UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERÍAS

DEPARTAMENTO DE MATEMÁTICAS

“ALGUNOS ASPECTOS COHOMOLÓGICOS DE LA TEORÍA DE GALOIS”

TESIS PARA OBTENER EL TITULO DE LICENCIADO EN MATEMÁTICAS

AUTOR:

ALDEBARÁN ALANÍZ ROCHÍN

DIRECTOR DE TESIS:

DR. LUIS ÁNGEL ZALDIVAR CORICHI

GUADALAJARA, JALISCO, OCTUBRE 2019

UNIVERSIDAD DE GUADALAJARA
CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERÍAS
SECRETARÍA ACADÉMICA
COORDINACIÓN DE LA LICENCIATURA EN MATEMÁTICAS

C. ALDEBARAN ALANIZ ROCHIN (214514678)
PASANTE DE LA CARRERA DE
LICENCIADO EN MATEMÁTICAS

Por este conducto le damos a conocer el Dictamen emitido por el Comité de Titulación de esta carrera en relación a su solicitud de aprobación de la modalidad y tema de titulación.

MODALIDAD: **TESIS, TESINA E INFORMES**
OPCION: **TESIS**
TÍTULO: **"ALGUNOS ASPECTOS COHOMOLÓGICOS DE LA TEORÍA DE GALOIS"**
DIRECTOR: **Dr. Luis Ángel Zaldívar Corichi.**

Con base en el Artículo 13, Fracción I, Capítulo II del Reglamento General de Titulación y Artículo 13, Fracción I del Reglamento del Centro Universitario de Ciencias Exactas e Ingenierías (CUCEI), el Comité emite el siguiente número de dictamen de aprobación de modalidad y tema:

DICTAMEN: 691.

Que queda asentado en el acta de Sesión # 02 de este Comité con fecha de 03 de Junio de 2019.

En base al procedimiento académico-administrativo de titulación del CUCEI se le otorga un periodo de 1 año a partir de la fecha del presente Dictamen para la realización de su ceremonia de titulación.

ATENTAMENTE
"PIENSA Y TRABAJA"
Guadalajara, Jal., a 05 de Septiembre de 2019.

Coordinación del Programa Docente de la Licenciatura en Matemáticas

DR. ALFONSO MANUEL HERNÁNDEZ MAGDALENO
PRESIDENTE DEL COMITÉ DE TITULACIÓN DE LA LICENCIATURA EN MATEMÁTICAS

H. COMITÉ DE TITULACIÓN

LICENCIATURA EN MATEMÁTICAS

PRESENTE

Guadalajara, Jalisco a 10 de octubre de 2019

Por este medio me permito informar a usted que los académicos asignados por el H. Comité de Titulación de la Licenciatura en Matemáticas, después de haber revisado el manuscrito del proyecto de tesis titulado:

"Algunos aspectos cohomológicos de la teoría de Galois"

Desarrollado por el alumno **ALDEBARÁN ALANIZ ROCHÍN,** han tenido a bien aprobada su impresión, trabajo que defenderá el alumno para obtener el grado de Licenciado en matemáticas.

Sin más por el momento, nos despedimos de ustedes enviándoles un cordial saludo.

Dr. Luis Ángel Zaldívar Corichi

Dr. Osbaldo Mata Gutiérrez

Dra. Miriam Bocardo Gaspar

UNIVERSIDAD DE GUADALAJARA
CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERÍAS
SECRETARÍA ACADÉMICA
COORDINACIÓN DE LA LICENCIATURA EN MATEMÁTICAS

DR. HUMBERTO GUTIERREZ PULIDO
Director de la División de Ciencias Básicas
Presente

A través de la presente informo a usted, que el pasante que se describe a continuación, desea sustentar su ceremonia de titulación, con la modalidad señalada, el próximo **miércoles 9 de octubre** del año en curso a las **14:00 horas**.

Nombre del Pasante**: ALDEBARAN ALANIZ ROCHIN**

Carrera**: Licenciatura en Matemáticas** Código: **214514678** Fecha de egreso: **2019A**

Modalidad: **Tesis, Tesina e Informes.**
Opción: **Tesis**

Lo anterior en virtud de que el Comité de Titulación ha revisado su trabajo académico y documentación correspondiente, por lo que considera que cubre los requisitos para presentar su examen de grado.

Así mismo hago de su conocimiento que el Comité designó como Jurado de Titulación a los siguientes académicos:

Nombre	**Departamento o Institución de procedencia**
Presidente. Dr. Luis Ángel Saldívar Corichi	**Matemáticas**
Secretario. Dr. Osbaldo Mata Gutiérrez	**Matemáticas**
Vocal. Dra. Miriam Bocardo Gaspar	**Matemáticas**

Lo anterior sobre la base del Reglamento General de Titulación, por lo que solicito a usted gire instrucciones para el uso de la sala de titulación y los citatorios correspondientes.

Sin otro particular, quedo de usted para cualquier aclaración.

Atentamente,
"Piensa y Trabaja"
Guadalajara, Jal. 4 de Octubre de 2019.

Dr. Alfonso Manuel Hernández Magdaleno
Presidente del Comité de Titulación

COMITÉ DE TITULACIÓN
LICENCIATURA EN MATEMÁTICAS

C.c.p. Expediente del Pasante

AGRADECIMIENTOS

Agradezco a todas las personas que me ayudaron en la elaboración y corrección de este documento, principalmente a mi asesor Luis Ángel Zaldívar Corichí, asi como a mis sinodales, el Dr. Osbaldo Mata y la Dra. Miriam Bocardo. También agradezco a mis maestros y compañeros que me ayudaron a fortalecer mis conocimientos durante la carrera y estuvieron creyendo en mí. Quiero agradecer a los profesores Muñoz Chavez, Ricardo Águila, Ándres García, Martín Casillas, Humberto Gutiérrez, la Dra. Paz, y al resto de profesores que me ayudaron a salir adelante, así como al cuerpo administrativo de la Lic. en matemáticas, Martita y Lupita que me ayudaban cuando lo requeía. Agradezco a mis compañeros Miguel Guerrero, Rogelio Cruz, Yuli Gutiérrez, Ernesto Cruz, Atziri Padilla, Rafael Blanco, Francisco Alvarez, Luis Sánchez, Manuel Sánchez, Román Zuñiga, Andrea Martínez, y los que me faltan por mencionar. Especialmente quiero agradecer a Cynthia por estar siempre cuando lo necesitaba y apoyarme incondicionalmente.

