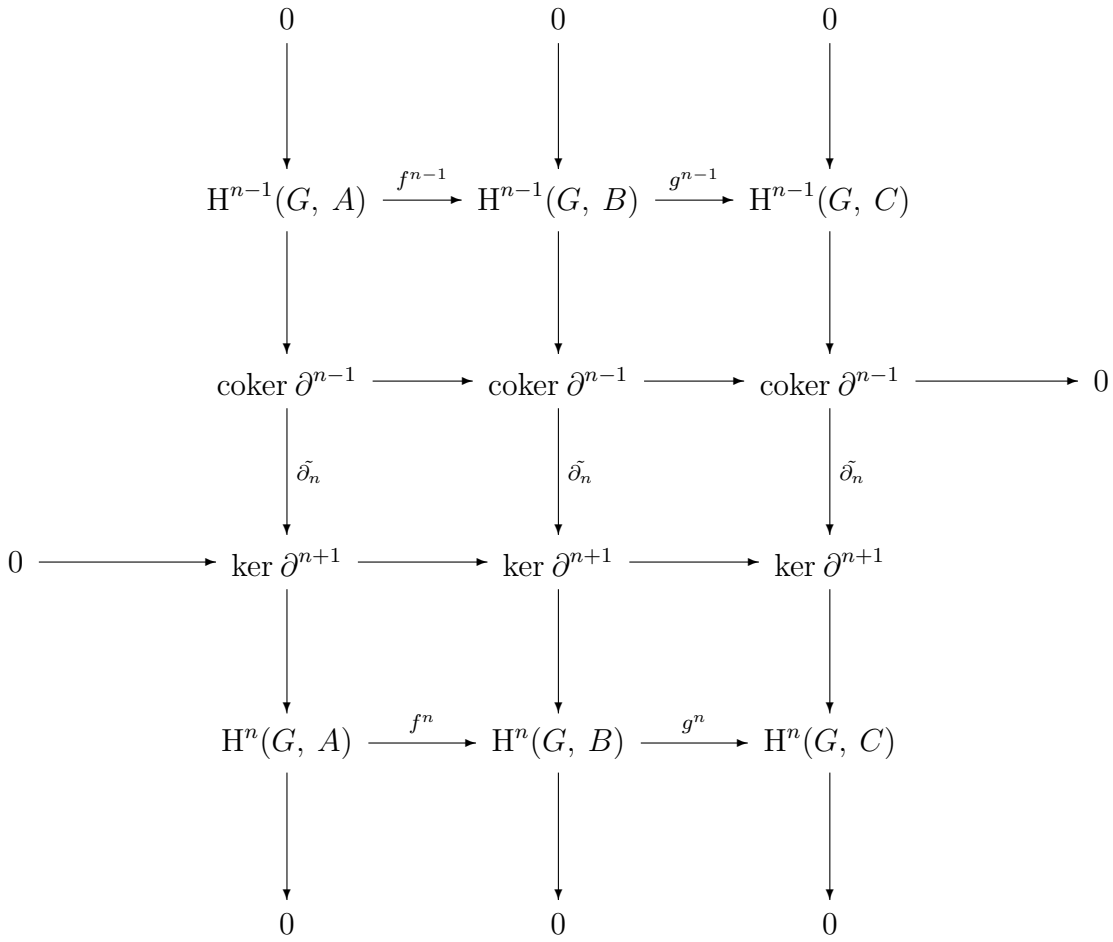
$$\mathrm{H}_n(G,\ A) \to \mathrm{H}_n(G,\ B) \to \mathrm{H}_n(G,\ C) \xrightarrow{\varepsilon_{n-1}} \mathrm{H}_{n-1}(G,\ A)$$
$$\to \mathrm{H}_{n-1}(G,\ B) \to \mathrm{H}_{n-1}(G,\ C)$$

es exacta.

Similarmente, para la cohomología se tienen diagramas:


0
0
0
0
ker ∂^n
ker ∂^n
ker ∂^n
0
A^n
f^n
B^n
g^n
C^n
0
∂^n
∂^n
∂^n
0
A^{n-1}
f^{n+1}
B^{n-1}
g^{n+1}
C^{n-1}
0
coker ∂^n
coker ∂^n
coker ∂^n
0
0
0
0

y



Por el Lema de la Serpiente (Teorema 1.2.3), existe $\delta_{n-1} : \mathrm{H}^{n-1}(G,\ C) \to \mathrm{H}^n(G,\ A)$, que hace exacta la sucesión

$$\mathrm{H}^{n-1}(G,\ A) \to \mathrm{H}^{n-1}(G,\ B) \to \mathrm{H}^{n-1}(G,\ C) \xrightarrow{\delta_{n-1}} \mathrm{H}^n(G,\ A)$$
$$\to \mathrm{H}^n(G,\ B) \to \mathrm{H}^n(G,\ C). \quad \blacksquare$$

2.2 G-Módulos Inducidos y Coinducidos

El propósito de esta sección es el de proporcionar G-módulos especiales que serán importantes para la obtención de resultados.

Sea A un G-módulo arbitrario. Entonces, la sucesión de homología es

$$\cdots \to P_n \otimes A \xrightarrow{\partial_n \otimes 1_A} P_{n-1} \otimes A \to \cdots \to P_1 \otimes A \xrightarrow{\partial_1 \otimes 1_A} P_0 \otimes A \to 0,$$

con $\{P_i\}_{i=0}^{\infty}$ la resolución canónica dada en la sección anterior.

En particular, $P_0 = \mathbb{Z}[G]$ y $P_0 \otimes A \cong A$. Luego,

$$\mathrm{H}_0(G,\ A) = (P_0 \otimes A)/(\operatorname{im} \partial_1 \otimes 1_A).$$

Ahora bien, se tiene que $(\partial_1 \otimes 1_A)((g_1, g_2) \otimes a) = g_1 a - g_2 a$, lo cual implica que

$$\operatorname{im}(\partial_1 \otimes 1_A) = \langle a - ga \mid g \in G, a \in A \rangle = DA \subseteq A,$$

ya que

$$g_1 a - g_2 a = a - g_2 a - a + g_1 a = (a - g_2 a) - (a - g_1 a) \in DA.$$

Puesto que $P_0 \otimes A \cong A$, $\mathrm{H}_0(G,\ A) = A_G = A/DA$, A_G es el módulo cociente maximal de A en donde G actúa trivialmente.

Sea $\mathrm{I}_G = \left\{ \sum_{\sigma \in G} a_\sigma \sigma \mid \sum_{\sigma \in G} a_\sigma = 0 \right\}$. Entonces, si

$$\sum_{\sigma \in G} a_\sigma \sigma \in \mathrm{I}_G,\ \ a_1 = -\sum_{\sigma \neq 1} a_\sigma,$$

se tiene que,

$$\sum_{\sigma \in G} a_\sigma \sigma = a_1 \cdot 1 + \sum_{\sigma \neq 1} a_\sigma \sigma = \left(-\sum_{\sigma \neq 1} a_\sigma \right) 1 + \sum_{\sigma \neq 1} a_\sigma \sigma =$$
$$= \sum_{\sigma \neq 1} a_\sigma (\sigma - 1) \in \ \langle \sigma - 1 \mid \ \sigma \in G \rangle.$$

Recíprocamente, se tiene que $\sigma - 1 \in \mathrm{I}_G$ para $\sigma \in G$. Entonces

$$DA = \langle a - \sigma a \mid \sigma \in G, a \in A \rangle = \mathrm{I}_G A.$$

Por lo tanto, $\mathrm{H}_0(G,\, A) = A/\mathrm{I}_G A$.

Proposición 2.2.1. *Para cualquier grupo G, se tiene que $\mathrm{I}_G/\mathrm{I}_G^2 \cong G/G'$, donde G' es el subgrupo conmutador de G.*

Demostración: Sea $f : G \to \mathrm{I}_G/\mathrm{I}_G^2$ el mapeo $f(\sigma) = (\sigma-1)+\mathrm{I}_G^2$. Ahora bien,

$$\begin{aligned} f(\sigma\phi) &= (\sigma\phi - 1) + \mathrm{I}_G^2 = (\sigma\phi - \sigma + \sigma - 1) + \mathrm{I}_G^2 \\ &= \sigma(\phi - 1) + (\sigma - 1) + \mathrm{I}_G^2 \\ &= (\sigma - 1)(\phi - 1) + (\phi - 1) + (\sigma - 1) + \mathrm{I}_G^2 \end{aligned}$$

y puesto que $(\sigma - 1)(\phi - 1) \in \mathrm{I}_G^2$, se tiene que $f(\sigma\phi) = f(\sigma) + f(\phi)$, esto es, f es un homomorfismo.

Puesto que $\mathrm{I}_G/\mathrm{I}_G^2$ es abeliano, $G/\ker f$ es abeliano y, por tanto, $[G, G] = G' \subseteq \ker f$. Entonces, f induce $\tilde{f} : G/G' \to \mathrm{I}_G/\mathrm{I}_G^2$, dada por:

$$\tilde{f}(\sigma G') = (\sigma - 1) + \mathrm{I}_G^2.$$

Ahora bien, sea $h : \mathrm{I}_G \to G/G'$ el mapeo $h(\sigma - 1) = \sigma G'$. Si $x \in \mathrm{I}_G^2$ se tiene

$$\begin{aligned} x &= \left(\sum_{\sigma\in G} a_\sigma(\sigma - 1)\right)\left(\sum_{\sigma\in G} b_\sigma(\sigma - 1)\right) = \sum_{\sigma,\theta\in G} a_\sigma b_\theta(\sigma - 1)(\theta - 1) \\ &= \sum_{\sigma,\theta\in G} a_\sigma b_\theta[(\sigma\theta - 1) - (\sigma - 1) - (\theta - 1)], \end{aligned}$$

por lo tanto

$$\begin{aligned} h(x) &= \prod_{\sigma,\theta\in G} \left[h(\sigma\theta - 1)h(\sigma - 1)^{-1}h(\theta - 1)^{-1}\right]^{a_\sigma b_\theta} \\ &= \prod_{\sigma,\theta\in G} \left(\sigma\theta\sigma^{-1}\theta^{-1}\right)^{a_\sigma b_\theta} G' = G', \end{aligned}$$

por lo que $h(x) = 1$, esto es,$\mathrm{I}_G^2 \subseteq \ker h$ y por lo tanto h induce $\tilde{h} : \mathrm{I}_G/\mathrm{I}_G^2 \to G/G'$ dada por:

$$\tilde{h}((\sigma - 1) + \mathrm{I}_G^2) = \sigma G'.$$

Claramente $\tilde{f}$ y $\tilde{h}$ son isomorfismos inversos. ■

Definición 2.2.1. *Sea X un grupo abeliano, X considerado con G-acción trivial, y sea A el G-módulo* $\mathrm{Hom}(\mathbb{Z}[G], X)$. *Cualquier G-módulo de este tipo se llama* ***coinducido****.*

La acción de G en $A = \mathrm{Hom}(\mathbb{Z}[G], X)$ explícitamente está definida por: $\varphi \in A,\ g, g' \in G,\ g \circ \varphi(g') = g\varphi(g^{-1}g') = \varphi(g^{-1}g')$.

Definición 2.2.2. *Sea X un grupo abeliano y sea A el G-módulo $\mathbb{Z}[G] \otimes_{\mathbb{Z}} X$. Un G-módulo de este tipo se llama* ***inducido****.*

La acción de G en A es: $g, g' \in G,\ x \in X,\ g(g' \otimes x) = gg' \otimes x$.

Proposición 2.2.2. *Sea $A = \mathrm{Hom}(\mathbb{Z}[G], X)$. Entonces para cualquier G-módulo B,* $\mathrm{Hom}_G(B, A) \cong \mathrm{Hom}(B, X)$ *como grupos.*

Demostración: Sea $\varphi \in \mathrm{Hom}_G(B, A)$, esto es, $\varphi(b) \in \mathrm{Hom}(\mathbb{Z}[G], X)$ para $b \in B$. Sea $\theta_\varphi : B \to X$ dada por: $\theta_\varphi(b) = \varphi(b)(1)$.
Se tiene que:

$$\begin{aligned} \theta_\varphi(b + b_1) &= (\varphi(b + b_1))(1) = (\varphi(b) + \varphi(b_1))(1) = \varphi(b)(1) + \varphi(b_1)(1) \\ &= \theta_\varphi(b) + \theta_\varphi(b_1) \end{aligned}$$

esto es, $\theta_\varphi \in \mathrm{Hom}(B, X)$.

$$(\theta_{\varphi+\psi})(b) = ((\varphi + \psi)(b))(1) = (\varphi(b) + \psi(b))(1) =$$

$$= \varphi(b)(1) + \psi(b)(1) = \theta_\varphi + \theta_\psi,$$

por tanto $\theta_{\varphi+\psi} = \theta_\varphi + \theta_\psi$.

Por lo que θ es un homomorfismo de grupos entre $\mathrm{Hom}_G(B, A)$ y $\mathrm{Hom}_{\mathbb{Z}}(B, X)$.

Ahora, si $\theta_\varphi = 0$, esto es, $\theta_\varphi : B \to X, \theta_\varphi(b) = 0$ para todo $b \in B, \varphi(b)(1) = 0$ para todo $b \in B$. Puesto que $\varphi \in \mathrm{Hom}_G(B,\, A)$, se tiene $\varphi(gb) = g\varphi(b)$ para $g \in G,\, b \in B$.
Ahora, si $g^{'} \in G \subseteq \mathbb{Z}[G],\, (g\varphi(b))(g^{'}) = g[\varphi(b)(g^{-1}g^{'})] = \varphi(b)(g^{-1}g^{'})$.

En particular, $\varphi(gb)(1) = (g\varphi(b))(1) = \varphi(b)(g^{-1})$ o, equivalentemente, $\varphi(g^{-1}b)(1) = \varphi(b)(g)$. Por lo tanto, $\theta_\varphi = 0$ implica que $\varphi(b)(g) = 0$ para todo $g \in G,\, b \in B$ de donde $\varphi(b) = 0$ para todo $b \in B$, es decir, $\varphi = 0$. Esto prueba que θ es inyectiva.

Por otro lado, sea $\sigma \in \mathrm{Hom}_{\mathbb{Z}}(B,\, X)$. Queremos hallar $\varphi \in \mathrm{Hom}_G(B,\, A)$ tal que $\sigma(b) = \varphi(b)(1)$ para toda $b \in B$. Sea $\varphi \in \mathrm{Hom}_G(B,\, A)$, dada por

$$\varphi(b) : \mathbb{Z}[G] \to X, \quad \varphi(b)(g) = \sigma(g^{-1}b).$$

Se tiene que:

$$\varphi(b + b^{'})(g) = \sigma(g^{-1}(b + b^{'})) = \sigma(g^{-1}b) + \sigma(g^{-1}b^{'}) = \varphi(b)(g) + \varphi(b^{'})(g),$$

esto es, $\varphi \in \mathrm{Hom}(B,\, A)$. Ahora bien,

$$[\varphi(gb)](g^{'}) = \sigma\left((g^{'})^{-1}gb\right),$$

$$(g\varphi(b))(g^{'}) = g\left(\varphi(b)\left(g^{-1}g^{'}\right)\right) = \varphi(b)\left(g^{-1}g^{'}\right) =$$

$$= \sigma\left((g^{'})^{-1}gb\right) = \varphi(gb)(g^{'}).$$

Por lo tanto $g\varphi(b) = \varphi(gb)$, es decir, tenemos que $\varphi \in \mathrm{Hom}_G(B,\, A)$ y $\theta_\varphi = \varphi(b)(1) = \sigma(1^{-1}b) = \sigma(b)$. luego θ es suprayectiva, así que θ es un isomorfismo como se quería probar. ■

Teorema 2.2.1. *Si* $A = \mathrm{Hom}(\mathbb{Z}[G],\ X)$ *es un módulo coinducido, entonces* $\mathrm{H}^n(G,\ A) = 0$ *para* $n \geq 1$. (*Si* A *es* G*-módulo inyectivo, entonces también se tiene que* $\mathrm{H}^n(G,\ A) = 0$ *para* $n \geq 1$.)

Demostración: La sucesión en cohomología es

$$0 \to \mathrm{Hom}_G(P_0,\ A) \xrightarrow{\partial_1^*} \mathrm{Hom}_G(P_1,\ A) \xrightarrow{\partial_2^*} \cdots$$

Por la Proposición 2.2.2, esta sucesión es igual a la sucesión

$$0 \to \mathrm{Hom}(P_0,\ X) \xrightarrow{\partial_1^*} \mathrm{Hom}(P_1,\ X) \xrightarrow{\partial_2^*} \cdots$$

Como $\cdots \to P_n \xrightarrow{\partial_n} P_{n-1} \to \cdots \to P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathbb{Z} \to 0$ es exacta a partir de P_1, siendo los $P_i^{'}$s grupos libres, se sigue que la sucesión de cohomología es exacta apartir del primer índice, esto es, $\mathrm{H}^n(G,\ A) = 0$ para $n \geq 1$. ■

En general, para cualquier módulo A, de la resolución

$$\cdots \to P_n \xrightarrow{\partial_n} P_{n-1} \to \cdots \to P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathbb{Z} \to 0$$

se tiene que

$$0 \to \mathrm{Hom}_G(\mathbb{Z},\ A) \xrightarrow{\partial_0^*} \mathrm{Hom}_G(P_0,\ A) \xrightarrow{\partial_1^*} \mathrm{Hom}_G(P_1,\ A)$$

es exacta en $\mathrm{Hom}_G(\mathbb{Z},\ A)$ y $\mathrm{Hom}_G(P_0,\ A)$, por tanto

$$\mathrm{H}^0(G,\ A) = \ker \partial_1^* = \mathrm{im}\, \partial_0^* = \mathrm{Hom}_G(\mathbb{Z},\ A) = (\mathrm{Hom}(\mathbb{Z},\ A))^G \cong A^G.$$

Resumiendo lo obtenido hasta ahora, tenemos el siguiente

Teorema 2.2.2. *Para cualquier* G*-módulo* A, *se tiene* $\mathrm{H}_0(G,\ A) = A/DA = A_G$, *donde* $DA = \langle a - \sigma a \mid \sigma \in G \rangle$, y $\mathrm{H}^0(G,\ A) = A^G$. ■

Corolario 2.2.1. *Si* $0 \to A \to B \to C \to 0$ *es una sucesión exacta de* G*-módulos y* B *es un* G*-módulo coinducido, entonces* $\mathrm{H}^q(G,\, C) = \mathrm{H}^{q+1}(G,\, A)$ *para* $q \geq 1$.