Mis mas grandes agradecimientos van a mi familia, quienes siempre creyeron en mí y estuvieron apoyandome en las decisiones que he tomado en mi vida; a mi mamá Sandra Rochín López, a mi papá Abel Alaníz Sánchez, a mis hermanos Abel Alaníz Rochín y Alkaid Alaníz Rochín, a mis abuelos, tíos y primos. Agradezco a mi cuñada Clara de la Toba por su apoyo y a mi sobrina Altaír por ser una motivación para lograr esto.

A todos los que mencione y a todos los que alguna vez me ayudaron o aconsejaron en algo, muchas gracias.

Índice general

Capítulo 1

Introducción

En sus primeras formulaciones la teoría de Galois estudiaba los efecto de la sustitución de raíces en una ecuación polinómica; en el lenguaje de teoría de grupos, esto es una acción de permutación. Después la teoría de Galois se fue desarrollando para dar un enfoque diferente a la topología algebraica. [3]
El teorema fundamental de la teoría de Galois es una herramienta importante que relaciona los campos intermedios de una extensión finita de Galois con los subgrupos del grupo de Galois correspondiente a la extensión, además, esta relación es biyectiva, por lo que nos da una herramienta para trabajar con grupos de Galois utilizando teoría de campos.
Además, veremos que en el caso de los grupos de Galois de extensiones finitas, estos están dotados con una nueva topología, la de Krull, la cual brinda una herramienta importante que se utiliza para demostrar el teorema de Krull (teorema fundamental de la teoría de Galois para extensiones infinitas), ya que con los abiertos definidos en ésta topología, se puede apreciar que los subgrupos abiertos también son cerrados (de índice finito).
El álgebra homológica es una herramienta usada para demostrar la existencia de teoremas no-constructivos en álgebra (y topología algebráica). Además, proporciona herramientas para realizar varios tipos de construcciones. [4]
El álgebra homológica es una herramienta que nos brinda una relación entre la teoría de grupos y la topología algebraica, ya que trata de encontrar relaciones entre los grupos de homología y los grupos de cohomología de un espacio. [2] Una relación entre dichos grupos es que si tomamos un complejo finito, si su n-ésimo grupo de homología es 0, esto implica que el complejo (visto como espacio) no tiene agujeros n-dimesionales.
Antes no se podían calcular los grupos de cohomología de un grupo de Galois infinito, sin embargo, se encontró una herramienta para poder trabajar esto, ya que

se desarolló la cohomología de grupos profinitos.
Este documento está desarrollado como sigue: en el capítulo 1 veremos los aspectos básicos de la teoría de Galois, concluyendo con el teorema de krull (generalización del teorema fundamental de la teoría de Galois) y, además, veremos que un grupo de Galois de una extensión infinita es de hecho un grupo profinito. En el capítulo 2 empezaremos con las definiciones de cohomología de grupos, veremos como calcular los grupos de cohomología teniendo un grupo y daremos forma a los primeros tres grupos de cohomología. En el capítulo 3 veremos cohomología en el caso específico de grupos finitos, también se definira una conexión entre los grupos de cohomología de un grupo y sus grupos de homología, dicha relación estará dada por la cohomología de Tate. Finalmente, concluiremos en el capitulo 4 con la cohomología de los grupos de Galois, para esto, necesitaremos definir los grupos de cohomología para grupos profinitos, y por ende, para grupos de Galois de una extensión infinita.

Capítulo 2

Teoría de Galois

La teoría de Galois es una parte de la matemática cuyos orígenes se encuentran en el problema de la solubilidad de ecuaciones polinomiales mediante radicales. La teoría de Galois resolvió este problema, y a lo largo del camino, problemas geométricos clásicos de constructibilidad con regla y compás también quedaron resueltos. [6]

2.1. El grupo de k-automorfismos

La idea básica de la teoría de Galois es una idea que permea la matemática entera: asociarle a una estructura (algebraica en este caso) otro tipo de estructura y obtener información de estos objetos mediante el intercambio de ideas de una a otra estructura.[6]

Definición 2.1.1. *Sea L una extensión del campo k. Un k-automorfismo de L es un automorfismo de L que fija al campo k, i.e., isomorfismos de la forma $\sigma : L \to L$ tal que $\sigma|_k = id$.*

Lemma 2.1.2. *Sea L/k una extensión de campos. El conjunto de k-automorfismos de L, denotado $Aut(L/k)$ es un grupo con la composición de automorfismos.*

Demostración.

(i) Es claro que $id_L \in Aut(L/k)$.

(ii) Si $\sigma, \tau \in Aut(L/k)$ entonces $\sigma \circ \tau : L \to L$ es un isomorfismo tal que para todo $x \in k$ se tiene que $\sigma \circ \tau(x) = \sigma(\tau(x)) = \sigma(x) = x$ ya que $\tau|_k = id$ y $\sigma|_k = id$, y así, $\sigma \circ \tau \in Aut(L/k)$.

(iii) Si $\sigma \in Aut(L/k)$ entonces $\sigma^{-1} : L \to L$ es un isomorfismo, y si $x \in k$ se tiene que

$$\begin{aligned} x &= \sigma^{-1}(\sigma(x)) \\ &= \sigma^{-1}(x) \quad \text{ya que } \sigma|_k = id \end{aligned}$$

y así, $\sigma^{-1} \in Aut(L/k)$.

(iv) Como la composición de funciones es asociativa, se sigue que $Aut(L/k)$ es un grupo.

□

Definición 2.1.3. *Sea M un campo intermedio de L/k. En esta situación, usaremos la notación*

$$S(M) := Aut(L/M) \subseteq Aut(L/k),$$

para denotar al subgrupo del grupo $Aut(L/k)$ asociado al campo intermedio M. Se tiene así una función

$$S : \{\textit{Campos intermedios de } L/k\} = \mathcal{C}_{L/k} \to \{\textit{Subgrupos de } Aut(L/k)\} = \mathcal{G}_{L/k}.$$

Lemma 2.1.4. *La función $S : \mathcal{C}_{L/k} \to \mathcal{G}_{L/k}$ satisface:*

(1) Si $M_1 \subseteq M_2$ son campos intermedios, entonces S invierte inclusiones, i.e., $S(M_1) \supseteq S(M_2)$.

(2) Para el campo intermedio $M = k$ se tiene que $S(M) = Aut(L/k)$ es el grupo total.

(3) Para el campo intermedio $M = L$, se tiene que $S(L) = Aut(L/L) = \{id\}$ es el subgrupo trivial.

Ahora, dado un subgrupo H del grupo $G = Aut(L/k)$ queremos asociarle un campo intermedio entre L y k. Este campo se define como sigue: Dado $H \subseteq Aut(L/k)$ un subgrupo, sea

$$L^H := \{a \in L : \sigma(a) = a \forall \sigma \in H\}.$$

es decir, L^H es el subconjunto de todos los elementos de L que permanecen fijos bajo todos los automorfismos de $H \subseteq Aut(L/k)$.

Lemma 2.1.5. *Si H es un subgrupo de $Aut(L/k)$ entonces L^H es un campo intermedio entre L y k.*

Demostración. Como conjuntos se tiene que $k \subseteq L^H \subseteq L$. Ahora, L^H es un campo con las operaciones del campo grande L, ya que si $x, y \in L^H$ entonces para todo $\sigma \in H$ se tiene que

$$\sigma(x+y) = \sigma(x)\sigma(y) = x + y$$

y así, $x + y \in L^H$. Similarmente, si $x, y \in L^H$ entonces $x \cdot y \in L^H$. Las demás condiciones de campo se heredan del hecho de que L es un campo. □

Definición 2.1.6. *En la situación anterior, al campo intermedio L^H se le llama el campo fijo del subgrupo $H \subseteq Aut(L/k)$. Se tiene así una función*

$$F \ : \ \mathcal{G}_{L/k} \to \mathcal{C}_{L/k}$$

que a cada subgrupo $H \subseteq Aut(L/k)$ le asocia el campo fijo correspondiente $F(H) := L^H$.

Lemma 2.1.7. *La función $F \ : \ \mathcal{G}_{L/k} \to \mathcal{C}_{L/k}$ satisface:*

(1) Si $H_1 \subseteq H_2$ son subgrupos de $Aut(L/k)$, entonces F invierte inclusiones, es decir, $F(H_1) \supseteq F(H_2)$.

(2) Si H es un subgrupo de $Aut(L/k)$ entonces $H \subseteq S(F(H))$.

(3) Si M es un campo intermedio de L/k, entonces $M \subseteq F(S(M))$.

Demostración.

(1) Sea $x \in F(H_2) = L^{H_2}$, entonces $\sigma(x) = x \ \ \forall \sigma \in H_2$. Como lo anterior se cumple para todo σ en H_2, en particular se debe de cumplir para todo $\sigma' \in H_1 \subseteq H_2$.

(2) Si $\sigma \in H \subseteq Aut(L/k)$, entonces

$$S(F(H)) = Aut(L/L^H) = \{\tau \ : \ L \to L \ : \ \tau|_{L^H} = id\},$$

y como $L^H = \{x \in L \ : \ \sigma(x) = x \ \ \forall \sigma \in H\}$, entonces, para $\sigma \in H, \sigma|_{L^H} = id$ y así $\sigma \in Aut(L/L^H) = S(F(H))$.

(3) Similarmente como en el caso anterior.

□

En general, las funciones S y F no son inversas una de la otra, pero existen condiciones en las cuales estas funciones son inversas entre sí.

Teorema 2.1.8. *Sea k un campo. Entonces, cualquier conjunto finito de automorfismos distintos $\sigma_1, \ldots, \sigma_n : k \to k$ es independiente, i.e., si $a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0$ para todos los $x \in k$, entonces $a_i = 0$ para todos los $i = 1, \ldots, n$.*

Demostración. Por inducción sobre $n \geq 1$.

(i) $n = 1$: Si $a_1\sigma_1(x) = 0$ para todos los $x \in k$, entonces poniendo $x = 1$ se tiene que $a_1 = 0$.

(ii) Sea $n \geq 1$ y supongamos que calquier conjunto de menos de n automorfismos distintos es independiente.

(iii) Supongamos que los n automorfismos $\sigma_1, \ldots, \sigma_n$ son dependientes, i.e., se tiene una ecuación

$$a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0 \tag{2.1}$$

válida para todos los $x \in k$ y con algún $a_i \neq 0$. Nótese entonces que ninguno de los $a_j = 0$ ya que de lo contrario se tendría una ecuación

$$a_1\sigma_1(x) + \cdots + a_m\sigma_m(x) = 0$$

válida para todos los $x \in k$, con algún $a_i \neq 0$ y con $m < n$ automorfismos, en contradicción con la hipótesis de inducción.
Ahora, sin pérdida de generalidad, supongamos $\sigma_1 \neq \sigma_n$, exsite un elemento $a \in k, a \neq 0, 1$ tal que $\sigma_1(a) \neq \sigma_n(a)$.
Entonces, como la relación (1) es verdadera para todas las $x \in k$, reemplazando x por ax en esta ecuación se obtiene

$$a_1\sigma_1(a)\sigma_1(x) + \cdots + a_n\sigma_n(a)\sigma_n(x) = 0 \tag{2.2}$$

y multiplicando la ecuación (1) por $\sigma_1(a)$ se obtiene

$$a_1\sigma_1(a)\sigma_1(x) + \cdots + a_n\sigma_1(a)\sigma_n(x) = 0. \tag{2.3}$$

Substrayendo estas dos últimas ecuaciones obtenemos

$$a_2[\sigma_2(a) - \sigma_1(a)]\sigma_2(x) + \cdots + a_n[\sigma_n(a) - \sigma_1(a)] = 0, \tag{2.4}$$

y observamos que en esta última ecuación el coeficiente $a_n[\sigma_n(a) - \sigma_1(a)] \neq 0$ ya que $an \neq 0$ y $\sigma_n(a) \neq \sigma_1(a)$.
Así, (4) es una relación de dependencia no trivial entre $\sigma_2, \ldots, \sigma_n$ en contradicción con la hipótesis de inducción.