Demostración: De los Teoremas 2.1.2 y 2.2.1 obtenemos la sucesión exacta de grupos

$$0 \to A^G \to B^G \to C^G \to \mathrm{H}^1(G,\, A) \to \mathrm{H}^1(G,\, B) \to \mathrm{H}^1(G,\, C) \to \cdots$$
$$\to \mathrm{H}^q(G,\, A) \to \mathrm{H}^q(G,\, B) \to \mathrm{H}^q(G,\, C) \to \mathrm{H}^{q+1}(G,\, A) \to \mathrm{H}^{q+1}(G,\, B) \to \cdots$$

Como $\mathrm{H}^q(G,\, B) = 0$ para $q \geq 1$, se sigue el resultado.■

Ahora bien, se tiene el siguiente

Teorema 2.2.3. *Si* A *es un* G*-módulo inducido,* $A = \mathbb{Z}[G] \otimes_{\mathbb{Z}} X$. *Entonces* $\mathrm{H}_n(G,\, A) = 0$ *para* $n \geq 1$. *(Si* A *es un* G*-módulo proyectivo, entonces* A *es plano y* $\mathrm{H}_n(G,\, A) = 0$ *para* $n \geq 1$.*)*

Demostración: Se tiene

$$P_n \otimes_G A \cong P_n \otimes_G (\mathbb{Z}[G] \otimes_{\mathbb{Z}} X) \cong (P_n \otimes_G \mathbb{Z}[G]) \otimes_{\mathbb{Z}} X \cong P_n \otimes_{\mathbb{Z}} X.$$

Así, de la resolución

$$\cdots \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to \mathbb{Z} \to 0,$$

obtenemos

$$\cdots \to P_n \otimes_G A \to P_{n-1} \otimes_G A \to \cdots \to P_1 \otimes_G A \to P_0 \otimes_G A \to \mathbb{Z} \otimes_G A \to 0,$$

la cual es equivalente a

$$\cdots \to P_n \otimes_{\mathbb{Z}} X \to P_{n-1} \otimes_{\mathbb{Z}} X \to \cdots \to P_1 \otimes_{\mathbb{Z}} X \to P_0 \otimes_{\mathbb{Z}} X \to \mathbb{Z} \otimes_{\mathbb{Z}} X \cong X \to 0.$$

Puesto que P_i es un grupo abeliano libre, la sucesión es exacta. Por lo tanto $\mathrm{H}_n(G,\, A) = 0$ para $n \geq 1$.
Para $n = 0$, $\mathrm{H}_0(G,\, A) = (\mathbb{Z}[G] \otimes_{\mathbb{Z}} X)/\operatorname{im} \partial_1 \cong A/I_G A$. ■

Corolario 2.2.2. *Si* $0 \to A \to B \to C \to 0$ *es una sucesión exacta de* G*-módulos y* B *es un* G*-módulo inducido, entonces* $\mathrm{H}_{q+1}(G,\, C) = \mathrm{H}_q(G,\, A)$ *para* $q \geq 1$.

Demostración: Del Teorema 2.1.2 se tiene la sucesión exacta

$$\cdots \to \mathrm{H}_{q+1}(G,\, B) \to \mathrm{H}_{q+1}(G,\, C) \to \mathrm{H}_q(G,\, A) \to \mathrm{H}_q(G,\, B) \to \cdots$$

Puesto que $\mathrm{H}_q(G,\, B) = 0$ para $q \geq 1$, se sigue el resultado. ■

2.3 Homología y Cohomología en Bajas Dimensiones

El propósito de esta sección es el cálculo de algunos de los grupos de homología H_n y de cohomología H^n, para $n = 0, 1, 2$.

Lema 2.3.1. *Sea* G *un grupo finito. Se tiene que* $\mathbb{Z}[G] \cong \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$. *En particular* $\mathbb{Z}[G]$ *es coinducido.*

Demostración: Sea $A = \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$. Para $f \in A$, sea $\varphi(f) = \sum\limits_{\sigma \in G} f(\sigma)\, \sigma$, $\varphi : A \to \mathbb{Z}[G]$. Entonces

$$\varphi(f+g) = \sum_{\sigma \in G} (f+g)(\sigma)\, \sigma = \sum_{\sigma \in G} (f(\sigma) + g(\sigma))\, \sigma = \varphi(f) + \varphi(g).$$

Claramente φ es suprayectiva y finalmente si $\varphi(f) = \sum\limits_{\sigma \in G} f(\sigma)\sigma = 0$, entonces $f(\sigma) = 0$ para toda $\sigma \in G$ y por tanto $f = 0$, por lo que φ es biyectiva.

Ahora, si $\theta \in G$,

$$\varphi(\theta f) = \sum_{\sigma \in G} (\theta f)(\sigma)\, \sigma = \sum_{\sigma \in G} \left(\, \theta f \left(\theta^{-1}\sigma\right)\right)\ \sigma = \sum_{\sigma \in G} f\left(\theta^{-1}\sigma\right)\ \sigma =$$

$$= \sum_{\sigma \in G} f\left(\theta^{-1}\sigma\right)\ \theta\ \left(\theta^{-1}\sigma\right) = \theta \sum_{\sigma \in G} f(\sigma)\, \sigma = \theta\varphi(f),$$

por lo que φ es un G-isomorfismo. ■

Proposición 2.3.1. *Se tiene que* $\mathrm{H}_1(G,\,\mathbb{Z}) \cong \mathrm{I}_G/\,\mathrm{I}_G^2 \cong G/\,G'$.

Demostración: Sea $0 \to \mathrm{I}_G \to \mathbb{Z}[G] \xrightarrow{\pi} \mathbb{Z} \to 0$ la sucesión exacta donde

$$\pi\left(\sum_{\sigma\in G} a_\sigma\sigma\right) = \sum_{\sigma\in G} a_\sigma.$$

Ahora bien, puesto que $\mathbb{Z}[G]$ es coinducido, se tiene la sucesión exacta.

$$0 = \mathrm{H}_1(G,\,\mathbb{Z}[G]) \to \mathrm{H}_1(G,\,\mathbb{Z}) \to \mathrm{H}_0(G,\,\mathrm{I}_G) \xrightarrow{f}$$
$$\xrightarrow{f} \mathrm{H}_0(G,\,\mathbb{Z}[G]) \xrightarrow{h} \mathrm{H}_0(G,\,\mathbb{Z}) \to 0.$$

Por lo tanto $\mathrm{H}_1(G,\,\mathbb{Z}) = \ker\left(\mathrm{H}_0(G,\,\mathrm{I}_G) \xrightarrow{f} \mathrm{H}_0(G,\,\mathbb{Z}[G])\right)$.

Ahora $\mathrm{H}_0(G,\,\mathrm{I}_G) \cong \mathrm{I}_G/\,\mathrm{I}_G^2 \cong G/\,G'$, $\mathrm{H}_0(G,\mathbb{Z}[G]) \cong \mathbb{Z}[G]/\,\mathrm{I}_G \cong \mathbb{Z}$.

De la exactitud de la sucesión obtenemos que $\operatorname{im} f = \ker h$.

Por otro lado $\mathrm{H}_0(G,\,\mathbb{Z}) \cong \mathbb{Z}/\,\mathrm{I}_G\mathbb{Z} \cong \mathbb{Z}$ y como h es suprayectiva, $h : \mathbb{Z} \to \mathbb{Z}$, entonces $\ker h = 0 = \operatorname{im} f$, esto es, $\ker f = \mathrm{H}_0(G,\,\mathrm{I}_G) \cong \mathrm{I}_G/\,\mathrm{I}_G^2 \cong G/\,G'$, lo cual prueba la proposición. ■

Ahora analicemos la cohomología. De la resolución

$$\cdots \to P_n \xrightarrow{\partial_n} P_{n-1} \to \cdots \to P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathbb{Z} \to 0$$

donde $P_n = \mathbb{Z}[G^{n+1}]$, $\partial_n(g_0, ..., g_n) = \sum_{i=0}^{n}(-1)^i(g_0, ..., \hat{g}_i, ..., g_n)$, entonces, con $K_n = \mathrm{Hom}_G(P_n,\,A)$, tenemos la sucesión exacta

$$0 \to K_0 \xrightarrow{\partial_1^*} K_1 \to \cdots \xrightarrow{\partial_n^*} K_n \xrightarrow{\partial_{n+1}^*} \cdots,$$

$\mathrm{H}^n(G,\,A) = \ker \partial_{n+1}^*/\operatorname{im} \partial_n^*$.

Notemos que $f \in \mathrm{Hom}_G(P_n,\ A) = \mathrm{Hom}_G(\mathbb{Z}[G^{n+1}],\ A)$ está determinado por sus valores en G^{n+1} y $f(g_0, ..., g_n) = g_0 f\left(1, g_0^{-1}g_1, ..., g_0^{-1}g_n\right)$ por lo que f está determinado por sus valores en los elementos

$$(1, g_1, g_1g_2, g_1g_2g_3, ..., g_1g_2...g_n) \text{ de } G^{n+1}.$$

Pongamos $\varphi(g_1, ..., g_n) = f(1, g_1, g_1g_2, g_1g_2g_3, ..., g_1g_2...g_n)$.

Sea $[\, g_1 \mid g_2 \mid \cdots \mid g_{n+1}] = (1, g_1, g_1g_2, g_1g_2g_3, ..., g_1g_2...g_n)$.

Entonces
$\partial_{n+1}([\, g_1 \mid g_2 \mid \cdots \mid g_{n+1}])$

$$\begin{aligned}
&= (g_1, g_1g_2, g_1g_2g_3, ..., g_1g_2...g_{n+1}) \\
&\quad + \sum_{i=1}^{n+1}(-1)^i(1, g_1, ..., \widehat{g_1...g_i}, ..., g_1g_2...g_{n+1}) \\
&= g_1(1, g_2, ..., g_2...g_{n+1}) \\
&\quad + \sum_{i=1}^{n+1}(-1)^i(1, g_1, ..., g_1...g_{i-1}, g_1...g_ig_{i+1}, ..., g_1g_2...g_{n+1}) \\
&= g_1[\, g_2 \mid \cdots \mid g_{n+1}] \ + \ \sum_{i=1}^{n+1}(-1)^i\, [\, g_1 \mid \cdots \mid g_{i-1} \mid g_ig_{i+1} \mid \cdots \mid g_{n+1}].
\end{aligned}$$

Por tanto $f \in \ker \partial_{n+1}^* \Leftrightarrow \partial_{n+1}^*(f) = f \circ \partial_{n+1} = 0 \Longleftrightarrow$ para $g_1, ..., g_{n+1} \in G$,

$(f \circ \partial_{n+1})[\, g_1 \mid g_2 \mid \cdots \mid g_{n+1}]$

$$\begin{aligned}
&= g_1 f([\, g_2 \mid \cdots \mid g_{n+1}]) \\
&\quad + \sum_{i=1}^{n+1}(-1)^i f([\, g_1 \mid \cdots \mid g_i \mid g_ig_{i+1} \mid \cdots \mid g_{n+1}]) \\
&= 0. \qquad (2.3)
\end{aligned}$$

Por tanto, puesto que $\varphi(x_1, x_2, ..., x_{n+1}) = f([x_1 \mid x_2 \mid \cdots \mid x_{n+1}])$, la relación dada en (2.3), nos dice que $\ker \partial_{n+1}^*$ consiste de las funciones $\varphi : G^n \to A$, que satisfacen:

$$g_1\varphi\left(g_2,...,g_{n+1}\right) + \sum_{i=1}^{n+1}(-1)^i\varphi\left(g_1,...,g_{i-1},g_ig_{i+1},g_{i+2},...,g_n\right) = 0. \quad (2.4)$$

Teorema 2.3.1. *Se tiene* $\mathrm{H}^1(G,\ A) \cong \mathrm{Z}^1(G,\ A)/\mathrm{B}^1(G,\ A)$, *donde*

$$\mathrm{Z}^1(G,\ A) = \{f : G \to A \mid f(gh) = gf(h) + f(g) \text{ para todo } g, h \in G\}$$

y

$$\mathrm{B}^1(G,\ A) = \{f : G \to A \mid \text{existe } a \in A \text{ con } f(g) = ga - a \text{ para } g \in G\}.$$

En particular, si A *es un* G*-módulo trivial,* $\mathrm{H}^1(G,\ A) = \mathrm{Hom}(G,\ A)$.

Demostración: Se tiene $\mathrm{H}^1(G,\ A) = \ker \partial_2^*/\ \mathrm{im}\ \partial_1^*$. Ahora bien, por la ecuación (2.4)

$$\ker \partial_2^* = \{f : G \to A \mid gf(h) - f(gh) + f(g) = 0\} = \mathrm{Z}^1(G,\ A).$$

Ahora sea $f \in \mathrm{im}\,\partial_1^*$, esto es, $f = \partial_1^*(\varphi) = \varphi \circ \partial_1$ con $\varphi \in \mathrm{Hom}_G(P_0,\ A) \cong A$. Entonces $f(g) = \varphi \circ \partial_1([g])$. Sea $a = \varphi(1) \in A$, $f(g) = \varphi \circ \partial_1([g]) = \varphi(\partial_1(1,\ g)) = \varphi(g - 1) = \varphi(g) - \varphi(1) = g\varphi(1) - \varphi(1) = ga - a$.

Por lo tanto $\mathrm{im}\ \partial_1^* = \mathrm{B}^1(G,\ A)$.

En particular, si la acción de G es trivial, $ga - a = 0$ para toda $g \in G$, por lo tanto $\mathrm{B}^1(G,\ A) = \{0\}$ y $f \in \mathrm{Z}^1(G,\ A) \iff f(gh) = gf(h) + f(g) = f(g) + f(h)$ para todo $g, h \in G$, es decir, $f \in \mathrm{Hom}(G,\ A)$. ■

$\mathrm{Z}^1(G,\ A)$ es el grupo de los **homomorfismos cruzados o derivaciones de** G **en** A, y $\mathrm{B}^1(G, A)$ el grupo de los **homomorfismos cruzados principales o 1-cofrontera de** G **en** A.

Por otro lado, tenemos que $\mathrm{H}^2(G,\ A) = \mathrm{Z}^2(G,\ A)/\mathrm{B}^2(G,\ A)$.

Por la ecuación (2.4) se sigue que:

$$\mathrm{Z}^2(G, A) = \left\{ f : G^2 \to A \mid gf(h,\, m) - f(gh,\, m) + f(g,\, hm) - f(g,\, h) = 0 \right\}.$$

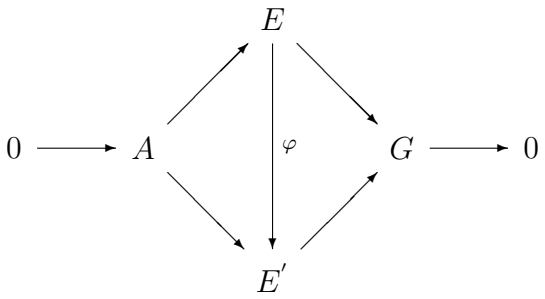
Un elemento $f \in \mathrm{Z}^2(G,\, A)$ se llama un **conjunto de factores de** G. Estos conjuntos nos determinan los grupos E tales que $A \triangleleft E$ y tal que $E/A \cong G$, donde A es un grupo abeliano. En otras palabras, nos determinan los grupos E dados por la sucesión exacta $0 \to A \to E \xrightarrow{\pi} G \to 0$ y tal que $g \in G$ actúa en A de la siguiente forma: si $g = \pi(e)$, $e \in E, g \circ a = eae^{-1}$. Como A es conmutativo, la acción de g no depende de $e \in E$.

Para ver cómo está determinado E, sea $s : G \to E$ una **sección**, esto es, s satisface $\pi \circ s = \mathrm{Id}_G$, s no necesariamente es un homomorfismo. Ahora, $\pi(s(g)s(h)) = (\pi s)(g)(\pi s)(h) = gh = (\pi s)(gh)$.

Por lo tanto $s(g)s(h)s(gh)^{-1} \in \ker \pi \cong A$, esto es, existe un elemento $f(g,\, h) \in A$ tal que $s(g)s(h) = f(g,\, h)s(gh)$ para cualquiera $g, h \in G$.

El conocimiento de $f : G^2 \to A$, $f(g,\, h)$, nos permite conocer E. Se puede verificar que f es un conjunto de factores.

Dos de tales extensiones, E y E', se llaman **equivalentes** si existe un isomorfismo $\varphi : E \to E'$ tal que el diagrama



es conmutativo.