□

Como corolario de este teorema, obtenemos una cota para el orden del grupo de k-automorfismos de una extensión finita de campos:

Corolario 2.1.9. *Sea L/k una extensión finita. Entonces $|Aut(L/k)| \leq [L : k]$.*

Demostración. Sean $n = [L : k]$ y $u_1, \ldots, u_n \in L$ una base de L sobre k. Supongamos que $|Aut(L/k)| > n$. Entonces existen, al menos, $n+1$ k-automorfismos de L distintos, digamos $\sigma_1, \ldots, \sigma_n \in Aut(L/k)$. Consideremos ahora el sistema de ecuaciones lineales

$$\begin{aligned} \sigma_1(u_1)(x) + \cdots \qquad & +\sigma_{n+1}(u_1)x_{n+1} = 0 \\ \vdots & \\ \sigma_1(u_n)(x) + \cdots \qquad & +\sigma_{n+1}(u_n)x_{n+1} = 0 \end{aligned}$$

y obsérvese que como el número de ecuaciones n es menor que el número de incógnitas $n+1$, el sistema anterior tiene una solución no trivial $(a_1, \ldots, a_{n+1})$ en k, i.e., algún $a_i \leq 0$. Así, reemplazando esta solución en las ecuaciones del sistema se obtiene que

$$\sigma_1(u_j)a_1 + \cdots + \sigma_{n+1}(u_j)a_{n+1} = 0, \quad 1 \leq j \leq n$$

con algún $a_i \neq 0$.
Ahora, como $\{u_1, \ldots, u_n\}$ es una base de L/k, entonces para todo $x \in L$ existen $\alpha_1, \ldots, \alpha_n \in k$ tales que

$$x = \alpha_1 u_1 + \cdots + \alpha_n u_n$$

y así

$$\sigma_i(x) = \sigma_i \left(\sum_{j=1}^{n} \alpha_j u_j \right) = \sum_{j=1}^{n} \alpha_j \sigma_i(u_j)$$

ya que los $\alpha_j \in k$ y los $\sigma_j : L \to L$ son k-automorfismos. Se sigue que

$$\begin{aligned} a_1\sigma_1(x) + \cdots + a_{n+1}\sigma_{n+1}(x) &= \sum_{i=1}^{n+1} a_i \left(\sum_{j=1}^{n} \alpha_j \sigma_i(u_j) \right) \\ &= \sum_{j=1}^{n} \alpha_j \left(\sum_{i=1}^{n+1} a_i \sigma_i(u_j) \right) \\ &= \sum_{j=1}^{n} \alpha_j \cdot (0) \\ &= 0. \end{aligned}$$

Es decir, para todo $x \in L$ se tiene que

$$a_1\sigma_1(x) + \cdots + a_{n+1}\sigma_{n+1}(x) = 0$$

con algún $a_i \neq 0$, en contradicción con el teorema previo. □

2.2. Normalidad y separabilidad

Teorema 2.2.1. *Si $G = \{\sigma_1, \ldots, \sigma_n\}$ es un grupo finito de automorfismos de un campo L y si L^G es el campo fijo de G, entonces*

$$[L \ : \ L^G] = |G| = n.$$

Corolario 2.2.2. *Sea G un subgrupo finito del grupo de automorfismos de una campo L. Sea L^G el campo fijo de G. Entonces, $Aut(L/L^G) = G$.*

Corolario 2.2.3. *Sea L un campo. La función F que asigna a cada subgrupo finito G del grupo de automorfismos de L el correspondiente campo fijo L^G, es inyectiva.*

Demostración. Si G_1 y G_2 con dos subgrupos finitos de $Aut(L)$ tales que $L^{G_1} = L^{G_2}$, entonces por el corolario (2,2,2) anterior se tiene que

$$G_1 = Aut(L/L^{G_1}) = Aut(L/L^{G_2}) = G_2.$$

□

Definición 2.2.4. *Sean k un campo y $f(x)$ en $k[x]$. Una extensión L de k se llama un campo de descomposición de $f(x)$ sobre k, si*

(i) *$f(x)$ se descompone en factores lineales en $L[x]$.*

(ii) *Si M es otra extensión de k, donde $f(x)$ se descompone en factores lineales en $M[x]$ y $M \subseteq L$, entonces $M = L$.*

Las condiciones anteriores son equivalentes a:

(iii) *$L = k(\alpha_1, \ldots, \alpha_n)$, donde las α_i son las raíces de $f(x)$.*

Proposición 2.2.1. *Si k es un campo y $f(x) \in k[x]$ es un polinomio de grado ≥ 1, entonces existe un campo de descomposición L/k de $f(x)$, y más aún, $[L \ : \ k] \leq n!$, donde $n = gr(f(x))$.*

Lemma 2.2.5. *Sean $\phi : k \to k'$ un isomorfismo de campos y $f(x) \in k[x]$ un polinomio. Sea L un campo de descomposición de $f(x)$ sobre k, y sea L' una extensión de k' tal que $\phi(f(x)) \in k'[x]$ se descompone en factores lineales en $L'[x]$. Entonces, existe un monomorfismo $\psi : L \to L'$ tal que $\psi|_k = \phi$.*

Demostración. Gráficamente tenemos la situación

$$\begin{array}{ccc} L & \overset{\psi}{\dashrightarrow} & L' \\ | & & | \\ k & \xrightarrow[\phi]{} & k' \end{array}$$

donde la flecha punteada indica el morfismo que queremos construir, las flechas verticales son las extensiones dadas y $\phi : k \to k'$ es el isomorfismo dado.
El morfismo $\psi : L \to L'$ se construye usando inducción sobre el grado $n = gr(f)$. Observemos primero que como L es campo de descomposición de f sobre k, entonces en $L[x]$ se tiene que:

$$f(x) = c \cdot (x - \alpha_1) \cdots (x - \alpha_n) \tag{2.1}$$

con c una constante.
Si $m(x) = Irr(\alpha_1, k) := polinomioirreducibleseparabledeαconcoeficientesenk$, entonces $m(x)$ es un factor irreducible (en $k[x]$) de $f(x)$ y como el isomorfismo $\phi : k \to k'$ induce un isomorfismo de anillos $\phi : k[x] \to k'[x]$ de la manera natural, entonces $\phi(m(x))$ divide a $\phi(f(x))$ en $k'[x]$, y $\phi(m(x))$ es irreducible en $k'[x]$.
Ahora, por hipótesis, $\phi(f(x))$ se descompone en $L'[x]$, y como $\phi(m(x))$ es un factor de $\phi(f(x))$ entonces $\phi(m)$ también se descompone en $L'[x]$,

$$\phi(m(x)) = (x - \beta_1) \cdots (x - \beta_r),$$

$\beta_i \in L'$. Nótese que $\phi(m)$ es mónico porque $m(x)$ lo es. Ahora, como $\phi(m)$ es irreducible en $k'[x]$, entonces $\phi(m(x)) = Irr(\beta_i, k')$, para cada $1 \leq i \leq r$.
En particular, para β_1, estamos en la situación

$$\begin{array}{ccc} k(\alpha_1) & \overset{\psi_1}{\dashrightarrow} & k'(\beta_1) \\ | & & | \\ k & \xrightarrow[\phi]{} & k' \end{array}$$

donde $\phi(Irr(\alpha_1, k)) = Irr(\beta_1, k')$, y así, existe un isomorfismo ψ_1 tal que $\psi|_k = \phi$ y tal que $\psi_1(\alpha_1) = \beta_1$.

Ahora, como L es un campo de descomposición de f sobre k, entonces L es un campo de descomposición de $g := f/(x - \alpha_i)$ sobre k_{α_i}. Finalmente, como $gr(g) = n - 1 < gr(f)$, por hipótesis de inducción existe un monomorfismo

$$\psi \ : \ L \to L'$$

tal que $\psi|_{k(\alpha_1)} = \psi_1$. Pero como $\psi_1|_k = \phi$, entonces $\psi|_k = \phi$. □

Teorema 2.2.6. *Sean $\phi \ : \ k \to k'$ un isomorfismo de campos y $f(x) \in k[x]$ un polinomio. Sea L un campo de descomposición de f sobre k y sea L' un campo de descomposición de $\phi(f)$ sobre k'. Entonces, existe un isomorfismo $\psi \ : \ L \to L'$ tal que $\psi|_k = \phi$. (Es decir, las extensiones L/k y L'/k' son isomorfas).*

Demostración. Por el lema anterior existe un monomorfismo $\psi \ : \ L \to L'$ tal que $\psi|_k = \phi$.
Se puede observar que $\psi(L)$ es un campo de descomposición de $\phi(f)$ sobre k', y como $\psi(L) \subseteq L'$, entonces $\psi(L) = L'$ por definición de campo de descomposición (2,2,4)(ii). Entonces ψ es suprayectiva. □

Corolario 2.2.7. *Sean k un campo y $f(x) \in k[x]$ un polinomio. Si L y L' son campos de descomposición de $f(x)$ sobre k, entonces existe un isomorfismo $\psi \ : \ L \to L'$ tal que $\psi|_k = id$.*

Demostración. El corolario se sigue directamente del teorema anterior poniendo $\phi = id$. □

Definición 2.2.8. *Una extensión L/k se llama normal si todo polinomio irreducible $f(x) \in k[x]$ que tiene una raíz en L, las tiene todas.*

Ejemplo. La extensión $\mathbb{C}/\mathbb{R}$ es normal, ya que cualquier polinomio con coeficientes en $\mathbb{R}$ tiene todas sus raíces en $\mathbb{C}$.

Ejemplo. Si $\alpha = \sqrt{3}2 \in \mathbb{R}$, entonces la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$ no es normal, ya que el polinomio irreducible $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ tiene sólo una raíz $\alpha \in \mathbb{Q}(\alpha)$ pero no tiene a las otras.

El siguiente teorema nos relaciona el concepto de normalidad con el de campo de descomposición: [6]

Teorema 2.2.9. *Una extensión L/k es normal y finita si y sólo si L es el campo de descomposición de algún polinomio en $k[x]$.*

Ahora introduciremos el concepto de separabilidad, empezando con la definición de polinomio separable, siguiendo con la definición de elemento separable y finalmente con extensión separable.

Definición 2.2.10. *Un polinomio irreducible $f(x) \in k[x]$ se llama separable sobre k si no tiene raíces múltiples (en su campo de descomposición). Un polinomio irreducible $f(x) \in k[x]$ se llama inseparable (sobre k) si no es separable.*

Así, un polinomio separable $f(x) \in k[x]$ se factoriza (en un campo de descomposición) como

$$f(x) = c \cdot (x - \alpha_1) \cdots (x - \alpha_n)$$

con $c \in k$ y α_i distintas.
Para determinar si un polinomio $f(x) \in k[x]$ es o no separable, debemos tener un criterio para saber si tiene raíces múltiples. En el caso de polinomios con coeficientes en $\mathbb{R}$ ó $\mathbb{C}$ se puede utilizar la derivada para dicho criterio, pero como estamos tratando con polinomios con coeficientes en un campo arbitrario, es necesario formalizar el concepto de derivada de un polinomio que sea compatible con $\mathbb{R}$ y $\mathbb{C}$.

Definición 2.2.11. *Si $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in k[x]$, su derivada es el polinomio*

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in k[x].$$

Las propiedades siguientes son inmediatas de esta definición:

Lemma 2.2.12. *Sea k un campo y sean $f, g \in k[x]$. Entonces*

(1) $(f + g)' = f' + g'$

(2) $(f \cdot g) = f \cdot g' + f' \cdot g$.

y para el polinomio constante $f = a \in k$, se tiene que

(3) $(a)' = 0$, *y consecuentemente*

(4) $(a \cdot f)' = a \cdot f'$, *para toda $a \in k$.*

Lemma 2.2.13. *Sea k un campo. Un polinomio $f(x) \in k[x]$ no cero, tiene una raíz múltiple (en un campo de descomposición) si y sólo si f y f' tiene un factor común de grado ≥ 1 en $k[x]$.*

Demostración. Sea L un campo de descomposición de $f(x)$.

Si $\alpha \in L \supseteq k$ es un cero de multiplicidad $m \geq 2$ de $f(x)$, entonces en $L[x]$,

$$f(x) = (x-\alpha)^m g(x), \qquad m \geq 2,$$

y así, por el lema (2,2,12),

$$\begin{aligned} f'(x) &= m(x-\alpha)^{m-1}g(x) + (x-\alpha)^m g'(x) \\ &= (x-\alpha)^{m-1}[mg(x) + (x-\alpha)g'(x)] \end{aligned}$$

con $m-1 \geq 1$. Así, $f(x)$ y $f'(x)$ tienen el factor común $(x-\alpha)^{m-1}$ de grado ≥ 1.

Si f no tiene ceros de multiplicidad ≥ 2, mostraremos que f y f' son coprimos en $L[x]$, por inducción sobre $n = gr(f) \geq 1$.
Si $n = 1$ no hay nada que probar.
Supongamos válido el lema para polinomios de grado $\leq n-1$.
Como f no tiene ceros múltiples, entonces para cualquier raíz de f se tiene que

$$f(x) = (x-\alpha)g(x)$$

donde $(x-\alpha) \nmid g(x)$. Entonces,

$$f'(x) = (x-\alpha)g'(x) + g(x),$$

y por lo tanto, si f y f' tuvieran un factor irreducible de grado ≥ 1, este factor no puede ser $(x-\alpha)$ ya que $(x-\alpha) \nmid g(x)$. Pero tampoco puede ser diferente de $(x-\alpha)$ ya que entonces este factor irreducible dividiría a $g(x)$, y de la expresión para $f'(x)$, también dividiría a $g'(x)$. Pero como $gr(g) = n-1$, esto no puede suceder ya que por hipótesis de inducción, g y g' no tiene factores en común de grado ≥ 1. □

Como consecuencia del lema anterior tenemos el siguiente criterio que ayuda a determinar cuando un polinomio irreducible es separable:

Corolario 2.2.14. *Sean k un campo y $f(x) \in k[x]$ irreducible.*

(1) Si $car(k) = 0$, entonces $f(x)$ es separable sobre k.