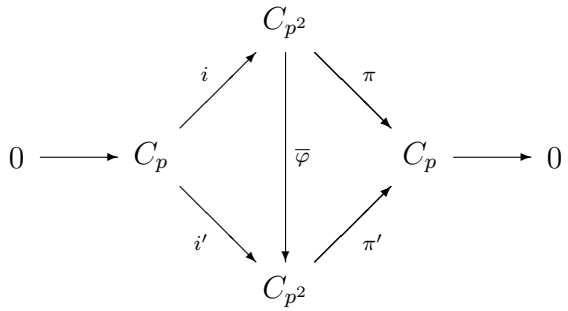
Esto es una relación de equivalencia y las clases de equivalencia están en correspondencia biyectiva con $\mathrm{H}^2(G,\ A)$.

Notemos que si E y E' son equivalentes, entonces son isomorfos, pero el recíproco no necesariamente se cumple.

En efecto en el siguiente ejemplo se hará patente lo dicho en la parte de arriba. Sea $A = C_p, G = C_p$ con acción trivial en A, donde C_p es el grupo cíclico de p elementos con $p > 2$. Entonces $\mathrm{H}^2(G,\ A) = C_p$, y sólo hay dos posibilidades para $E : E = C_p \times C_p$ o bien $E = C_{p^2}$.
En efecto, primeramente mostraremos que $\mathrm{H}^2(G,\ A) = C_p$. Por definicion, se tiene que $\mathrm{H}^2(G,\ A) \cong A^G/NA$, y como la acción es trivial $A^G = A$. Por otro lado, sea $x \in A$, así tenemos que

$$\begin{aligned} N_G(x) &= (1 + \sigma + \cdots + \sigma^{p-1})(x) = x + \sigma x + \cdots + \sigma^{p-1}x \\ &= x + x + \cdots + x = px. \end{aligned}$$

Por lo que se tiene que $\mathrm{H}^2(G,\ A) = A^G/NA = A^G/0 = A^G = A = C_p$. Ahora, sea E grupo tal que $A \triangleleft E$ y $E/A \cong G$, entonces $|E|/p = |E|/|A| = |E/A| = |G| = p$ por lo que $|E| = p^2$, luego se tiene que $E \cong C_{p^2}$ o $E \cong C_p \times C_p$.
Consideremos el siguiente diagrama:



donde definimos lo siguiente $A = \langle a\rangle$, $\circ(a) = p$, $G = \langle c\rangle$, donde $\circ(c) = p$, y, por último, $E = \langle b\rangle$, donde $\circ(b) = p^2$. Las siguientes funciones sobre los respectivos generadores están dadas por:
$i(a) = pb$ donde $\circ(pb) = p$, $i'(a) = 2pb$, $\pi(b) = c$, $\pi'(b) = c$ y notemos que $(\pi \circ i)(a) = \pi(pb) = pc = 0$ además $(\pi' \circ i')(a) = \pi'(2pb) = 2pc = 0$.

Ahora, supongamos que existe $\overline{\varphi}$ isomorfismo que hace al diagrama conmutativo. La conmutatividad del primer triángulo establece que $\overline{\varphi} \circ i = i'$, por lo que $(\overline{\varphi} \circ i)(a) = \overline{\varphi}(pb) = p\overline{\varphi}(b) = plb$ donde $(l\,, b) = 1$ y, como $i'(a) = 2pb$, entonces $2pb = plb$ lo cual implica que $2pb - plb = 0$; así la relación $p(2-l)b = 0$ implica que $p^2 | p(2-l)$, que a su vez implica que $p|(2-l)$. Por lo tanto, $l \equiv 2 \bmod p$.
Por otro lado, la conmutatividad del segundo triángulo nos dice que $\pi = \pi' \circ \overline{\varphi}$, luego $c = \pi(b) = \pi' \circ \overline{\varphi}(b) = \pi(lb) = lc$ entonces tenemos que $c = lc$, es decir $(1-l)c = 0$, lo cual implica que $p|(1-l)$. Así, $l \equiv 1 \bmod p$. Lo cual es una contradición. Por lo tanto, $\overline{\varphi}$ no es un isomorfismo.

2.4 Cohomología de Galois

En esta sección presentaremos algunos ejemplos de lo que es la cohomología de Galois.

Para esto, consideremos L/K una extensión finita de campos con grupo de Galois $\mathrm{Gal}(L/K) = G$. Entonces L y L^* son, de manera natural, G-módulos. Además, como L/K tiene una base normal, esto es, existe $\alpha \in L$ tal que $\{\sigma\alpha\}_{\sigma \in G}$ es base de L/K, tendremos que $L = \bigoplus_{\sigma \in G} K(\sigma\alpha) \cong K \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ como G-módulos. En particular, L es inducido. Así tenemos la siguiente proposición.

Proposición 2.4.1. *Se tiene* $\mathrm{H}_n(G,\, L) = 0$ *para todo* $n \geq 1$.

Demostración: Se sigue inmediatamente de Teorema 2.2.3 ■

De hecho, como se podrá observar en el Capítulo 3, se tiene $\hat{\mathrm{H}}^n(G,\, L) = 0$ para todo $n \in \mathbb{Z}$, donde $\hat{\mathrm{H}}^n(G,\, L)$ denota **los grupos de cohomología de Tate**, los cuales se definen en dicho capítulo.

Finalmente, tenemos el siguiente teorema.

Teorema 2.4.1 (Teorema 90 de Hilbert). *Se tiene que* $\mathrm{H}^1(G,\, L^*) = 0$.

Demostración: Sea $f \in \mathrm{Z}^1(G,\ L^*)$, esto es, $f : G \to L^*$ satisface $f(\theta\sigma) = \sigma(f(\theta))f(\sigma)$ para cualesquiera $\theta, \sigma \in G$.

Usando la independencia lineal de los automorfismos de L, se tiene que existe $x \in L^*$ tal que :

$$y = \sum_{\sigma \in G} f(\sigma)\sigma(x) \in L^*.$$

Luego, para $\theta \in G$,

$$\theta(y) = \sum_{\sigma \in G} (\theta f)\ (\sigma)\ (\theta\sigma)\ (x) = \sum_{\sigma \in G} f\ (\theta\sigma)\ f\ (\theta)^{-1}\ (\theta\sigma)\ (x) = f\ (\theta)^{-1}\ y.$$

Por lo tanto, f satisface $f\ (\theta) = \theta(y)^{-1}\ y \in \mathrm{B}^1(G,\ L^*)$, y de aquí que $\mathrm{H}^1(G,\ L^*) = 0$. ■

2.5 Extensiones de Artin-Schreier y de Kummer

Terminamos este capítulo abriendo un breve paréntesis para revisar algunos hechos básicos acerca de las extensiónes de Artin-Schreier y de Kummer, para lo cual empezamos con la siguiente definición.

Definición 2.5.1. *Sea F/K una extensión finita de campos con $F \subseteq \overline{K}$, donde $\overline{K}$ denota una cerradura algebraica de K. Sean $\{\sigma_1, \sigma_2, \cdots, \sigma_r\}$ todos los distintos $K-$monomorfismos F en $\overline{K}$.*
Si $u \in F$, la **norma** *de u, denotada por $N_{L/K}u$, es el elemento*

$$N_{L/K}u = (\sigma_1(u)\sigma_2(u)\cdots\sigma_r(u))^{\,[F:K]_i}.$$

La **traza** *de u, denotada por $Tr_{F/K}u$, es el elemento*

$$Tr_{F/K}u = [F : K]_i(\sigma_1(u) + \sigma_2(u) + \cdots + \sigma_r(u)).$$

Teorema 2.5.1. *Sea L/K una extensión cíclica de grado n y sea además $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$. Considere $\alpha \in L$. Entonces,*

(*i*) $Tr_{L/K}\alpha = 0$ *si y solamente si existe $\beta \in L$ tal que $\alpha = \beta - \sigma\beta$.*

(*ii*) $N_{L/K}\alpha = 1$ *si y solamente si existe $\beta \in L$ tal que $\alpha = \beta/\sigma\beta$.*

Demostración:

(*i*) Suponga que $\alpha = \beta - \sigma\beta$, entonces

$$Tr_{L/K}\alpha = Tr_{L/K}\beta - Tr_{L/K}(\sigma\beta) = Tr_{L/K}\beta - Tr_{L/K}\beta = 0.$$

Recíprocamente, ya que L/K es una extensión separable, existe $\gamma \in L$ tal que $Tr_{L/K}\gamma = a \neq 0$, con $a \in K$. Entonces, $Tr_{L/K}(a^{-1}\gamma) = a^{-1}\, Tr_{L/K}\gamma = 1$. Suponga que $Tr_{L/K}\alpha = 0$. Tenemos que $\sigma^0\alpha = -\sum_{j=1}^{n-1} \sigma^j\alpha$.

Si $\beta = a^{-1}\sum_{i=0}^{n-2}\left(\sum_{j=0}^{i}\sigma^j\alpha\right)\sigma^i\gamma$, entonces $\beta - \sigma\beta = \alpha$.

(*ii*) Esto es precisamente el Teorema 90 de Hilbert. ■

Teorema 2.5.2. (Extensiones de Artin-Schreier) *Suponga que la característica del campo K es $p > 0$. Entonces, L/K es una extensión cíclica de grado p si y solamente si existe $z \in L$ tal que $L = K(z)$ con $\mathrm{Irr}(z, T, K) = T^p - T - a \in K[T]$.*

Demostración: Sea $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$, con $o(\sigma) = p$. Entonces, $Tr_{L/K}\, 1 = p1 = 0$. Por el teorema anterior, existe $z \in L$ tal que $\sigma z - z = 1$ o $\sigma z = z + 1$. Por lo tanto, $\sigma^i z = z + i$ y $\sigma^i z = z$ si y solamente si $p \mid i$. Más aún,

$$\mathrm{Irr}(z, T, K) = \prod_{i=0}^{p-1}(T - (z + i))$$

es de grado p. Note que

$$\sigma(z^p - z) = (\sigma z)^p - \sigma z = (z+1)^p - (z+1) = z^p - z.$$

Por lo tanto,

$$z^p - z = a \in K \quad \text{y} \quad z^p - z - a = 0.$$

De esto se sigue que

$$\text{Irr}(z, T, K) = T^p - T - a \ \ (\text{y} \ \ T^p - T - a = \prod_{i=0}^{p-1}(T - (z+i)), \ \ a = z^p - z).$$

Recíprocamente, si $L = K(z)$ y $\text{Irr}(z, T, K) = T^p - T - a$, entonces para cualquier $i \in \mathbb{Z}$,

$$i^p \equiv i \bmod p \quad y \ \ (z+i)^p - (z+i) = z^p + i^p - z - i = z^p - z = a.$$

Más aún $z, z+1, \ldots, z+(p-1)$ son las raíces de $\text{Irr}(z, T, K)$. En particular, z y $z+1$ son conjugados sobre K y $L = K(z)$ es una extensión de Galois sobre K. Sea $G = \text{Gal}(L/K)$. Entonces, existe $\sigma \in G$ tal que $\sigma z = z + 1$. De aquí que, $\sigma^i z = z + i$ y $o(\sigma) = p$. Luego, $G = \langle \sigma \rangle$ es un grupo cíclico de orden p. ■

Teorema 2.5.3. (Extensiones de Kummer) *Supongamos que la característica del campo K es $p \geq 0$ y sea $n \in \mathbb{N}$ tal que $p \nmid n$ (n puede ser tomado arbitrariamente en caso de que $p = 0$). Suponga que el campo K contiene una raíz primitiva n-ésima de la unidad ζ_n. Entonces, L/K es una extensión cíclica de grado n si y solamente si existe $z \in L$ tal que $L = K(z)$ e*

$$\text{Irr}(z, T, K) = T^n - a \in K[T].$$

Demostración: Sean $G = \text{Gal}(L/K) = \langle \sigma \rangle$ y $o(\sigma) = n$. Tenemos que $N_{L/K}\zeta_n = \zeta_n^n = 1$. Entonces, tenemos que existe $z \in L$ tal que $\sigma z = \zeta_n z$. Ya que $\sigma^i z = \zeta_n^i z$ y $\sigma^i z = z$ si y solamente si $n|i$, se sigue que $z, \zeta_n z, \ldots, \zeta_n^{n-1} z$ son los diferentes conjugados de z. Entonces,

$$\text{Irr}(z, T, K) = \prod_{i=0}^{n-1}(T - \zeta_n^i z).$$

Por otro lado, $\sigma(z^n) = (\sigma z)^n = (\zeta_n z)^n = z^n$. Por lo tanto, $z^n = a \in K$ y $z, \zeta_n z, \ldots, \zeta_n^{n-1} z$ son las raíces de $T^n - a \in K[T]$. Más aún,

$$\mathrm{Irr}(z, T, K) = T^n - a \quad \text{y} \quad z^n = a \in K.$$

Recíprocamente, para $a \neq 0$, $T^n - a$ es un polinomio separable con raíces distintas $z, \zeta_n z, \ldots, \zeta_n^{n-1} z$, donde z es cualquier elemento de la cerradura algebraica $\overline{K}$ de K tal que $z^n = a$. Por lo tanto, $L = K(z)$ es una extensión normal y separable de K, y L/K es una extensión de Galois. Ahora, ya que $T^n - a$ es tomado como polinomio irreducible, z y $\zeta_n z$ son conjugados sobre K. Entonces, existe $\sigma \in G = \mathrm{Gal}(L/K)$ tal que $\sigma z = \zeta_n z$. De esto, se sigue que $o(\sigma) = n = o(G) = [L : K]$ y L/K es una extensión cíclica de grado n. ■

Ahora analizamos los casos cuando dos extensiones cíclicas L_1/K y L_2/K son o bien extensiones de Artin-Schreier o bien extensiones de Kummer.

Proposición 2.5.1. *Suponga que la característica de K es $p > 0$ y sean $L_i = /K$, $i = 1, 2$ dos extensiones cíclicas de grado p dadas por $z_i^p - z_i = a_i \in K$, $i = 1, 2$. Entonces, las siguientes relaciones son equivalentes:*

(i) $L_1 = L_2$;

(ii) $z_1 = j z_2 + b$ para $1 \leq j \leq p-1$ y $b \in K$;

(iii) $a_1 = j a_2 + (b^p - b)$ para $1 \leq j \leq p-1$ y $b \in K$.

Demostración: Si $z_1 = j z_2 + b$, entonces $z_2 = j' z_1 - j' b$ con $jj' \equiv 1 \bmod p$. Entonces, $L_1 = L_2$.
Recíprocamente, si $L_1 = L_2$, con $G = \mathrm{Gal}(L_1/K) = \mathrm{Gal}(L_2/K) = \langle \sigma \rangle$, entonces podemos elegir σ tal que $\sigma z_1 = z_1 + 1$. Ahora, ya que σz_2 es un conjugado de z_2 sobre K, tenemos que $\sigma z_2 = z_2 + j'$ con $1 \leq j' \leq p-1$. Sea $1 \leq j \leq p-1$ tal que $jj' \equiv 1 \bmod p$. Entonces,

$$\sigma(j z_2) = j \sigma z_2 = j z_2 + jj' = j z_2 + 1.$$

Por lo tanto, $\sigma(z_1 - j z_2) = z_1 - j z_2$. De esto se sigue que $z_1 - j z_2 = b \in K$. Continuando, si $z_1 = j z_2 + b$, entonces

$$z_1^p - z_1 = a_1 = (j z_2 + b)^p - (j z_2 + b) = j(z_2^p - z_2) + (b^p - b) = j a_2 + (b^p - b).$$

Recíprocamente, si $a_1 = ja_2 + (b^p - b)$ tenemos que $z_1^p - z_1 = (jz_2 + b)^p - (jz_2 + b)$, es decir,

$$(z_1 - (jz_2 + b))^p - (z_1 - (jz_2 + b)) = 0.$$

Se sigue que $\omega = z_1 - jz_2 - b$ es una raíz de la ecuación $\omega^p - \omega = 0$. Luego, $\omega \in \mathbb{F}_p$. Por lo tanto $z_1 = jz_2 + b'$, donde $b' = b + w \in K$. ■

Proposición 2.5.2. *Suponga que la característica del campo K es $p \geq 0$ y que K contiene una raíz n-ésima primitiva de la unidad ζ_n, con $(n,\ p) = 1$. Sean $L_i = K(z_i)$ con $i = 1, 2$, dos extensiones cíclicas de K de grado n, dadas por $z_i^n = a_i \in K$. Entonces, las siguientes relaciones son equivalentes:*

(*i*) $L_1 = L_2$.

(*ii*) $z_1 = z_2^j c$ para todo $1 \leq j \leq n-1$ tal que $(j,\ n) = 1$ y $c \in K$.

(*iii*) $a_1 = a_2^j c^n$ para todo $1 \leq j \leq n-1$ tal que $(j,\ n) = 1$ y $c \in K$.

Demostración: Suponga que $L_1 = L_2$, con $G = \mathrm{Gal}(L_1/K) = \mathrm{Gal}(L_2/K) = \langle\sigma\rangle$, tomando σ tal que $\sigma z_1 = \zeta_n z_1$. Ahora, σz_2 es un conjugado de z_2 sobre K, por lo que $\sigma z_2 = \zeta_n^{j'} z_2$ con $1 \leq j' \leq n-1$. Sea $d = (j',\ n)$. Entonces $\sigma^{n/d} z_2 = \zeta_n^{j'\, n/d} z_2 = z_2$, y por tanto $\sigma^{n/d} = Id$. Entonces, como $o(\sigma) = n$, tenemos que $d = (j',\ n) = 1$. Elegimos j tal que $jj' \equiv 1 \bmod n$. Entonces, $\sigma(z_2^j) = \zeta_n^{jj'} z_2^j = \zeta_n z_2^j$, y $\sigma(z_1 z_2^{-j}) = z_1 z_2^{-j}$, por lo que $z_1 z_2^{-j} = c \in K$. Recíprocamente, si $z_1 = z_2^j c \in L_2$, $(j,\ n) = 1$ y $c \in K$, entonces $L_1 \subseteq L_2$, y si $jj' \equiv 1 \bmod n$, entonces $z_1^j = z_2^{jj'} c^j = z_2^{i+\ell} c^j = z_2 a_2^\ell c^j$, por lo que $z_2 = z_1^j a_2^{-\ell} c^{-j} \in L_1$. Por lo tanto, $L_1 = L_2$.
Así pues, hemos probado la equivalencia de (*i*) y (*ii*). Por otro lado, (*ii*) implica (*iii*) se tiene por elevar a la n, ambos miembros, la ecuación $z_1 = z_2^j c$; mientras que, la recíproca, se obtiene por sacar raíz n-ésima la ecuación $a_1 = a_2^j c^n$, tomando en cuenta que $(j, n) = 1$ y que K contiene una raíz n-ésima primitiva de la unidad. ■

Capítulo 3

Cohomología de Tate

3.1 Grupos de Cohomología de Tate

Definición 3.1.1. *Sea G un grupo finito. El elemento $N = \sum_{\sigma \in G} \sigma \in \mathbb{Z}[G]$ recibe el nombre de* **norma**.