(2) Si $car(k) \neq 0$, entonces $f(x)$ es inseparable si y sólo si $f(x)$ es de la forma $f(x) = g(x^p)$ con $g \in k[x]$. (Esta última condición dice que las potencias de la indeterminada x que aparecen en $f(x)$ son sólo aquellas cuyo exponente es un múltiplo (entero) de p).

Demostración. Por el lema anterior, f es inseparable si y sólo si f y f' tienen un factor común de grado ≥ 1.
Ahora, como f es irreducible, y también $gr(f') < gr(f)$, entonces f y f' tiene un factor común de grado ≥ 1 si y sólo si $f' = 0$. Pero como

$$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1},$$

entonces:

(1) $car(k) = 0$ implica que $ja_j = 0$ para $j \geq 1$, y así, $a_j = 0$ (en característica cero $j \geq 1$ no es cero en k) y entonces $f(x) = a_0$ en contradicción con la hipótesis de que $f(x)$ es irreducible (y por lo tanto no es constante). Se sigue que $f(x)$ debe ser separable.

(2) $car(k) \neq 0$ implica que $ja_j = 0$ para $j \geq 1$, y así, $a_j = 0$ ó $j \equiv 0 \pmod p$, i.e., $j = pm_j$ con $m_j \in \mathbb{N}$ y por lo tanto f es de la forma

$$\begin{aligned} f(x) &= a_0 + a_px^p + \cdots + a_{ip}x^{ip} + \cdots \\ &= g(x^p) \end{aligned}$$

con $g(x) = a_0 + a_px^p + \cdots + a_{ip}x^{ip} + \cdots$, como se quería demostrar.

□

Finalmente, definimos lo que es un elemento separable y una extensión separable:

Definición 2.2.15. *Si L/k es una extensión, un elemento $\alpha \in L$ algebraico sobre k, se llama separable sobre k, si $Irr(\alpha, k) \in k[x]$ es separable. Una extensión algebraica L/k es separable si todo $\alpha \in L$ es separable sobre k. Un polinomio arbitrario $f(x) \in k[x]$ se llama separable sobre k, si todos sus factores irreducibles son separables sobre k.*

Proposición 2.2.2. *Sea L/k una extensión algebraica separable. Si $k \subseteq M \subseteq L$ es un campo intermedio, entonces las subextensiones L/M y M/k también son separables.*

Demostración. La extensión M/k es separable ya que $M \subseteq L$.
Para la extensión L/M, sea $\alpha \in L$ un elemento arbitrario, y sean $m_k = Irr(\alpha, k)$ y $m_M = Irr(\alpha, M)$. Entonces, en $M[x], m_M \mid m_k$. Pero como α es separable sobre k, m_k es separable sobre k, i.e., no tiene raíces múltiples, y por lo tanto tampoco m_M ya que es factor de m_k. Se sigue que α es separable sobre M, i.e., L/M es separable. □

El siguiente teorema relaciona los conceptos de normalidad y separabilidad de una extensión finita L/k con la condición del teorema de Artin (2,2,2), i.e., con la condición de que $k = L^{Aut(L/k)}$.

Teorema 2.2.16. *Sea L/k una extensión finita con grupo de automorfismos (finito) $G = Aut(L/k)$. Las afirmaciones siguientes son equivalentes:*

(1) L/k es normal y separable.

(2) L es el campo de descomposición de un polinomio separable $p(x) \in k[x]$.

(3) k es el campo fijo de G.

Demostración.

(1) $\Rightarrow$ (2): Como L/k es finita, entonces $L = k(\alpha_1, \ldots, \alpha_n)$ con α_i algebraico sobre k, y como la extensión L/k es separable entonces los α_i son separables sobre k, i.e., los polinomios

$$p_i(x) = Irr(\alpha_i, k) \in k[x]$$

son separables sobre k.
También, como L/k es normal y cada $\alpha_i \in L$ es una raíz de $p_i(x)$ entonces cada $p_i(x)$ se descompone en L. Sea

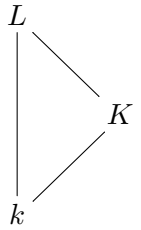
$$p(x) := p_1(x) \cdot \cdots \cdot p_n(x) \in k[x].$$

Como todos los factores irreducibles $p_i(x)$ de $p(x)$ son separables entonces $p(x)$ es separable, y se descompone en L. Finalmente, como $\alpha_i, \ldots, \alpha_n$ son raíces de $p(x)$ entonces $L = k(\alpha_1, \ldots, \alpha_n)$ es el campo de descomposición del polinomio separable $p(x) \in k[x]$.

(2) $\Rightarrow$ (3): Sea $p(x) \in k[x]$ separable tal que L es el campo de descomposición de $p(x)$. Mostraremos que $k = L^G$, $G = Aut(L/k)$, por inducción sobre el número de raíces de $p(x)$ en $L - k$.

(i). Si el número de raíces de $p(x)$ en $L - k$ es 0, entonces todas las raíces de $p(x)$ están en k y así $L = k$ y consecuentemente $G = Aut(L/k) = \{id\}$ y ciertamente $k = L^G = L$.