Para un G-módulo A, N define un endomorfismo de A dado por $Na = \sum_{\sigma \in G} \sigma a \in A$. Este endomorfismo también recibe el nombre de **norma** de A; en caso de considerar varios G-módulos, se distinguirán a las diferentes normas usadas por el símbolo N_A.

Sea $\mathrm{I}_G = \langle \sigma - 1 \mid \sigma \in G \rangle \subseteq \mathbb{Z}[G]$. Como hemos visto,

$$\mathrm{I}_G = \ker \ (\varepsilon : \mathrm{I}_G\mathbb{Z}[G] \to \mathbb{Z}), \quad \varepsilon\left(\sum_{\sigma \in G} a_\sigma \sigma\right) = \sum_{\sigma \in G} a_\sigma.$$

Ahora bien, si $\sigma \in G$, $N((\sigma - 1)\, a) = \sum_{\theta \in G} \sigma\theta a - \sum_{\theta \in G} \theta a = N_A - N_A = 0$, esto es, $\mathrm{I}_G A \subseteq \ker N$. Por otro lado, $N\sigma a = \sigma N a = Na$, por lo que $NA = \mathrm{im}\ N \subseteq A^G$.

Recordemos que $\mathrm{H}_0(G,\, A) = A/\mathrm{I}_G A$ y $\mathrm{H}^0(G,\, A) = A^G$, por lo que al pasar al cociente, N define un homomorfismo $N^* : \mathrm{H}_0(G,\, A) \to \mathrm{H}^0(G,\, A)$.

Definimos

$$\hat{\mathrm{H}}_0(G,\ A) = \ker\ N^* = \ker\ N/\mathrm{I}_G A, \quad \hat{\mathrm{H}}^0(G,\ A) = \operatorname{coker}\ N^* = A^G/NA.$$

Esto es, tenemos la sucesión exacta

$$0 \to \hat{\mathrm{H}}_0(G,\ A) \to \mathrm{H}_0(G,\ A) \xrightarrow{N_A^*} \mathrm{H}^0(G,\ A) \to \hat{\mathrm{H}}^0(G,\ A) \to 0.$$

Teorema 3.1.1. *Sea G un grupo finito y sea $0 \to A \to B \xrightarrow{\pi} C \to 0$ una sucesión exacta de G-módulos. Entonces, el diagrama*

$$\begin{array}{ccccccccc}
\mathrm{H}_1(G,\ C) & \xrightarrow{\varepsilon_0} & \mathrm{H}_0(G,\ A) & \longrightarrow & \mathrm{H}_0(G,\ B) & \longrightarrow & \mathrm{H}_0(G,\ C) & \longrightarrow & 0 \\
\downarrow & & \downarrow{\scriptstyle N_A^*} & & \downarrow{\scriptstyle N_B^*} & & \downarrow{\scriptstyle N_C^*} & & \downarrow \\
0 & \longrightarrow & \mathrm{H}^0(G,\ A) & \longrightarrow & \mathrm{H}^0(G,\ B) & \longrightarrow & \mathrm{H}^0(G,\ C) & \xrightarrow{\delta_0} & \mathrm{H}^1(G,\ A)
\end{array}$$

es conmutativo y las filas son exactas, donde ε_0 y δ_0 denotan los homomorfismos de conexión.

Demostración: Las filas son exactas por el Teorema 2.1.2. Por definición, la conmutatividad de los cuadrados interiores es clara. Para ver la conmutatividad de los cuadrados exteriores, usaremos la descripción explícita de ε_0 y δ_0.

Sólo verificaremos la exactitud en el cuadrado exterior, donde

$$\delta_0 : \mathrm{H}^0(G,\ C) = C^G \to \mathrm{H}^1(G,\ A) = \mathrm{Z}^1(G,\ A)/\mathrm{B}^1(G,\ A).$$

Sean $c \in C^G$ y $b \in B$ tales que $\pi(b) = c$. La función ∂b está dada por $(\partial b)(g) = gb - b \in A$, $g \in G$. Ahora, $\pi(gb - b) = g\pi(b) - \pi(b) = gc - c =$

$c-c=0$, por tanto $gb-b \in A$, y $\partial b \in \mathrm{Z}^1(G,\, A)$. Así, $\delta_0(c) = \partial b \bmod \mathrm{B}^1(G,\, A)$ "=" $\partial\pi^{-1}(c) \bmod \mathrm{B}^1(G,\, A)$. Se quiere probar que $\delta_0 \circ N_C^* = 0$.
Sea $x \in \mathrm{H}_0(G,\, C) = C/\,\mathrm{I}_G C$, digamos $x = c + \mathrm{I}_G C$, $N_C^* x = \sum_{\sigma\in G} \sigma c$. Entonces,

$$\delta_0(N_C^* x) \;=\; \delta_0\left(\sum_{\sigma\in G}\sigma c\right) \;=\; \sum_{\sigma\in G}\delta_0(\sigma c) \;=\; \sum_{\sigma\in G}\partial\pi^{-1}(\sigma c) \;=\; \sum_{\sigma\in G}\partial(\sigma b),$$

donde $\pi(b) = c$. Ahora,

$$\left(\sum_{\sigma\in G}\partial\,(\sigma b)\right)(g) = \sum_{\sigma\in G}(\partial\,(\sigma b)\,)(g) = \sum_{\sigma\in G}(g\sigma b - \sigma b) = Nb - Nb = 0,$$

para todo $g \in G$. Por tanto, $\delta_0 \circ N_C^* = 0$. ■

Corolario 3.1.1. *Existe un homomorfismo canónico* $\delta : \hat{\mathrm{H}}_0(G, C) \to \hat{\mathrm{H}}^0(G, A)$ *que hace exacta la sucesión*

$$\hat{\mathrm{H}}_0(G,\, A) \to \hat{\mathrm{H}}_0(G,\, B) \to \hat{\mathrm{H}}_0(G,\, C) \xrightarrow{\delta} \hat{\mathrm{H}}^0(G,\, A) \to \hat{\mathrm{H}}^0(G,\, B) \to \hat{\mathrm{H}}^0(G,\, C).$$

Demostración: Es simplemente el Lema de la Serpiente (Teorema 1.2.3) aplicado al Teorema 3.1.1 ■

Teorema 3.1.2. *δ nos da una sucesión exacta:*

$$\to \mathrm{H}_1(G,\, C) \xrightarrow{\varepsilon_0} \hat{\mathrm{H}}_0(G,\, A) \to \hat{\mathrm{H}}_0(G,\, B) \to \hat{\mathrm{H}}_0(G,\, C) \xrightarrow{\delta}$$
$$\xrightarrow{\delta} \hat{\mathrm{H}}^0(G,\, A) \to \hat{\mathrm{H}}^0(G,\, B) \to \hat{\mathrm{H}}^0(G,\, C) \xrightarrow{\delta_0} \mathrm{H}^1(G,\, A)$$

Demostración: Se tiene que

$$\begin{array}{ccc} \hat{\mathrm{H}}_0(G,\, A) & \subseteq & \mathrm{H}_0(G,\, A) \\ \| & & \| \\ \ker N_A/\, I_G A & \subseteq & \ker A/\, I_G A \end{array}$$

$$\hat{\mathrm{H}}^0(G,\, C) = \ker \mathrm{H}^0(G,\, C)/\,\mathrm{im}\, N_C^*.$$

Los mapeos de conexión $\varepsilon_0,\ \delta_0$ satisfacen $N_A^* \circ \varepsilon_0 = 0$, esto es,
$\mathrm{im}\,\varepsilon_0 \subseteq \ker N_A^*$ y $\delta_0 \circ N_C^* = 0$, es decir, $\mathrm{im}\, N_C^* \subseteq \ker \delta_0$, de donde se sigue inmediatamente el resultado. ■

Definición 3.1.2. *Sea G un grupo finito y sea A un G-módulo.Se definen los* ***grupos de cohomología de Tate*** *con exponentes en $\mathbb{Z}$ por:*

$$\begin{aligned}
\hat{\mathrm{H}}^n(G,\, A) &= \mathrm{H}^n(G,\, A) \quad \text{para} \quad n \geq 1,\\
\hat{\mathrm{H}}^0(G,\, A) &= A^G/\, NA,\\
\hat{\mathrm{H}}^{-1}(G,\, A) &= \ker N_A/\, I_G A,\\
\hat{\mathrm{H}}^{-n}(G,\, A) &= \mathrm{H}_{n-1}(G,\, A) \quad \text{para} \quad n \geq 2.
\end{aligned}$$

El Teorema 2.1.2 junto con el Teorema 3.1.1 nos dan:

Teorema 3.1.3. *Si $0 \to A \to B \to C \to 0$ es una sucesión exacta de G-módulos, entonces*

$$\begin{aligned}
\cdots \to \hat{\mathrm{H}}^{n-1}(G,\, C) \to \hat{\mathrm{H}}^n(G,\, A) \to \hat{\mathrm{H}}^n(G,\, B) \to\\
\to \hat{\mathrm{H}}^n(G,\, C) \to \hat{\mathrm{H}}^{n+1}(G,\, A) \to \cdots
\end{aligned}$$

es exacta para todo $n \in \mathbb{Z}$. ■

3.2 Cohomología de Grupos Cíclicos

Sea G un grupo cíclico finito de orden n, digamos que $G = \langle \sigma \rangle$. Sean $N = \sum_{i=0}^{n-1} \sigma^i$, $D = \sigma - 1$. Entonces,

$$ND \;=\; DN \;=\; \left(\sum_{i=0}^{n-1} \sigma^i\right)(\sigma - 1) = \sum_{i=1}^{n} \sigma^i - \sum_{i=0}^{n-1} \sigma^i = \sigma^n - 1 = 0.$$

Además, $\mathrm{I}_G = \langle g - 1 \mid g \in G \rangle = \langle \sigma^i - 1 = (\sigma - 1)(1 + \sigma + \cdots + \sigma^{i-1}) \mid i \in \mathbb{Z} \rangle = \langle \sigma - 1 \rangle = D\,\mathbb{Z}[G]$.

Se tiene que $N : \mathbb{Z}[G] \to \mathbb{Z}[G]$, $D : \mathbb{Z}[G] \to \mathbb{Z}[G]$. Entonces, tenemos lo siguiente.

Proposición 3.2.1. *Se tiene que* $\ker N = I_G = \operatorname{im} D$ y $\ker D = \mathbb{Z}[G]^G = \operatorname{im} N$.

Demostración: Puesto que $ND = 0$ y $DN = 0$, se sigue que $\operatorname{im} D \subseteq \ker N$ e $\operatorname{im} N \subseteq \ker D$.
Recíprocamente, si $s = \sum_{i=0}^{n-1} a_i\sigma^i \in \ker N$, se tiene que:

$$\begin{aligned} Ns &= \sum_{j=0}^{n-1} \sigma^j s = \sum_{j=0}^{n-1} \sigma^j \left(\sum_{i=0}^{n-1} a_i\sigma^i \right) \\ &= \sum_{i=0}^{n-1} a_i \left(\sum_{j=0}^{n-1} \sigma^{i+j} \right) = \sum_{i=0}^{n-1} a_i \left(\sum_{j=0}^{n-1} \sigma^j \right) \\ &= \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} a_i \right) \sigma^j = 0 \end{aligned}$$

$$\iff \sum_{i=0}^{n-1} a_i \iff s \in \mathrm{I}_G = D\,\mathbb{Z}[G] = \operatorname{im} D.$$

Por otro lado, $s \in \ker D \iff (\sigma - 1)\, s = \sigma s - s = 0 \iff \sigma s = s \iff s \in \mathbb{Z}[G]^G$.
Sea $s = \sum_{i=0}^{n-1} a_i\sigma^i \in \mathbb{Z}[G]^G$. Entonces, $\sigma s = \sum_{i=0}^{n-1} a_i\sigma^{i+1} = \sum_{i=0}^{n-1} a_{i-1}\sigma^i$, con $a_{-1} = a_{n-1}$. Por tanto, $\sigma s = s$ implica $a_i = a_{i-1}$, $i = 0, 1, ..., n-1$, esto es, $a_i = a \in \mathbb{Z}$ para toda i. Es decir, tenemos $s = a \left(\sum_{i=0}^{n-1} \sigma^i \right) = N(a \cdot 1) \in \operatorname{im} N$. ■

Sea $T_i = \mathbb{Z}[G]$, $i = 0, 1, \ldots$ y sea $\partial_i : T_i \to T_{i-1}$, donde

$$\partial_i = \begin{cases} D & \text{si } i \text{ es impar} \\ N & \text{si } i \text{ es par} \end{cases}$$

Sea $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$ el homomorfismo $\varepsilon \left(\sum_{i=0}^{n-1} a_i\sigma^i \right) = \sum_{i=0}^{n-1} a_i$.

Proposición 3.2.2. *La sucesión de G-módulos*

$$\cdots \to T_i \xrightarrow{\partial_i} T_{i-1} \to \cdots \to T_1 \xrightarrow{\partial_1} T_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

es exacta.

Demostración: Si i es par, $\ker \partial_i = \ker N = \operatorname{im} D = \operatorname{im} \partial_{i+1}$. Si i es impar, $\ker \partial_i = \ker D = \operatorname{im} N = \operatorname{im} \partial_{i+1}$. Finalmente, ε es suprayectiva y $\ker \varepsilon = \mathrm{I}_G = \operatorname{im} D = \operatorname{im} \partial_1$. ■

Se tiene que la sucesión $\{T_i,\ \partial_{i+1}\}_{i=0}^{\infty}$ es una resolución de $\mathbb{Z}$ cuando G es grupo cíclico finito. Por tanto, para un G-módulo A, obtenemos en cohomología:

$$0 \to \operatorname{Hom}_G(T_0,\ A) \xrightarrow{D^*} \operatorname{Hom}_G(T_1,\ A) \xrightarrow{N^*} \cdots$$

Ahora, $\operatorname{Hom}_G(T_i,\ A) = \operatorname{Hom}_G(\mathbb{Z}[G],\ A) \cong A$, con lo cual obtenemos:

$$0 \to A \xrightarrow{D^*} A \xrightarrow{N^*} A \xrightarrow{D^*} \cdots,$$

donde

$$D^*a = Da = (\sigma - 1)(a) = \sigma a - a,\ \ N^*a = Na = \sum_{i=0}^{n-1} \sigma^i a.$$

Luego, se tiene que:

$$\hat{\mathrm{H}}^{2n-1}(G,\ A) = \mathrm{H}^{2n-1}(G,\ A) = \frac{\ker N^*}{\operatorname{im} D^*} = \frac{\ker N_A}{DA} = \hat{\mathrm{H}}^{-1}(G,\ A)\,,$$

$$\hat{\mathrm{H}}^{2n}(G,\ A) = \mathrm{H}^{2n}(G,\ A) = \frac{\ker D^*}{\operatorname{im} N^*} = \frac{A^G}{NA} = \hat{\mathrm{H}}^{0}(G,\ A),$$

para $n = 1, 2...$

Similarmente, para la homología obtenemos: $T_i \otimes_G A \cong \mathbb{Z}[G] \otimes_G A \cong A$ y

$$\cdots \xrightarrow{N^*} A \xrightarrow{D^*} A \to 0\,,$$

por lo que se tiene

$$\hat{\mathrm{H}}^{-2n}(G,\ A) = \mathrm{H}_{2n-1}(G,\ A) = \frac{\ker D^*}{\operatorname{im} N^*} = \frac{A^G}{NA} = \hat{\mathrm{H}}^{0}(G,\ A)\,,$$

$$\begin{aligned}\hat{\mathrm{H}}^{-(2n+1)}(G,\ A) &= \mathrm{H}_{2n}(G,\ A) = \frac{\ker N^*}{\operatorname{im} D^*} = \frac{\ker N_A}{DA} \\ &= \hat{\mathrm{H}}^{-1}(G,\ A) = \hat{\mathrm{H}}^1(G,\ A),\end{aligned}$$

para $n = 1, 2, \ldots$

Así, hemos obtenido el siguiente resultado.

Teorema 3.2.1. *Sea G un grupo cíclico finito. Entonces se tiene para cualquier G-módulo A*

$$\hat{\mathrm{H}}^{2n}(G,\ A) \cong \hat{\mathrm{H}}^0(G,\ A) = \frac{A^G}{NA}\,,$$

$$\hat{\mathrm{H}}^{2n+1}(G,\ A) \cong \hat{\mathrm{H}}^{-1}(G,\ A) = \frac{\ker N_A}{DA}\,,$$

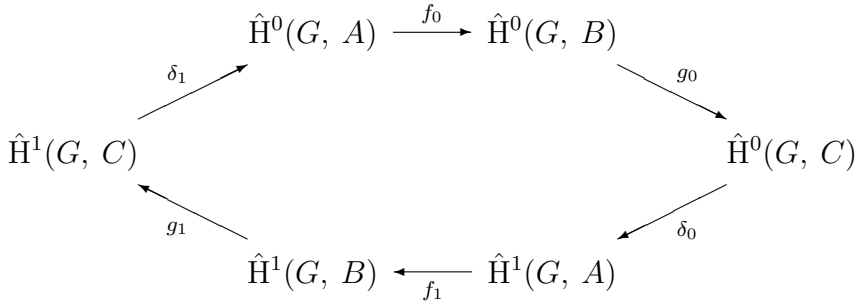
para $n \in \mathbb{Z}$. ■

3.3 El Cociente de Herbrand

Definición 3.3.1. *Sea G un grupo cíclico finito, y sea A un G-módulo tal que $\hat{\mathrm{H}}^0(G,\ A)$ y $\hat{\mathrm{H}}^1(G,\ A)$ son finitos, digamos de órdenes $h_0(A)$ y $h_1(A)$, respectivamente. Se define* **el cociente de Herbrand de A** *por*

$$h(A) = \frac{h_0(A)}{h_1(A)}\,.$$

Teorema 3.3.1. *Sea* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *una sucesión exacta de* G*-módulos. Entonces, se tiene el hexágono exacto*



y si dos de $h(A), h(B), h(C)$ *están definidos, entonces el tercero está definido, y se tiene que* $h(B) = h(A)h(C)$.

Demostración: El hexágono es simplemente la sucesión exacta del Teorema 3.1.3 y la ciclicidad de la cohomología de Tate cuando G es cíclico finito, Teorema 3.2.1.
Ahora, digamos que $h(A)$ y $h(B)$ están definidos. Entonces, se tiene que $h_0(C) \leq h_0(B)h_1(A) < \infty$ y $h_1(C) \leq h_1(B)h_0(A) < \infty$. Por lo tanto, $h(C)$ está definido.
También $h_0(B) = \,|\, \hat{\mathrm{H}}^0(G,\, B) \,|\, = \,|\, \mathrm{im}\, g_0 \,|\, |\, \ker g_0 \,|$. Similarmente, para los demás obtenemos:

$$h(B) = \frac{h_0(B)}{h_1(B)} = \frac{|\, \mathrm{im}\, g_0 \,|\, |\, \ker g_0 \,|}{|\, \mathrm{im}\, g_1 \,|\, |\, \ker g_1 \,|}\,,$$

$$h(A)h(C) = \frac{h_0(A)}{h_1(A)}\frac{h_0(C)}{h_1(C)} = \frac{|\, \mathrm{im}\, f_0 \,|\, |\, \ker f_0 \,|}{|\, \mathrm{im}\, f_1 \,|\, |\, \ker f_1 \,|}\frac{|\, \mathrm{im}\, \delta_0 \,|\, |\, \ker \delta_0 \,|}{|\, \mathrm{im}\, \delta_1 \,|\, |\, \ker \delta_1 \,|}. \qquad (3.1)$$

De la exactitud del hexágono obtenemos que $|\, \mathrm{im}\, \delta_1 \,| \,=\, |\, \ker f_0 \,|\,, |\, \mathrm{im}\, f_0 \,| \,=\, |\, \ker g_0 \,|\,, |\, \mathrm{im}\, g_0 \,| \,=\, |\, \ker \delta_0 \,|$, etc. Ahora, sustituyendo estos últimos valores en la ecuación (3.1), se tiene la igualdad. ■

Proposición 3.3.1. *Si* A *es un* G*-módulo finito, entonces* $h(A) = 1$.

Demostración: Se tiene que

$$0 \to A^G = \ker D_A \to A \xrightarrow{D} A \to A/\, DA = A_G \to 0$$

es exacta. Por lo tanto, $\mid A_G \mid \; = \; \mid A^G \mid$ y

$$0 \to \hat{\mathrm{H}}^1(G, A) = \ker N^* \to \mathrm{H}_0(G, A) = A_G \xrightarrow{N^*} \mathrm{H}^0(G, A) = A^G \to \hat{\mathrm{H}}^0(G, A) \to 0$$

es exacta. Por lo tanto, $h_1(A) = h_0(A)$. ■

Corolario 3.3.1. *Si A y B son G-módulos y $f : A \to B$ es un G-homomorfismo tal que* $\ker f$ y $\operatorname{coker} f$ *son finitos, entonces $h(A)$ está definido $\iff$ $h(B)$ está definido, y $h(A) = h(B)$ en este caso.*

Demostración: Se tiene que $0 \to \ker f \to A \xrightarrow{f} \operatorname{im} f \to 0$ es exacta y, por lo tanto, $h(A)$ está definido $\iff h(\operatorname{im} f)$ lo está.
Ahora $0 \to \operatorname{im} f \to B \to \operatorname{coker} f \to 0$ es exacta y, por lo tanto, $h(B)$ está definido $\iff h(\operatorname{im} f)$ está definido $\iff h(A)$ está definido.
En este caso, $h(A) = h(\ker f)h(\operatorname{im} f) = h(\operatorname{im} f) = \dfrac{h(B)}{h(\operatorname{coker} f)} = h(B)$. ■

Capítulo 4

Aplicaciones

En este capítulo presentamos algunas aplicaciones de lo estudiado hasta ahora.

4.1 Algunos Resultados Generales y Ejemplos

Proposición 4.1.1. *Sea $G = \langle \sigma \rangle$ un grupo cíclico finito de orden n. Entonces los G-módulos $\mathbb{Z}[x]/(x^n - 1)$ y $\mathbb{Z}[G]$ son isomorfos, donde la acción de σ en $\mathbb{Z}[x]/(x^n - 1)$ está dada por la multiplicación:*

$$\sigma \left(f(x) \bmod (x^n - 1) \right) = x\, f(x) \bmod (x^n - 1).$$

Demostración: Veamos que la acción de G está bien definida, es decir no depende de los representantes de la clase. Sean $f(x) \bmod (x^n - 1)$, $g(x) \bmod (x^n - 1) \in \mathbb{Z}[x]/(x^n - 1)$ tales que

$$g(x) \bmod (x^n - 1) = f(x) \bmod (x^n - 1),$$

Ahora sea $h \in \langle \sigma \rangle$. Entonces $h = \sigma^j$ para $0 \leq j \leq n-1$, luego de lo anterior tenemos $(x^n - 1) \mid g(x) - f(x)$ entonces $g(x) - f(x) = (x^n - 1)q(x)$ con

$q(x) \in \mathbb{Z}[x]$. Entonces

$$x^j\, g(x) \bmod (x^n - 1) = x^j\, f(x) \bmod (x^n - 1)$$

Así, la acción está bien definida.
Por otro lado, veamos que $\mathbb{Z}[x]/(x^n - 1)$ es efectivamente un G-módulo. Si 1 es la identidad del grupo G tenemos que:

$$1\ (\ f(x) \bmod (x^n - 1)\ ) = \ f(x) \bmod (x^n - 1).$$

Ahora sean $\alpha, \beta \in G$ entonces $\alpha = \sigma^j, \beta = \sigma^i$ para $0 \leq j, i \leq n-1$ y $g(x) \bmod (x^n - 1) \in \mathbb{Z}[x]/(x^n - 1)$. Se tiene

$$\alpha\, g(x) \bmod (x^n - 1) \ = \ \sigma^j\, g(x) \bmod (x^n - 1) = \ x^j\, g(x) \bmod (x^n - 1).$$

Definimos $h(x) \ = \ x^j\, g(x)$. Entonces

$$\begin{aligned} \beta\, h(x) \bmod (x^n - 1) &= \sigma^i\, h(x) \bmod (x^n - 1) \ = \ x^i\ (\ h(x) \bmod (x^n - 1)) \\ &= x^i (x^j\, g(x)) \bmod (x^n - 1) \\ &= (x^{i+j})\, g(x) \bmod (x^n - 1) \\ &= (\beta\, \alpha)\, g(x) \bmod (x^n - 1). \end{aligned}$$

Por lo tanto

$$\beta\ (\ \alpha\, g(x) \bmod (x^n - 1)) \ = \ (\beta\, \alpha)\, g(x) \bmod (x^n - 1).$$

Finalmente sean $f(x) \bmod (x^n - 1), g(x) \bmod (x^n - 1) \in \mathbb{Z}[x]/(x^n - 1)$ y $\gamma \in G$ entonces $\gamma = \sigma^i$ para algún $0 \leq i \leq n-1$, notemos que:

$$f(x) \bmod (x^n - 1) \ + \ g(x) \bmod (x^n - 1) \ = \ (f(x) + g(x)) \bmod (x^n - 1).$$

Por otro lado, tenemos que

$$\begin{aligned} \gamma\, (f(x) + g(x)) \bmod (x^n - 1) &= \sigma^i\, (f(x) + g(x)) \bmod (x^n - 1) \\ &= (\sigma^i\, f(x) \ + \sigma^i\, g(x)\ ) \bmod (x^n - 1) \\ &= x^i\, f(x) \bmod (x^n - 1) \\ &\quad + x^i\, g(x) \bmod (x^n - 1). \end{aligned}$$

Por lo tanto

$$\gamma\,(f(x)+g(x)) \bmod (x^n-1) \;=\; \gamma\, f(x) \bmod (x^n-1) \;+\; \gamma\, g(x) \bmod (x^n-1).$$

Lo anterior muestra que $\mathbb{Z}[x]/(x^n-1)$ es un G-módulo.
Resta por mostrar que este módulo y $\mathbb{Z}[G]$ son isomorfos. Para esto definamos el epimorfismo $\rho : \mathbb{Z}[x] \to \mathbb{Z}[G]$ dado por:
Para $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m \in \mathbb{Z}[x]$, se define $\rho(f(x)) = a_0 + a_1\sigma + a_2\sigma^2 + \cdots + a_m\sigma^m$.
Ahora sean $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m, g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_kx^k \in \mathbb{Z}[x]$, con $k\,,\, m \in \mathbb{Z},\ k \geq m \geq 0$. Se tiene

$$\begin{aligned}
\rho(f(x)+g(x)) &= \rho((a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots \\
&\quad +(a_m+b_m)x^m+\cdots+b_kx^k \\
&= (a_0+b_0)+(a_1+b_1)\sigma+(a_2+b_2)\sigma^2+\cdots \\
&\quad +(a_m+b_m)\sigma^m+\cdots+b_k\sigma^k \\
&= (\,a_0+a_1\sigma+a_2\sigma^2+\cdots+a_m\sigma^m) \\
&\quad +(b_0+b_1\sigma+b_2\sigma^2+\ldots+b_k\sigma^k) \\
&= \rho(f(x))+\rho(g(x)).
\end{aligned}$$

Para el producto, escribimos los polinomios de la siguiente manera $f(x) = \sum_{i=0}^{m} a_ix^i,\ \ g(x) = \sum_{j=0}^{k} b_kx^k$. Entonces tenemos que $\left(\sum_{i=0}^{m} a_ix^i\right)\left(\sum_{j=0}^{k} b_kx^k\right) = \sum_{l=0}^{m+k} c_lx^l$ donde $c_l = \sum_{i+j=l} a_ib_j$. Así que

$$\begin{aligned}
\rho(f(x)g(x)) &= \rho\left(\left(\sum_{i=0}^{m} a_ix^i\right)\left(\sum_{j=0}^{k} b_kx^k\right)\right) = \rho\left(\sum_{l=0}^{m+k} c_lx^l\right) = \sum_{l=0}^{m+k} c_l\sigma^l \\
&= \left(\sum_{i=0}^{m} a_i\sigma^i\right)\left(\sum_{j=0}^{k} b_k\sigma^k\right) = \rho\left(\sum_{i=0}^{m} a_ix^i\right)\rho\left(\sum_{j=0}^{k} b_kx^k\right) \\
&= \rho(f(x))\rho(g(x)).
\end{aligned}$$

Por lo que ρ es homomorfismo de anillos.

Veamos que es epimorfismo. Sea $r_0+r_1\sigma+r_2\sigma^2+\cdots+r_n\sigma^n \in \mathbb{Z}[G]$. Entonces el polinomio $h(x) = r_0 + r_1x + r_2x^2 + \cdots + r_nx^n \in \mathbb{Z}[x]$ es tal que $\rho(h(x)) = r_0 + r_1\sigma + r_2\sigma^2 + \cdots + r_n\sigma^n$.
Por ver que $\ker\rho = \langle x^n - 1\rangle$. Se tiene

$$\langle x^n - 1\rangle = \{(x^n - 1)q(x) \mid q(x) \in \mathbb{Z}[x]\}.$$

Sea $(x^n - 1)h(x) \in \langle x^n - 1\rangle$, luego

$$\rho((x^n - 1)h(x)) = (\sigma^n - 1)h(\sigma) = 0h(\sigma) = 0.$$

entonces $\langle x^n - 1\rangle \subseteq \ker\rho$.
Recíprocamente, sea $q(x) \in \ker\rho$. Entonces debemos probar que $q(x) = (x^n - 1)r(x)$ con $r(x) \in \mathbb{Z}[x]$. Se tiene que $\rho(q(x)) = q(\sigma) = 0$. Ahora, aplicando el algoritmo de la division, tenemos que $q(x) = (x^n - 1)r(x) + t(x)$ donde $t(x) = 0$ o $\operatorname{gr} t(x) < n$. Entonces

$$0 = q(\sigma) = (\sigma^n - 1)r(\sigma) + t(\sigma) = 0r(\sigma) + t(\sigma).$$

Se sigue que $t(\sigma) = 0$ y, por lo tanto, $t(x) = 0$ y $\ker\rho \subseteq \langle x^n - 1\rangle$. Así, $\ker\rho = \langle x^n - 1\rangle$. Por el Primer Teorema de Isomorfismo, obtenemos que $\mathbb{Z}[x]/(x^n - 1) \cong \mathbb{Z}[G]$ como anillos.
Ahora bien el isomorfismo $\overline{\rho} : \mathbb{Z}[x]/(x^n - 1) \to \mathbb{Z}[G]$ está dado por

$$\overline{\rho}(f(x) \bmod (x^n - 1)) = f(\sigma),$$

y se tiene que $\sigma^i \cdot f(x) \bmod (x^n - 1) = x^i \cdot f(x) \bmod (x^n - 1)$, o sea $\sigma^i \cdot f(x) \bmod (x^n - 1) = \overline{\rho}^{\,-1}(\sigma^i f(\sigma))$. Por lo tanto $\mathbb{Z}[x]/(x^n - 1) \cong \mathbb{Z}[G]$, como G-módulos. ■

Proposición 4.1.2. *Sea G un p-grupo finito y sea A un G-módulo cuyo orden es una potencia de p, entonces $A^G = \{0\}$ implica que $A = \{0\}$.*

Demostración: Supongamos que $A \neq 0$ luego existe $a \in A, a \neq 0$. El submódulo $A' \subseteq A$ generado por a es finito, de orden una potencia de p. Consideremos las órbitas de los elementos de A', estas órbitas tienen orden una potencia de p, pues el orden de G es una potencia de p y notemos que al menos existe un punto fijo a saber el 0 pues, si $g \in G$ es cualquier elemento de G tenemos que $g \circ 0 = 0$ luego la órbita de 0 que consta sólo de 0, tiene orden 1.

Ahora pongamos $A' = \bigcup_{y \in A'} \text{orb}(y)$ entonces

$$p^r = |A'| = \sum_{y \in A'} |\text{orb}(y)| = \sum_{e \neq y \in A'} |\text{orb}(y)| + |\text{orb}(0)| = \sum_{e \neq y \in A'} |\text{orb}(y)| + 1.$$

Ya que cada $|\text{orb}(y)|$ es una potencia de p, para que la igualdad anterior sea cierta se necesita que existan al menos otros $p-1$ puntos fijos además de 0, y por lo tanto existen al menos p puntos fijos de tal forma que $A^G \neq 0$. ■

Ejemplo 4.1.1. Sean G un grupo, H subgrupo normal de G y A un G-módulo. Considere la función

$$\text{Res} : \text{H}^1(G,\ A) \longrightarrow \text{H}^1(H,\ A)$$

definida como sigue: si $f \in \text{H}^1(G,\ A)$ y $\chi \in \text{Z}^1(G,\ A)$ es tal que $\chi \bmod \text{B}^1(G,\ A) = f$, con $\chi : G \to A$ entonces Res $f = \chi_{|_H} \mod \text{B}^1(H,\ A)$. Entonces Res es un homomorfismo de grupos.