(ii). Si el número de raíces de $p(x)$ en $L-k$ es $n>0$, nuestra hipótesis de inducción es: Para cualquier campo intermedio K:



(ciertamente entonces $p(x)\in K[x]$ y L sigue siendo campo de descomposición de $p(x)$ sobre K), supongamos que siempre que $p(x)$, ahora visto en $K[x]$, tenga menos que n raíces en $L-K$, se tiene que

$$K=L^{Aut(L/k)}.$$

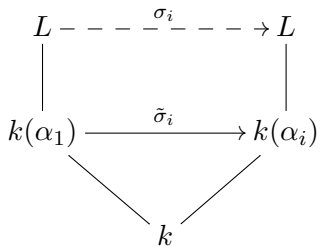
Ahora, consideremos una factorización de $p(x)\in k[x]$ en factores irreducibles en $k[x]$:

$$p(x)=p_1(x)\cdots p_r(x).$$

Obsérvese que algunos de estos factores $p_i(x)$ deben tener grado ≥ 1 ya que de los contrario $p(x)$ se descompondría en k en contradicción con la hipótesis de que $p(x)$ tiene raíces en $L-k$. Sin perder generalidad, supongamos que $gr(p_1(x))=s>1$.
Como, por hipótesis, $p(x)$ es separable, entonces $p_1(x)$ también es separable. Sean $\alpha_1,\ldots,\alpha_s$ las raíces distintas de $p_1(x)(gr(p_1)=s)$. Como las α_i también son raíces de $p(x)$, y este se descompone en L entonces todas las $\alpha_i\in L$ y de hecho $\alpha_i\in L-k$ ya que $p_i(x)$ es irreducible sobre k (i.e., todas sus raíces no están en k).
Ahora, para $p(x)\in k[x]\subseteq k(\alpha_1)[x]$ se tiene que L también es campo de descomposición de $p(x)$ considerado como polinomio sobre $k(\alpha_1)$. También, como α_1 es una raíz de $p(x)$ que no está en k, entonces el polinomio $p(x)\in k(\alpha_1)[x]$ tiene menos que n raíces en $L-k(\alpha_1)$.
Por hipótesis de inducción se tiene que

$$k(\alpha_1)=L^{Aut(L/k(\alpha_1))}.$$

Consideremos ahora las extensiones $L \supseteq k(\alpha_i) \supseteq k$, para $1 \leq i \leq s$:



y obsérvese que como las $\alpha_i, 1 \leq i \leq s$, son raíces del mismo polinomio irreducible $p_1(x) \in k[x]$, entonces existen isomorfismos $\tilde{\sigma}_i : k(\alpha_1 \to k(\alpha_i)$ tales que $\tilde{\sigma}_i|_k = id$ y $\tilde{\sigma}_i(\alpha_1) = \alpha_i$.
También como L es campo de descomposición de $p(x)\ ink(\alpha_1)[x]$ y por la misma razón L es campo de descomposición de $p(x)$ considerado como polinomio sobre $k(\alpha_i)$, $1 \leq i \leq s$, entonces por (2,2,7) existen isomorfismos $\sigma_i \in Aut(L/k)$.
Finalmente, mostraremos que $k = L^{Aut(L/k)}$: Sea $\theta \in L$ cualquier elemento que permanece fijo bajo la acción de todos los $\sigma \in Aut(L/k)$. Mostraremos que $\theta \in k$.
Obsérvese primero que $\theta \in L^{Aut(L/k(\alpha_1))}$ ya que $Aut(L/k(\alpha_1)) \subseteq Aut(L/k)$ y así θ queda fijo bajo la acción de $Aut(L/k(\alpha_1))$ ya que estaba ya fijo por $Aut(L/k)$, y así, por hipótesis de inducción $\theta \in k(\alpha_1)$.
Ahora, como $\theta \in k(\alpha_1)$ y $1, \alpha_1, \ldots, \alpha_1^{s-1}$ es una base de $k(\alpha_1)$ sobre k, entonces

$$\theta = c_0 + c_1\alpha_1 + \cdots + c_{s-1}\alpha_1^{s-1} \quad \text{con } c_i \in k,$$

y si ahora aplicamos a esta expresión para los θ los isomorfismos $\sigma_i \in Aut(L/k)$ y, recordamos que $\sigma_i|_{k(\alpha_i)} = \tilde{\sigma}_i$, obtenemos:

$$\begin{aligned}\theta = \sigma_i(\theta) &= c_0 + c_1\tilde{\sigma}_i(\alpha_1) + \cdots + c_{s-1}\tilde{\sigma}_i\alpha_1^{s-1} \\ &= c_0 + c_1\alpha_1 + \cdots + c_{s-1}\alpha_i^{s-1}\end{aligned}$$

para $1 \leq i \leq s$. Y así, el polinomio

$$q(x) := (c_0 - \theta) + c_1x + \cdots + c_{s-1}x^{s-1} \in k(\alpha_1)[x].$$

de grado a lo más $s-1$ tiene las s raíces distintas $\alpha_1, \ldots, \alpha_s$. Se sigue que todos sus coeficientes deben ser cero. En particular, $c_0 - \theta = 0$, i.e., $\theta = c_0 \in k$ como se quería.

(3) $\Rightarrow$ (1): Escribamos $G = Aut(L/k) = \{\sigma_1, \ldots, \sigma_n\}$. Nuestra hipótesis es: $k = L^G$.

(i). Mostraremos que L/k es separable: Sea $\alpha \in L$ cualquier elemento. Aplicando los σ_j a α se obtiene el conjunto $\{\sigma_j(\alpha) \in L \ : \ 1 \leq j \leq n\}$. Supongamos que $\alpha = \alpha_1, \ldots, \alpha_n$ son los elementos distintos en este conjunto ($\sigma_1 = id$).
Como G es un grupo, para toda j se tiene que:

$$\begin{aligned} \sigma_j(\alpha_i) &= \sigma_j(\sigma_k(\alpha)) \quad \text{si } \alpha_i = \sigma_k(\alpha) \\ &= \sigma_j\sigma_k(\alpha) \\ &= \sigma_t(\alpha) \\ &= \alpha_l \quad \text{para algún } 1 \leq l \leq s, \end{aligned}$$

i.e., los elementos del conjunto $\alpha_1, \ldots, \alpha_s$ son permutados por los elementos σ_i del grupo G. Así, los morfismos de anillos

$$\sigma_t \ : \ L[x] \to L[x]$$

son tales que cuando se aplican al polinomio

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_s) \in L[x]$$

se obtiene que:

$$\begin{aligned} \sigma_i(p(x)) &= \sigma_i(x - \alpha_i) \cdots \sigma_i(x - \alpha_s) \\ &= (x - \sigma_i(\alpha_i)) \cdots (x - \sigma_i(\alpha_s)) \\ &= p(x) \end{aligned}$$

ya que los σ_i sólo permutan a los $\alpha_1, \ldots, \alpha_s$. Se sigue que los coeficientes de $p(x)$ son fijados por la acción del grupo G, y así por hipótesis estos coeficientes deben estar en $L^G = k$, i.e., $p(x) \in k[x]$.
Hemos así construido un polinomio separable $p(x) \in k[x]$ del cual $\alpha = \alpha_1$ es raíz. Se sigue que $\alpha \in L$ es separable sobre k ya que su irreducible $Irr(\alpha, k) \in k[x]$ es tal que $Irr(\alpha, k) \mid p(x)$ ya que si $g(x) \in k[x]$ es cualquier polinomio con $g(\alpha) = 0$, entonces

$$0 = \sigma_i(g(\alpha)) = g(\sigma_i(\alpha)) = g(\alpha_i)$$

pues los coeficientes de g están en k, y así son fijados por σ_i. Entonces, todas las raíces $\alpha_1, \ldots, \alpha_s$ de $p(x)$ también son raíces de $g(x)$ y así $p(x) \mid g(x)$. En particular, para $g(x) = Irr(\alpha, k)$, como $p(x)$ es mónico, y $p(x) \mid Irr(\alpha, k)$, se sigue que $p(x) = Irr(\alpha, k)$.