El homomorfismo **Res** es el llamado **homomorfismo restricción.**

Mostremos que en efecto la función Res es un homomorfismo. Para esto, primero veremos que la función está bien definida, es decir, que no depende del representante de la clase; pero antes notemos que obviamente Res $f \in \text{H}^1(H,\ A)$.
Ahora sean $F_1, F_2 \in \text{H}^1(G,\ A)$ con $F_1 = F_2$ luego por definición existen $\alpha, \beta \in \text{Z}^1(G,\ A)$ tales que

$$F_1 = \alpha \bmod \text{B}^1(G,\ A) = \beta \bmod \text{B}^1(G,\ A) = F_2$$

lo cual implica

$$(\alpha - \beta) \bmod \text{B}^1(G,\ A) = 0$$

que a su vez implica

$$(\alpha - \beta) \in \text{B}^1(G,\ A)$$

entonces por definición de $\mathrm{B}^1(G,\ A)$ existe $a \in A$ tal que

$$(\alpha - \beta)(g) = ga - a \qquad \text{para todo } g \in G.$$

Así que, restringiendo $\alpha - \beta$ a H mod $\mathrm{B}^1(H,\ A)$ es decir

$$(\alpha - \beta)_{|_H}(h) \bmod \mathrm{B}^1(H,\ A) = 0 \qquad \text{para todo } h \in H,$$

lo cual implica que

$$(\alpha - \beta)_{|_H} \bmod \mathrm{B}^1(H,\ A) = 0$$

que a su vez implica

$$\mathrm{Res}\, F_1 = \alpha_{|_H} \bmod \mathrm{B}^1(H,\ A) = \beta_{|_H} \bmod \mathrm{B}^1(H,\ A) = \mathrm{Res}\, F_2,$$

luego la función Res está bien definida.
Mostremos ahora que Res es un homomorfismo de grupos. En efecto, sean $f_1, f_2 \in \mathrm{H}^1(G,\ A)$, luego existen $\gamma, \delta \in \mathrm{Z}^1(G,\ A)$ tales que $f_1 = \gamma$ mod $\mathrm{B}^1(G,\ A)$, $f_2 = \delta$ mod $\mathrm{B}^1(G,\ A)$. Así tenemos

$$\begin{aligned} \mathrm{Res}\,(f_1 + f_2) &= (\gamma + \delta)_{|_H} \bmod \mathrm{B}^1(H,\ A) \\ &= \gamma_{|_H} \bmod \mathrm{B}^1(H,\ A) + \delta_{|_H} \bmod \mathrm{B}^1(H,\ A) \\ &= \mathrm{Res}\, f_1 + \mathrm{Res}\, f_2. \end{aligned}$$

Ejemplo 4.1.2. Con la notación del ejemplo anterior, sea

$$\mathrm{Inf}\ : \mathrm{H}^1(G/H,\ A^H) \longrightarrow \mathrm{H}^1(G,\ A)$$

definida como sigue: para $f \in \mathrm{H}^1(G/H,\ A^H)$ y $\chi \in \mathrm{Z}^1(G/H,\ A)$ tal que $\chi \bmod \mathrm{B}^1(G/H,\ A^H) = f$, con $\chi : G/H \to A^H$, definimos $\mathrm{Inf}\,(f) = \chi \circ \pi \bmod \mathrm{B}^1(G,\ A)$ donde $\pi : G \to G/H$ es la proyección natural. Entonces Inf es un homomorfismo de grupos.

El homomorfismo **Inf** es el llamado **homomorfismo inflación.**

Al igual que en el ejemplo anterior, mostraremos aquí que Inf es un homomorfismo de grupos.

Notemos que A^H es un (G/H)-módulo mediante la acción dada por $(gH)a := ga$ pues si $a \in A^H$ y $g_1H = g_2H$, entonces $g_1 = g_2h$ para algún $h \in H$ y $g_1a = g_2ha = g_2a$, es decir $(gH)a$ no depende del representante. Ahora veamos que $gHa \in A^H$.
Sea $h \in H$ arbitrario. Así

$$h(ga) = (hg)a = (gh')a = ga \qquad (\text{ya que } gH = Hg).$$

Veamos primero que $\text{Inf}\,(f) \in \text{H}^1(G,\ A)$ con $f \in \text{H}^1(G/H,\ A^H)$, donde $f = \chi \bmod \text{B}^1(G/H,\ A^H)$ y $\chi \in \text{Z}^1(G/H,\ A^H)$. Si $g_1, g_2 \in G$ entonces

$$\begin{aligned} \chi \circ \pi(g_1g_2) &= \chi(g_1g_2H) = \chi(g_1Hg_2H) \\ &= g_1H\chi(g_2H) + \chi(g_1H) \\ &= g_1\chi \circ \pi(g_2) + \chi \circ \pi(g_1). \end{aligned}$$

Por tanto tenemos que $\chi \circ \pi \bmod \text{B}^1(G,\ A) \in \text{H}^1(G,\ A)$ como se quería.
Por otro lado, la función Inf está bien definida, es decir que no depende del representante de la clase. Para verificar esto consideremos $f_1, f_2 \in \text{H}^1(G/H,\ A^H)$ con $f_1 = f_2$ luego, por definición, existen $\varsigma, \tau \in \text{Z}^1(G/H,\ A)$ tales que

$$f_1 = \varsigma \bmod \text{B}^1(G/H,\ A^H) = \tau \bmod \text{B}^1(G/H,\ A^H) = f_2$$

lo cual implica que

$$(\varsigma - \tau) \bmod \text{B}^1(G/H,\ A^H) = 0$$

que a su vez implica que

$$(\varsigma - \tau) \in \text{B}^1(G/H,\ A^H).$$

Entonces, por definición de $\text{B}^1(G/H,\ A^H)$, existe $a \in A^H$ tal que

$$(\varsigma - \tau)(gH) = gHa - a = ga - a \qquad \text{para todo } gH \in G/H$$

lo cual implica

$$(\varsigma - \tau) \circ \pi \bmod \mathrm{B}^1(G,\ A) = 0$$

que a su vez implica

$$\mathrm{Inf}\ f_1 = \varsigma \circ \pi \bmod \mathrm{B}^1(G,\ A) = \tau \circ \pi \bmod \mathrm{B}^1(G,\ A) = \mathrm{Inf}\ f_2$$

es decir la función Inf está bien definida.
Finalmente, sean $t_1, t_2 \in \mathrm{H}^1(G/H,\ A^H)$, luego existen $\psi, \lambda \in \mathrm{Z}^1(G/H,\ A^H)$ tales que $t_1 = \psi \bmod \mathrm{B}^1(G/H,\ A^H),\ t_2 = \lambda \bmod \mathrm{B}^1(G/H,\ A^H)$. Así tenemos

$$\begin{aligned} \mathrm{Inf}\ (t_1 + t_2) &= (\psi + \lambda) \circ \pi \bmod \mathrm{B}^1(G,\ A) \\ &= \psi \circ \pi \bmod \mathrm{B}^1(G,\ A) + \lambda \circ \pi \bmod \mathrm{B}^1(G,\ A) \\ &= \mathrm{Inf}\ t_1 + \mathrm{Inf}\ t_2. \end{aligned}$$

Proposición 4.1.3. (Sucesión Espectral de Hoschild-Serre) *Con la notación de los dos ejemplos anteriores se tiene que la sucesión*

$$0 \to \mathrm{H}^1(G/H,\ A^H) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1(G,\ A) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(H,\ A)$$

es exacta.

Demostración: En efecto, veremos a continuación que Inf es inyectiva. Suponga que $\mathrm{Inf}(f) = 0$ para $f \in \mathrm{H}^1(G/H,\ A^H)$. Entonces existe $\rho \in \mathrm{Z}^1(G/H,\ A^H)$ tal que $f = \rho \bmod \mathrm{B}^1(G/H,\ A^H)$ y por tanto $\mathrm{Inf}(f) = \rho \circ \pi \bmod \mathrm{B}^1(G,\ A) = 0$ lo cual implica que $\rho \circ \pi \in \mathrm{B}^1(G,\ A)$. Entonces, por definición, existe $a \in A$ tal que

$$\begin{aligned} \rho \circ \pi(g) = \rho(gH) &= gHa - a \qquad \text{para todo } gH \in G/H \\ &= ga - a \qquad \text{para todo } g \in G. \end{aligned}$$

Por lo tanto $\rho \in \mathrm{B}^1(G/H,\ A^H)$, de donde se sigue que $f = 0$. Mostraremos ahora que $(\mathrm{Res} \circ \mathrm{Inf})(f) = 0$ para $f \in \mathrm{H}^1(G/H,\ A^H)$. Por definición, existe $\varphi \in \mathrm{Z}^1(G/H,\ A^H)$ tal que $f = \varphi \bmod \mathrm{B}^1(G/H,\ A^H)$. Así,

$$\mathrm{Res}(\mathrm{Inf}(f)) = \mathrm{Res}(\varphi \circ \pi \bmod \mathrm{B}^1(G,\ A)) = \varphi \circ \pi_{|_H} \bmod \mathrm{B}^1(H,\ A).$$

Se tiene $\varphi \circ \pi(h) = \varphi(H)$. Ahora bien

$$\begin{aligned} \varphi(H) &= \varphi(eHeH) = eH\varphi(eH) + \varphi(eH) = \varphi(eH) + \varphi(eH) \\ &= \varphi(H) + \varphi(H). \end{aligned}$$

de donde se sigue que $\varphi(H) = \varphi \circ \pi(h) = 0$ para todo $h \in H$. Por lo tanto $(\mathrm{Res} \circ \mathrm{Inf}) = 0$. Así $\mathrm{Im}\,(\mathrm{Inf}) \subseteq \ker(\mathrm{Res})$.
Recíprocamente, veamos que $\ker(\mathrm{Res}) \subseteq \mathrm{Im}\,(\mathrm{Inf})$. Sea $f \in \ker(\mathrm{Res})$. Entonces existe $\kappa \in \mathrm{Z}^1(G, A)$ tal que $f = \kappa \bmod \mathrm{B}^1(G, A)$ y como $f \in \ker(\mathrm{Res})$ entonces $(\mathrm{Res})(f) = 0$ lo que implica que $\kappa_{|_H} \bmod \mathrm{B}^1(H, A) = 0$ luego $\kappa_{|_H} \in \mathrm{B}^1(H, A)$.
Así, por definición, existe $a \in A$ tal que $\kappa_{|_H}(h) = ha - a$ para todo $h \in H$. Sea $\delta : G \to A$ dada por $\delta(g) = ga - a$ para todo $g \in G$ y para la a obtenida anteriormente.
Notemos que $(\kappa - \delta)(h) = 0$ para todo $h \in H$, luego sin pérdida de generalidad podemos suponer que $\kappa(h) = 0$ para todo $h \in H$.
Por otro lado, observemos que $\kappa(gh) = g\kappa(h) + \kappa(g) = \kappa(g)$ para todo $g \in G$ y para todo $h \in H$.
Además, ya que $\kappa \in rmZ^1(G, A)$ y como $\kappa(h) = 0$ para todo $h \in H$, se tiene que κ induce un homomorfismo $\widetilde{\kappa} : G/H \to A$ dado por $\widetilde{\kappa}(gH) = \kappa(g)$ para todo $gH \in G/H$.
Veamos que la función $\widetilde{\kappa}$ está bien definida. Sea $g_1 \in gH$, así

$$\kappa(g_1) = \kappa(gh) = \kappa(g).$$

Por lo tanto, la función está bien definida. Por otro lado, ya que $H \triangleleft G$, tenemos que $gH = Hg$, luego

$$\widetilde{\kappa}(Hg) = \widetilde{\kappa}(gH) = \kappa(g) \qquad \text{y}$$

$$\kappa(hg) = h\kappa(g) + \kappa(h) = h\kappa(g) \qquad \text{para todo } h \in H.$$

Así tenemos que $h\kappa(g) = \widetilde{\kappa}(Hg) = \kappa(g)$ para todo $h \in H$ es decir $\kappa(g) \in A^H$, por lo tanto tenemos realmente que $\widetilde{\kappa} : G/H \to A^H$. Veamos ahora que $\widetilde{\kappa}$ es un homomorfismo cruzado. Sean $g_1H, g_2H \in G/H$ luego

$$\begin{aligned} \widetilde{\kappa}(g_1Hg_2H) &= \widetilde{\kappa}(g_1g_2H) = \kappa(g_1g_2) = g_1\kappa(g_2) + \kappa(g_1) \\ &= g_1H\widetilde{\kappa}(g_2H) + \widetilde{\kappa}(g_1H). \end{aligned}$$

Por lo tanto $\widetilde{\kappa}$ es un homomorfismo cruzado y tenemos que $\widetilde{\kappa} : G/H \to A^H$ e $\mathrm{Inf}(\widetilde{\kappa}) = \widetilde{\kappa}\circ\pi \bmod \mathrm{B}^1(G, A)$, luego $\widetilde{\kappa}\circ\pi : G \to A$ y $\widetilde{\kappa}\circ\pi(g) = \widetilde{\kappa}(gH) = \kappa(g)$, es decir, $\widetilde{\kappa}\circ\pi = \kappa$ e $\mathrm{Inf}(\widetilde{\kappa}) = \kappa \bmod \mathrm{B}^1(G, A) = f$; por lo tanto, $f \in \mathrm{Im}\,(\mathrm{Inf})$, así $\ker\,(\mathrm{Res}) = \mathrm{Im}\,(\mathrm{Inf})$ y la sucesión es exacta. ■

Proposición 4.1.4. *Sea G arbitrario y sea H subgrupo normal de G tal que $[G : H] = n < \infty$. Si $a \in A^H$ y $\sigma \in G$, entonces se tiene que σa depende sólo de la clase izquierda $\sigma \bmod H$. Sea $N_{G/H}a := \sum_{\sigma\in G/H} \sigma a$. Entonces se tiene que $N_{G/H}a \in A^G$ y que la función*

$$N_{G/H} : \hat{\mathrm{H}}^0(H,\ A) \to \hat{\mathrm{H}}^0(G,\ A)$$

es un homomorfismo de grupos bien definido.

Demostración: Sea $G = \bigcup_{i=1}^{n} g_i H$ la descomposición de G en clases laterales izquierdas de H en G. $N_{G/H}$ está bien definido pues no depende de los representantes g_i de las clases laterales $g_iH \in G/H$, pues si tomamos otros representantes digamos $r_i \in g_iH$, entonces $r_i = g_ih_i$ con $h_i \in H,\ 1 \le i \le n$; así para todo $a \in A^H$ se tiene

$$\sum_{i=1}^{n} r_i a = \sum_{i=1}^{n} (g_ih_i)a = \sum_{i=1}^{n} g_i(h_i a) = \sum_{i=1}^{n} g_i a.$$

Veamos ahora que $N_{G/H} \in A^G$. Sean $g_i\,, g_j \in G$ tal que $g_i \neq g_j \bmod H$. Para $g \in G$ se tiene que si $gg_i \equiv gg_j \bmod H$ entonces $(gg_i)^{-1}gg_j \in H$ lo cual implica $g_i^{-1}g_j \in H$ entonces $g_i \equiv g_j \bmod H$ lo cual es una contradicción. Por lo tanto $gg_i \not\equiv gg_j \bmod H$. Para $\tau \in G$ se tiene

$$\tau N_{G/H}a = \tau \sum_{i=1}^{n} g_i a = \sum_{i=1}^{n} \tau g_i a = N_{G/H}a$$

pues τg_iH recorre a todo G/H cuando g_iH recorre a todo G/H.
Veamos por último que $N_{G/H}$ es un homomorfismo de grupos, en efecto sean $a, b \in A^H$ luego

$$N_{G/H}(a+b) = \sum_{i=1}^{n} g_i(a+b) = \sum_{i=1}^{n} g_i a + \sum_{i=1}^{n} g_i b = N_{G/H}a + N_{G/H}b. \quad ■$$

El homomorfismo de grupos $N_{G/H}$ es llamado **correstricción** en dimensión 0 y denotado por **Cor.**

Proposición 4.1.5. *Se tiene que* $(\mathrm{Cor}\circ\mathrm{Res})(z) = nz$ *para todo* $z \in \hat{\mathrm{H}}^0(G, A)$, *donde* $|G/H| = n$

Demostración: Sea $w \in A^G$ luego $\mathrm{Res}(w) = w$ por lo que $\mathrm{Cor} \circ \mathrm{Res}(w) = \mathrm{Cor}(w) = \sum_{g_i H \in G/H} g_i w = g_1 w + g_2 w + \cdots + g_n w = nw$ pues el índice de H en G es n. ■

Proposición 4.1.6. *Sea* G *un grupo cíclico de orden* p, *donde* p *es un número primo. Definamos los siguientes conjuntos* $A_1 = \mathbb{Z}_p$, $A_{p-1} := \mathbb{Z}_p[\zeta_p] = \mathbb{Z}_p[x]/(\Psi_p(x))$, *y* $A_p := \mathbb{Z}_p[G]$, *donde* $\mathbb{Z}_p$ *es el anillo de los enteros p-ádicos,* ζ_p *es una raíz p-ésima primitiva de la unidad y la acción es como en la Proposición 4.1.1. Entonces* A_1, A_{p-1} A_p *son* G*-módulos y*

$$\begin{array}{rclcrcl} \hat{\mathrm{H}}^0(G,\, A_1) & \cong & C_p\ , & & \hat{\mathrm{H}}^{-1}(G,\, A_1) & = & 0, \\ \hat{\mathrm{H}}^0(G,\, A_{p-1}) & = & 0, & & \hat{\mathrm{H}}^{-1}(G,\, A_{p-1}) & \cong & C_p\ , \\ \hat{\mathrm{H}}^0(G,\, A_p) & = & 0, & & \hat{\mathrm{H}}^{-1}(G,\, A_p) & = & 0, \end{array}$$

donde C_p *es el grupo cíclico de* p *elementos.*

Demostración: Hacemos actuar a G de manera trivial sobre $\mathbb{Z}_p$. Ahora bien, tenemos que $\hat{H}^0(G,\, A) = A^G/N_G A$. Así $\hat{H}^0(G,\, \mathbb{Z}_p) = \mathbb{Z}_p^G/N_G\mathbb{Z}_p$; por otro lado, sea $x \in \mathbb{Z}_p$ luego

$$\begin{array}{rcl} (1 + \sigma + \cdots + \sigma^{p-1})\, x & = & x + \sigma x + \cdots + \sigma^{p-1} x \\ & = & x + x + \cdots + x = p\, x. \end{array}$$

De lo anterior tenemos $\hat{\mathrm{H}}^0(G,\, \mathbb{Z}_p) = \mathbb{Z}_p^G/N_G\mathbb{Z}_p = \mathbb{Z}_p/p\mathbb{Z}_p$.
Definamos el siguiente mapeo $f : \mathbb{Z} \to \mathbb{Z}_p/p\mathbb{Z}_p$ dado por: para $n \in \mathbb{Z}$ escribamos $n = pq + r$ con $0 \leq r \leq p - 1$. Entonces $f(n) = r + p\mathbb{Z}_p$.

Sean ahora $n = pq + r_1,\ m = pl + r_2$ donde $0 \leq r_i \leq p-1$ con $i = 1, 2$. Si $r_1 + r_2 = pt + r_0$ entonces $n + m = p(q + l + t) + r_0$. Por lo tanto

$$\begin{aligned} f(n+m) &= r_0 + p\mathbb{Z}_p = r_0 + pt + p\mathbb{Z}_p = r_1 + r_2 + p\mathbb{Z}_p \\ &= (r_1 + p\mathbb{Z}_p) + (r_2 + p\mathbb{Z}_p) = f(n) + f(m). \end{aligned}$$

Esto prueba que f es un homomorfismo de grupos.
Veamos que f es un epimorfismo. Sea $c \in \mathbb{Z}_p$ entonces $c = r + p\mathbb{Z}_p$ para algún $0 \leq r \leq p-1$ entonces $f(r) = r + p\mathbb{Z}_p = c$ y por lo tanto f es suprayectivo.
Finalmente veamos cual es el núcleo de f.
Sea $n = pq + r_1$ con $0 \leq r_1 \leq p-1$. Si $n \in \ker(f)$, entonces $p\mathbb{Z}_p = f(n) = r_1 + p\mathbb{Z}_p$ lo cual equivale a que $r_1 \in p\mathbb{Z}_p$ y por tanto $r_1 = 0$ y $n = pq$. Por lo tanto $n \in p\mathbb{Z}$.
Se sigue que $\ker(f) = p\mathbb{Z}$. El Primer Teorema de Isomorfismo nos dice que $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p/p\mathbb{Z}_p$. Por lo tanto

$$\hat{\mathrm{H}}^0(G,\ \mathbb{Z}_p) = \mathbb{Z}_p^G/N_G\mathbb{Z}_p = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = C_p.$$

Sabemos que por definición $\hat{\mathrm{H}}^{-1}(G,\ A) = \ker N_G A/DA$.
Así $\hat{\mathrm{H}}^{-1}(G,\ \mathbb{Z}_p) = \ker\ N_G\mathbb{Z}_p/D\mathbb{Z}_p$, en donde $D = \sigma - 1$.
Sean $x \in \ker\ N_G\mathbb{Z}_p$ y $m \in \mathbb{Z}_p$. Entonces

$$(\sigma - 1)m = \sigma m - m = m - m = 0.$$

y

$$\begin{aligned} N_G(x) &= (1 + \sigma + \cdots + \sigma^{p-1})\, x = x + \sigma x + \cdots + \sigma^{p-1}x \\ &= x + x + \cdots + x = px = 0. \end{aligned}$$

Por lo tanto $\ker\ N_G\mathbb{Z}_p = \{0\}$ y $D\mathbb{Z}_p = \{0\}$. Así $\hat{\mathrm{H}}^{-1}(G,\ \mathbb{Z}_p) = \{0\}$.
Como ya sabemos, $\hat{\mathrm{H}}^0(G,\ \mathbb{Z}_p[\zeta_p]) = \mathbb{Z}_p[\zeta_p]^G/N_G\mathbb{Z}_p[\zeta_p]$ por definición.
Para ver cuáles son los puntos fijos de $\mathbb{Z}_p[\zeta_p]$, procedemos de la siguiente forma. Sean $m \in \mathbb{Z}_p[\zeta_p]^G$ y $\sigma \in G$. Supongamos que

$$\sigma \circ m = \zeta_p\, m = m$$

entonces

$$(\zeta_p - 1)m = \zeta_p\, m - m = 0,$$

lo cual implica que $\overline{(x-1)}\ m = 0$ y puesto que $\overline{\Psi_p(x)}\ m = 0$ donde $(x-1)$ y $\Psi_p(x)$ son primos relativos, elijamos $h(x),\ g(x) \in \mathbb{Z}_p[x]$ tales

que $(x-1)h(x)+\Psi_p(x)g(x)=1$ entonces $m=\overline{1}\,m=[\overline{(x-1)h(x)}+\overline{\Psi_p(x)g(x)}]\,m=\overline{(x-1)h(x)}\,m+\overline{\Psi_p(x)g(x)}\,m=0$, Por lo tanto $m=0$. Se sigue que $N_G\mathbb{Z}_p[\zeta]=\{0\}$. Así $\hat{H}^0(G,\,\mathbb{Z}_p[\zeta_p])=\{0\}$.

Para $\hat{\mathrm{H}}^{-1}(G,\,\mathbb{Z}_p[\zeta_p])=\ker N_G/D\mathbb{Z}_p[\zeta_p]$, consideremos $h(\zeta_p)=a_0+a_1\zeta_p+\cdots+a_{p-1}\zeta_p^{p-1}\in\mathbb{Z}_p[\zeta_p]$, con $a_i\in\mathbb{Z}_p$.
Luego

$$\begin{aligned} h(\zeta_p)\in\ker N_G &\iff 0=N_G(h(\zeta_p))\iff 0=(1+\sigma+\cdots+\sigma^{p-1})(h(\zeta_p))\\ &\iff 0=(1+\zeta_p+\cdots+\zeta_p^{p-1})(h(\zeta_p)).\end{aligned}$$

Por tanto $\ker N_G=\mathbb{Z}_p[\zeta_p]$.
Por otro lado como $D=\sigma-1$, entonces $(\sigma-1)h(\zeta_p)=(\zeta_p-1)h(\zeta_p)\in(\zeta_p-1)\mathbb{Z}_p[\zeta_p]$. Así $\hat{\mathrm{H}}^{-1}(G,\,\mathbb{Z}_p[\zeta_p])=\ker N_G/D\mathbb{Z}_p[\zeta_p]=\mathbb{Z}_p[\zeta_p]/(\zeta_p-1)\mathbb{Z}_p[\zeta_p]$.
Ahora definimos el siguiente isomorfismo:
$f:\mathbb{Z}_p\to\mathbb{Z}_p[\zeta_p]/(\zeta_p-1)\mathbb{Z}_p[\zeta_p]$ de la siguiente forma: sea $w\in\mathbb{Z}_p$, con $w=a_0+a_1p+a_2p^2\cdots$, $0\le a_0\le p-1$. Entonces definamos $f(w)=w+(\zeta_p-1)\mathbb{Z}_p[\zeta_p]$ y notemos que si $w=a_0+a_1p+a_2p^2+\cdots$, entonces $w-a_0=a_1p+a_2p^2+a_3p^3+\cdots=pv$ donde $v\in\mathbb{Z}_p$ y

$$\begin{aligned} p &= -[(\zeta_p^{p-1}-1)+((\zeta_p^{p-2}-1))+\cdots+((\zeta_p-1))]\\ &= -[(\zeta_p-1)(\zeta_p^{p-2}+\cdots+\zeta_p+1)\\ &\quad +(\zeta_p-1)(\zeta_p^{p-3}+\cdots+\zeta_p+1)+\cdots+(\zeta_p-1)]\\ &= -(\zeta_p-1)[(\zeta_p^{p-2}+\cdots+\zeta_p+1)\\ &\qquad +(\zeta_p^{p-3}+\cdots+\zeta_p+1)+\cdots+1]\in(\zeta_p-1)\mathbb{Z}_p[\zeta_p].\end{aligned}$$

Ya que $\zeta_p^{p-1}+\zeta_p^{p-2}+\cdots+\zeta_p+1=0$, tenemos que $w-a_0=pv\in(\zeta_p-1)\mathbb{Z}_p[\zeta_p]$, es decir, $w+(\zeta_p-1)\mathbb{Z}_p[\zeta_p]=a_0+(\zeta_p-1)\mathbb{Z}_p[\zeta_p]$. Así pues, si $w=a_0+a_1p+a_2p^2+\cdots$ entonces $f(w)=a_0+(\zeta_p-1)\mathbb{Z}_p$.
Sean ahora $w_1,\ w_2\in\mathbb{Z}_p$. Entonces

$$\begin{aligned} f(w_1+w_2) &= (w_1+w_2)+(\zeta_p-1)\mathbb{Z}_p[\zeta_p]\\ &= (w_1+(\zeta_p-1)\mathbb{Z}_p[\zeta_p])+(w_2+(\zeta_p-1)\mathbb{Z}_p[\zeta_p])\\ &= f(w_1)+f(w_2).\end{aligned}$$

Por lo que f es un homomorfismo. Veamos que f es un epimorfismo.
Sea $h(\zeta_p)+(\zeta_p-1)\mathbb{Z}_p[\zeta_p]\in\mathbb{Z}_p[\zeta_p]/(\zeta_p-1)\mathbb{Z}_p[\zeta_p]$, como $h(x)\in\mathbb{Z}_p[x]$ ahora por el algoritmo de la división para $h(x)$ y $(x-1)$ tenemos que

$h(x) = (x-1)q(x) + r(x)$, con grado de $r(x) \leq$ grado $(x-1)$ por lo que $r(x) = w \in \mathbb{Z}_p$. Así $h(\zeta_p) = (\zeta_p - 1)q(\zeta_p) + w$. Por lo tanto.

$$h(\zeta_p) + (\zeta_p - 1)\mathbb{Z}_p[\zeta_p] = w + (\zeta_p - 1)\mathbb{Z}_p[\zeta_p] = f(w).$$

Finalmente veamos cual es el núcleo de f.
Para $w \in \mathbb{Z}_p$, con $w = a_0 + a_1 p + \cdots$, $0 \leq a_0 \leq p-1$, se tiene que $w \in \ker f \iff f(w) = 0$, es decir $a_0 \in (\zeta_p - 1)\mathbb{Z}_p[\zeta_p]$. Ahora bien esto último es equivalente a $a_0 = (\zeta_p - 1)t(\zeta_p)$. Por tanto

$$a_0^{p-1} = N(\zeta_p - 1)N(t(\zeta_p)) = (-1)^{p-1} p N(t(\zeta_p)) \in \mathbb{Z}_p.$$

Por otro lado si $a_0 \neq 0$, entonces $a_0^{p-1} \equiv 1 \bmod p$ es decir $a_0^{p-1} = 1 + pt_1$, $t_1 \in \mathbb{N} \cup \{0\}$. Entonces

$$1 + pt_1 = p((-1)^{p-1} N(t(\zeta_p))) \in p\,\mathbb{Z}_p,$$

lo cual es una contradicción. Por lo tanto $a_0 = 0$, de donde $w \in p\,\mathbb{Z}_p$ por lo que $\ker f \subseteq p\,\mathbb{Z}_p$.
Recíprocamente sea $w \in p\mathbb{Z}_p$, Entonces $w = 0 + a_1 p + \cdots$, luego

$$f(w) = 0 + (\zeta_p - 1)\mathbb{Z}_p[\zeta_p] = 0$$

de donde obtenemos que $w \in \ker f$. Por lo tanto $\ker f = p\,\mathbb{Z}_p$. El Primer Teorema de Isomorfismo nos dice que

$$\mathbb{Z}_p / p\,\mathbb{Z}_p \cong \mathbb{Z}_p[\zeta_p]/(\zeta_p - 1)\mathbb{Z}_p[\zeta_p].$$

Así

$$\hat{\mathrm{H}}^{-1}(G,\, \mathbb{Z}_p[\zeta_p]) = \mathbb{Z}_p[\zeta_p]/(\zeta_p - 1)\mathbb{Z}_p[\zeta_p] \cong \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = C_p.$$

Calculemos

$$\hat{\mathrm{H}}^{0}(G,\, \mathbb{Z}_p[G]) = \mathbb{Z}_p[G]^G / N_G\, \mathbb{Z}_p[G].$$

Sea $m \in \mathbb{Z}_p[G]^G$, $m = a_0 + a_1\sigma + \cdots + a_{p-1}\sigma^{p-1}$.
Luego $\sigma \circ m = a_0\sigma + a_1\sigma^2 + \cdots + a_{p-1}\sigma^p$. Por lo tanto $\sigma \circ m = m$ si y sólo si $a_0 = a_1 = \cdots = a_{p-1}$. Se sigue que

$$m = a_0 + a_0\sigma + \cdots + a_0\sigma^{p-1} = (1 + \sigma + \cdots + \sigma^{p-1})a_0 = N_G\, a_0$$

es norma. Por lo tanto $\hat{\mathrm{H}}^0(G,\, \mathbb{Z}_p[G]) = \{0\}$.
Finalmente veamos que $\hat{\mathrm{H}}^{-1}(G,\, \mathbb{Z}_p[G]) = \ker N_G / D\, \mathbb{Z}_p[G]$. Sea $x \in \ker N_G$, con $x = a_0 + a_1\sigma + \cdots + a_{p-1}\sigma^{p-1}$. Entonces

$$N_G(x) = \left(\sum_{i=0}^{p-1} \sigma^i\right)\left(\sum_{j=0}^{p-1} a_j\sigma^j\right) = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_j\sigma^{i+j} = \sum_{t=0}^{p-1}\left(\sum_{j=0}^{p-1} a_j\right)\sigma^t.$$

Si $a = a_0 + a_1 + \cdots + a_{p-1}$, se tiene $N_G(x) = a + a\sigma + \cdots + a\sigma^{p-1}$. Por lo tanto $x \in \ker N_G$ si y sólo si $a = \sum_{i=0}^{p-1} a_i = 0$.
Por lo tanto $\ker N_G = \left\{ x = \sum_{i=0}^{p-1} a_i\sigma^i \mid \sum_{i=0}^{p-1} a_i = 0 \right\}$. Por otro lado, sea $b_0 + b_1\sigma + \cdots + b_{p-1}\sigma^{p-1} \in \mathbb{Z}_p[G]$, arbritario. Se tiene que

$$\begin{aligned}(\sigma-1)(b_0 + b_1\sigma + \cdots + b_{p-1}\sigma^{p-1}) &= (b_0\sigma + b_1\sigma^2 + \cdots + b_{p-1}\sigma^p) - (b_0 + b_1\sigma + \cdots + b_{p-1}\sigma^{p-1}) \\ &= (b_{p-1} - b_0) + (b_0 - b_1)\sigma + (b_1 - b_2)\sigma^2 + (b_2 - b_3)\sigma^3 \\ &\quad + \cdots + (b_{p-2} - b_{p-1})\sigma^{p-1}.\end{aligned}$$

Dado $x = \sum_{i=0}^{p-1} a_i\sigma^i \in \ker N_G$ definimos $y = b_0 + b_1\sigma + \cdots + b_{p-1}\sigma^{p-1}$ donde

$$\begin{aligned} b_0 &:= -a_0 = a_{p-1} + a_{p-2} + \cdots + a_2 + a_1 \\ b_1 &:= a_{p-1} + a_{p-2} + a_{p-3}\cdots + a_3 + a_2 \\ b_2 &:= a_{p-1} + a_{p-2} + a_{p-3}\cdots + a_4 + a_3 \\ &\vdots \\ b_{p-2} &:= a_{p-1} \\ b_{p-1} &:= 0. \end{aligned}$$

Entonces

$$\begin{aligned} Dy &= (b_{p-1} - b_0) + (b_0 - b_1)\sigma + (b_1 - b_2)\sigma^2 + \cdots + (b_{p-2} - b_{p-1})\sigma^{p-1} \\ &= a_0 + a_1\sigma + \cdots + a_{p-1}\sigma^{p-1} = x. \end{aligned}$$

Por lo tanto $\ker N_G \subseteq D\mathbb{Z}_p[G]$, lo cual implica que

$$\hat{\mathrm{H}}^{-1}(G,\, \mathbb{Z}_p[G]) = \ker N_G / D\, \mathbb{Z}_p[G] = \{0\}. \qquad \blacksquare$$

Proposición 4.1.7. *Sean G un grupo finito y p^m la máxima potencia de p que divide a $|G|$. Entonces $\hat{\mathrm{H}}^1(G,\ \mathbb{Z}_p) \cong \hat{\mathrm{H}}^{-1}(G,\ \mathbb{Z}_p) = \{0\}$ y $\hat{\mathrm{H}}^0(G,\ \mathbb{Z}_p) \cong \mathbb{Z}_p/p^m\mathbb{Z}_p$. También se tiene que $\hat{\mathrm{H}}^i(G,\ \mathbb{Q}_p) = \{0\}$ para todo i.*

Demostración: Se usará que $\hat{\mathrm{H}}^i(G,\ \mathbb{Q}_p)$ es un grupo finito. Se tiene que G actúa trivialmente sobre $\mathbb{Z}_p$. Entonces $\hat{\mathrm{H}}^0(G,\ \mathbb{Z}_p) = \mathbb{Z}_p^G/N_G\mathbb{Z}_p$, con $\mathbb{Z}_p^G = \mathbb{Z}_p$. Para $x \in \mathbb{Z}_p$ tenemos que

$$\begin{aligned} N_G(x) &= (1+\sigma+\cdots+\sigma^{p-1})x = x+\sigma x+\cdots+\sigma^{p-1}x \\ &= x+x+\cdots+x = p^m x. \end{aligned}$$

Por lo tanto, $\hat{\mathrm{H}}^0(G,\ \mathbb{Z}_p) \cong \mathbb{Z}_p/p^m\mathbb{Z}_p$.
Ahora para $\hat{\mathrm{H}}^{-1}(G, \mathbb{Z}_p) = \ker N_G/I_G\mathbb{Z}_p$, sea $x \in \ker N_G$. Se tiene que $N_G(x) = \sum_{\sigma\in G} \sigma x = p^m x = 0 \Longleftrightarrow x = 0$. De donde $\ker N_G = \{0\}$, y por tanto obtenemos que $\hat{\mathrm{H}}^{-1}(G,\ \mathbb{Z}_p) = \ker N_G/I_G\mathbb{Z}_p = \{0\}$.
Por otro lado, puesto que $\mathrm{H}^1(G,\ \mathbb{Z}_p) \cong \mathrm{Hom}\,(G,\ \mathbb{Z}_p)$, consideremos un homomorfismo $\psi : G \longrightarrow \mathbb{Z}_p$. Sea $\sigma \in G$, $\sigma \neq 1$.

$$p^m\psi(\sigma) = \psi(\sigma)+\psi(\sigma)+\cdots+\psi(\sigma) = \psi(\sigma\cdot\sigma\cdots\sigma) = \psi(\sigma^{|G|}) = \psi(1) = 0.$$

Puesto que $\mathbb{Z}_p$ no tiene torsión, se sigue que $\psi(\sigma) = 0$. Por lo tanto $\mathrm{H}^1(G, \mathbb{Z}_p) = \{0\}$.
Sea $f : \mathbb{Q}_p \to \mathbb{Q}_p$ el mapeo multiplicación por n, es decir $f(x) = nx$. Entonces f es un homomorfismo de G-módulos y tenemos la sucesión exacta:

$$0 \to \mathbb{Q}_p \xrightarrow{f} \mathbb{Q}_p \to 0 \to 0$$

Por el Teorema 3.1.3 se tiene la sucesión exacta

$$\hat{\mathrm{H}}^{i-1}(G,\ 0) = \{0\} \to \hat{\mathrm{H}}^i(G,\ \mathbb{Q}_p) \xrightarrow{f^*} \hat{\mathrm{H}}^i(G, \mathbb{Q}_p) \to \hat{\mathrm{H}}^i(G,\ 0) = \{0\}$$

Por lo tanto f^* es un isomorfismo. Tomando n tal que $nG = e$, se sigue que $f^* = 0$. Por lo tanto $\hat{\mathrm{H}}^i(G,\ \mathbb{Q}_p) = \{0\}$. ■

Proposición 4.1.8. *Con la notación de la Proposición* 4.1.7 *se tiene que*

$$\hat{\mathrm{H}}^i(G,\ R) \cong \hat{\mathrm{H}}^{i+1}(G,\ \mathbb{Z}_p)$$

para todo i, donde $R = \mathbb{Q}_p/\mathbb{Z}_p$.

Demostración: Se tiene la sucesión exacta

$$0 \to \mathbb{Z}_p \to \mathbb{Q}_p \to R \to 0$$

Por el Teorema 3.1.3 se tiene la sucesión exacta

$$\hat{\mathrm{H}}^i(G,\, \mathbb{Q}_p) = \{0\} \to \hat{\mathrm{H}}^i(G,\, R) \to \hat{\mathrm{H}}^{i+1}(G, \mathbb{Z}_p) \to \hat{\mathrm{H}}^{i+1}(G,\, 0) = \{0\}$$

Por lo tanto $\hat{\mathrm{H}}^i(G,\, R) \cong \hat{\mathrm{H}}^{i+1}(G, \mathbb{Z}_p)$. ■

Proposición 4.1.9. *Sean G un p-grupo finito y M un G-módulo. Suponga que existe $s \in \mathbb{N} \cup \{0\}$ tal que los grupos M y R^s son isomorfos, donde $R = \mathbb{Q}_p/\mathbb{Z}_p$. Considere la sucesión exacta*

$$0 \to {}_pM \to M \xrightarrow{p} M \to 0,$$

donde la función denotada por p es la multiplicación por p y ${}_pM := \{m \in M \mid pm = 0\}$. Si

$$\alpha_i(M) = \dim_{\mathbb{F}_p} \frac{\hat{\mathrm{H}}^i(G,\, M)}{{}_p\hat{\mathrm{H}}^i(G,\, M)} = \dim_{\mathbb{F}_p}\, {}_p\hat{\mathrm{H}}^i(G,\, M),$$

entonces $\hat{\mathrm{H}}^i(G,\, {}_pM) \cong C_p^{\alpha_{i-1}(M)+\alpha_i(M)}$.

Demostración: Por el Teorema 3.1.3 se tiene la sucesión exacta

$$\to \hat{\mathrm{H}}^{i-1}(G,\, M) \xrightarrow{p^*} \hat{\mathrm{H}}^{i-1}(G\,, M) \xrightarrow{\varphi} \hat{\mathrm{H}}^i(G,\, {}_pM) \to \hat{\mathrm{H}}^i(G,\, M) \xrightarrow{p^*} \hat{\mathrm{H}}^i(G,\, M)$$

Afirmamos que la siguiente sucesión también es exacta

$$0 \to \frac{\hat{\mathrm{H}}^{i-1}(G,\, M)}{{}_p\hat{\mathrm{H}}^{i-1}(G,\, M)} \to \hat{\mathrm{H}}^i(G,\, {}_pM) \to {}_p\hat{\mathrm{H}}^i(G,\, M) \to 0.$$

En efecto, se tiene que $\ker \varphi = \operatorname{im} p^* = {}_p\hat{\mathrm{H}}^{i-1}(G,\, M)$ y $\ker p^* = {}_p\hat{\mathrm{H}}^i(G,\, M)$. Por otro lado, recordemos que si V es un espacio vectorial de dimensión

finita sobre el campo K entonces si W es un subespacio de V se tiene que $\dim V/W = \dim V - \dim W$, es decir, $\dim V = \dim W + \dim V/W$. Sean ahora $m \in \hat{\mathrm{H}}^i(G,\ {}_pM)$ y $\overline{k} = [k] = k \bmod p$ para $k \in \mathbb{Z}$. Entonces definimos una acción de $\mathbb{F}_p$ en $\hat{H}^i(G, {}_pM)$ dada por $\overline{k}m := km$ la cual está bien definida pues si $\overline{k} = \overline{k'}$ con $\overline{k'} = k + rp$ entonces $k'm = km$, luego define un multiplicación por escalar haciendo a $\hat{\mathrm{H}}^i(G,\ {}_pM)$ espacio vectorial sobre $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$, y por lo tanto tomando $W = \dfrac{\hat{\mathrm{H}}^{i-1}(G,\ M)}{{}_p\hat{\mathrm{H}}^{i-1}(G,\ M)}$, $V = \hat{\mathrm{H}}^i(G,\ {}_pM)$, $U = {}_p\hat{\mathrm{H}}^i(G,\ M)$ tenemos entonces que

$$0 \to W \to V \to U \to 0$$

es exacta y $\dim V = \dim W + \dim U$ es decir

$$\begin{aligned} \dim{}_{\mathbb{F}_p}(\hat{\mathrm{H}}^i(G,\ {}_pM)) &= \dim{}_{\mathbb{F}_p}\left(\frac{\hat{\mathrm{H}}^{i-1}(G,\ M)}{{}_p\hat{\mathrm{H}}^{i-1}(G,\ M)}\right) + \dim{}_{\mathbb{F}_p}({}_p\hat{\mathrm{H}}^i(G,\ M)) \\ &= \alpha_{i-1}(M) + \alpha_i(M). \end{aligned}$$

Entonces, tenemos que $\hat{\mathrm{H}}^i(G, {}_pM) \cong \mathbb{F}_p^{\alpha_{i-1}(M)+\alpha_i(M)}$ como espacios vectoriales y $\hat{\mathrm{H}}^i(G,\ {}_pM) \cong C_p^{\alpha_{i-1}(M)+\alpha_i(M)}$ como grupos. ■

Ejemplo 4.1.3. Sea K/k un campo de funciones con k algebraicamente cerrado. Sea L/K una extensión finita de Galois con grupo de Galois G. Denotamos por D_L al grupo de divisores de L, y por D_K al grupo de divisores de K. Sea $r \geq 0$ el número de primos en K ramificados en L. Digamos que $\mathfrak{p}_1, \ldots,\ \mathfrak{p}_r$ son los primos de K ramificados en L, con índices de ramificación $e_1, \ldots,\ e_r$, respectivamente. Para cada $i = 1, \ldots, r$, expresamos

$$\mathfrak{p}_\mathfrak{i} = \left(\prod_{j=1}^{m_i} \mathcal{P}_{ij}\right)^{e_i},$$

donde cada $\mathcal{P}_{ij}$ es un primo de L que está sobre $\mathfrak{p}_i$.

Hacemos actuar G sobre D_L vía la acción de G sobre cada divisor primo de L, es decir, para cada divisor primo $\mathcal{P}$ de L y para cada $\sigma \in G$, tenemos que

$$\sigma(\mathcal{P}) = \{\sigma(a) \mid a \in \mathcal{P}\}.$$

Notemos que $\sigma(\mathcal{P})$ es un primo de L que está sobre el primo $\mathcal{P} \cap K$ de K. Así, tenemos que D_L es un G-módulo.
Sea $\mathcal{D}$ un elemento de D_L. Observemos que $\mathcal{D} \in D_L^G$ si y sólo si la factorización de $\mathcal{D}$ está dada por un producto finito de divisores de L, cada uno de los cuales es de la forma

$$(\mathcal{P}_1 \cdots \mathcal{P}_s)^l,$$

donde $\mathcal{P}_1, \ldots, \mathcal{P}_s$ son exactamente los primos de L que están sobre el primo $\mathcal{P}_1 \cap K$ de K, para algún $l \in \mathbb{Z}$. En particular, si para algún $j \in \{1, \ldots, m_i\}$, con $i \in \{1, \ldots, r\}$, se tiene que $\mathcal{P}_{ij}$ aparece en la factorización de $\mathcal{D}$, con $\mathcal{D} \in D_L^G$, entonces en $\mathcal{D}$ aparecerá como factor de $\mathcal{D}$ el divisor

$$\left(\prod_{j=1}^{m_i} \mathcal{P}_{ij}\right)^{l_i}, \tag{4.1}$$

para algún $l_i \in \mathbb{Z}$. Expresando $l_i = e_i q_i + r_i$, con $q_i, r_i \in \mathbb{Z}$ y $0 \leq r_i < e_i$, el divisor en (4.1) se puede expresar en la forma

$$\mathfrak{p}_i^{q_i} \left(\prod_{j=1}^{m_i} \mathcal{P}_{ij}\right)^{r_i}.$$

Por otro lado, puesto que k es algebraicamente cerrado, cada primo $\mathcal{P}$ de L tiene grado de inercia 1 sobre el primo $\mathcal{P} \cap K$. De aquí que, $N_G D_L = D_K$, donde D_K se puede considerar un subgrupo de D_L^G. Además, por lo establecido anteriormente, cada elemento del cociente D_L^G / D_K es de la forma

$$\prod_{i=1}^{r} \left(\prod_{j=1}^{m_i} \mathcal{P}_{ij}\right)^{r_i} \cdot D_K,$$

donde $0 \leq r_i < e_i$, para cada $i = 1, \ldots, r$. Más aún, los elementos $\prod_{j=1}^{m_i} \mathcal{P}_{ij} \cdot D_K$, con $i = 1, \ldots, r$, son de orden e_i y, puesto que los primos de L son generadores libres de D_L (lo mismo ocurre con el grupo D_K), se tiene que

$$\frac{D_L^G}{D_K} \cong \bigoplus_{i=1}^{r} \left\langle \prod_{j=1}^{m_i} \mathcal{P}_{ij} \cdot D_K \right\rangle .$$

Por lo tanto, hemos probado que

$$\hat{\mathrm{H}}^0(G,\ D_L) = \frac{D_L^G}{N_G D_L} = \frac{D_L^G}{D_K} \cong \bigoplus_{i=1}^{r} C_{e_i} \ .$$

Ahora, veamos que $\hat{\mathrm{H}}^{-1}(G,\ D_L) = \{0\}$. Para esto, sea $\mathcal{D}$ un divisor de L, digamos que $\mathcal{D} = \prod_{\iota=1}^{t} \mathcal{P}_\iota^{s_\iota}$. Entonces, $\mathcal{D} \in \ker N_G$ si y sólo si

$$\begin{aligned} 0 &= N_G(\mathcal{D}) = N_G\left(\prod_{\iota=1}^{t} \mathcal{P}_\iota^{s_\iota}\right) \\ &= \prod_{\iota=1}^{t} N_G(\mathcal{P}_\iota)^{s_\iota} = \prod_{\iota=1}^{t} \mathfrak{p}_\iota^{f_\iota s_\iota} \\ &= \prod_{\iota=1}^{t} \mathfrak{p}_\iota^{s_\iota}, \end{aligned}$$

ya que cada $f_\iota = 1$ por ser k algebraicamente cerrado, y donde no necesariamente los primos $\mathfrak{p}_\iota$ son distintos a pares. Así que, $\mathcal{D} \in \ker N_G$ si y sólo si la suma de exponentes s_ι que afectan a primos $\mathcal{P}_\iota$ que están sobre un mismo primo de K debe de ser cero, y puesto que estos primos de L forman un conjunto G-transitivo, lo anterior es equivalente a que el divisor $\mathcal{D}$ se ha de expresar como un producto de divisores de L de la forma $\mathcal{P}\sigma(\mathcal{P})^{-1}$ para ciertos primos $\mathcal{P}$ que aparecen en la factorización de $\mathcal{D}$ y para ciertos elementos $\sigma \in G$. Por lo tanto, tenemos que $\mathcal{D} \in \ker N_G$ si y sólo si $\mathcal{D} \in I_G D_L$. En consecuencia, $\ker N_G = I_G D_L$ y $\hat{\mathrm{H}}^{-1}(G,\ D_L) = \{0\}$.

Conclusiones

Desde el punto de vista algebraico, los G-módulos y las resoluciones proyectivas sobre $\mathbb{Z}$ son la herramienta fundamental que nos permite definir los grupos de homología y cohomología de un G-módulo A, a través de la aplicación del producto tensorial y de los homomorfismos de G-módulos, de manera respectiva, de los módulos proyectivos de cualquier resolución proyectiva sobre $\mathbb{Z}$ con A (Definición 2.1.1, Teorema 2.1.1 y Definición 2.1.2). Lo relevante de los grupos de homología y cohomología, además de las aplicaciones que uno pudiera tener de ellos, es de que estos grupos tienen un comportamiento bastante agradable; por ejemplo, si se tiene una sucesión exacta corta de G-módulos, los grupos de homología y cohomología de los G-módulos involucrados, en dicha sucesión exacta, también estarán conectados a través de una sucesión exacta infinita (Teorema 2.1.2).

Los grupos de homología y cohomología de G-módulos son difíciles de calcular en términos generales. Sin embargo, si sabemos cómo son estos grupos para algún G-módulo B, es posible que podamos conocer, por lo menos, la relación de estos grupos para dos G-módulos A y C que estén relacionados, de alguna manera, con el G-módulo B. Los grupos de homología son triviales para un G-módulo B inducido, y si $0 \to A \to B \to C \to 0$ es una sucesión exacta corta de G-módulos, entonces los grupos de homología de A y C son iguales (isomorfos), como se tiene en el Teorema 2.2.3 y Corolario 2.2.2. De manera similar, lo anterior ocurre para los grupos de cohomología, cuando se está trabajando con los G-módulos coinducidos (Teorema 2.2.1 y Corolario 2.2.1). Por otro lado, en algunos casos es posible caracterizar los grupos de homología y cohomología para $n = 0, 1$ y 2. Por ejemplo, una aplicación del cálculo del primer grupo de cohomología la obtenemos con el Teorema 90 de Hilbert (Teorema 2.4.1), en el cual para una extensión de campos L/K que es de Galois y finita, con grupo de Galois G, se tiene que $\mathrm{H}^1(G, L^*) = 0$.

La importancia de los grupos de cohomología de Tate para un G-módulo A, con G grupo finito, radica en que éstos están definidos para exponentes enteros, y relaciona a los grupos de homología y cohomología de A (Definición 3.1.2). Además, si se tiene una sucesión exacta corta de G-módulos, los grupos de cohomología de Tate, de los G-módulos involucrados, están conectados a través de una sucesión exacta infinita, como se tiene en el Teorema 3.1.3. En el caso particular de que se tenga un grupo cíclico finito G, los grupos de cohomología de Tate de un G-módulo A están completamente caracterizados (Teorema 3.2.1).

Bibliografía

[1] Brown, K. S., *Cohomology of Groups*, Springer-Verlag, New York, GTM 87, (1982).

[2] Eilenberg, Samuel, *Singular Homology Theory*, Annals of Math, 45, (1943), 407-446.

[3] Eilenberg, Samuel y Maclane, Saunders, *Cohomology Theory in Abstract Groups*, Annals of Math, 48, (1947), 51-78.

[4] Gruenberg, Karl W., *Cohomological Topics in Group Theory*, Springer-Verlag, New York 143, (1970).

[5] Lam-Estrada, Pablo, *Campos de Funciones Ciclotómicos y Extensiones Pseudo-Cogalois*, Tesis doctoral, CINVESTAV-IPN, México, (1997).

[6] Lam-Estrada, Pablo, y Villa-Salvador, Gabriel Daniel *Some Remarks on the Theory of Cyclotomic Function Fields*, Rocky Mountains Journal of Mathematics, 31, (2001), 483-502.

[7] Villa-Salvador, Gabriel Daniel, *Topics in the Theory of Algebraic Fuctions Fields*, Birkhäuser, Boston, (2006).

[8] Villa-Salvador, Gabriel Daniel, *Introducción a la Teoría de las Funciones Algebraicas*, Fondo de Cultura Económica, México, (2003).

[9] Washington, Lawrence C., *Introduction to Cyclotomic Fields*, Springer-Verlag, Second Edition, GTM 83, (1996).

[10] Weiss, Edwin, *Cohomology of Groups*, Academic Press, New York and London, (1969).

[11] Zaldívar-Cruz, Felipe, *Cohomología de Galois de Campos Locales*, Sociedad Matemática Mexicana, (2001).

Índice