(ii). La extensión L/k es normal: En efecto, sea $f(x) \in k[x]$ cualquier polinomio irreducible tal que tiene una raíz $\alpha \in L$.
Sea $p(x) \in k[x]$ el polinomio irreducible separable de α, $p(x) = Irr(\alpha, k)$ construido en (i). Por construcción en (i), $p(x)$ se descompone en L.
Ahora, como $p(x)$ y $f(x)$ son irreducibles sobre k y $p(\alpha) = 0 = f(\alpha)$, entonces $p(x) \mid f(x)$ y $f(x) \mid p(x)$ en $k[x]$. Se sigue que

$$f(x) = ap(x) \quad \text{con } a \in k^*,$$

y como $p(x)$ se descompone en L entonces $f(x)$ también se descompone en L.

□

2.3. El teorema fundamental de Galois

Si L/k es una extensión finita, normal y separable (de Galois), al grupo de automorfismos $Aut(L/k)$ se le llama el grupo de Galois de la extensión y se le denota $Gal(L/k)$.
Del teorema (2,2,16) y del corolario (2,2,3) se sigue, que si L/k es una extensión de Galois, la función (2,1,6)

$$F \ : \ \mathcal{G}_{L/k} \to \mathcal{C}_{L/k}$$

que asigna a cada subgrupo H del grupo de Galois $G = Gal(L(k)$ el campo fijo $F(H) := L^H$ es inyectiva. A continuación veremos que bajo las mismas hipótesis sobre L/k, la función F también es suprayectiva, con inversa la función S de (2,1,3), y de hecho obtenemos mucho más como parte del teorema fundamental de la teoría de Galois: Sabemos por (2,1,4) y (2,1,7) que las funciones

$$F \ : \ \mathcal{G}_{L/k} \to \mathcal{C}_{L/k}$$

y

$$S \ : \ \mathcal{C}_{L/k} \to \mathcal{G}_{L/k}$$

satisfacen

(i) F y S invierten inclusiones,

(ii) Para todo $H \subseteq Gal(L/k)$, se tiene que $H \subseteq SF(H)$,

(iii) Para todo campo intermedio $L \supseteq M \supseteq k$, se tiene que $M \subseteq FS(M)$.

Teorema 2.3.1. *Sea L/k una extensión finita, normal y separable y sea $G = Gal(L/k)$ el grupo (finito) de Galois de la extensión. Entonces*

(1) $|Gal(L/k)| = [L : k]$,

(2) Las funciones F y S son inversas una de la otra.

(3) Si M es un campo intermedio, $L \supseteq M \supseteq k$, entonces:

(i) $|S(M)| = |Gal(L/M)| = [L : M]$,

(ii) $[M : k] = |G|/|S(M)| = [G : S(M)] =$ *índice de $S(M)$ en $G = Gal(L/k)$.*

(4) Si M es un campo intermedio, $L \supseteq M \supseteq k$, entonces M/k es normal si y sólo si $Gal(L/M) \subseteq Gal(L/k)$ es un subgrupo normal.

(5) Si para un campo intermedio M, la extensión M/k es normal, entonces el grupo de Galois $Gal(M/k)$ es isomorfo al grupo cociente $Gal(L/k)/Gal(L/M)$.

Demostración. (1) Como L/k es Galois, entonces por el teorema (2,2,16), $k = L^{Gal(L/k)}$ y así, por (2,2,1) se tiene que

$$|Gal(L/k)| = [L : k].$$

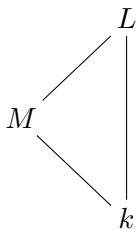
(2) La función $F : \mathcal{G}_{L/k} \to \mathcal{C}_{L/k}$ es inyectiva por (2,2,3), y

$$\begin{aligned} H &= Gal(L/L^H) \quad \text{por (2,2,2)} \\ &= Gal(L/F(H)) \quad \text{por definición de } F \\ &= SF(H) \quad \text{por definición de } S. \end{aligned}$$

Finalmente, que $F : \mathcal{G} \to \mathcal{C}$ es suprayectiva es porque como L/k es de Galois, por el teorema previo se tiene que L es el campo de descomposición de un polinomio separable $p(x) \in k[x]$, y así si $M \in \mathcal{C}_{L/k}$ es un campo intermedio, entonces L también es campo de descomposición de $p(x)$ sobre M. Por el teorema (2,2,16) anterior se sigue que L/M también es de Galois y así $M = L^{Gal(L/M)}$ por el mismo teorema, i.e., $M = F(Gal(L/M))$ con $Gal(L/M) \in \mathcal{G}_{L/k}$. Más aún,

$$M = L^{Gal(L/M)} = F(Gal(L/M)) = FS(M). \tag{2.2}$$

(3) Sea M un campo intermedio



(i): Como en la demostración (2) de arriba, L/M es de Galois y así, por la parte (1) se tiene que:

$$[L\ :\ M] = |Gal(L/M)| = |S(M)|$$

por definición de S.

(ii): $[M\ :\ k] = [L\ :\ k]/[L\ :\ M] = |Gal(L/k)|/|S(M)|$ por las partes (1) y (3)(i)

Para probar las partes (4) y (5) del teorema necesitaremos los lemas siguientes:

Lemma 2.3.2. *Sea M/k una extensión finita. Son equivalentes:*

(1) M/k es normal

(2) Para cualquier extensión L de M tal que L/k es normal y finita, se tiene que todo morfismo $\tau\ :\ M \to L$ que deja fijo a k es de hecho un k-automorfismo $\tau\ :\ M \to M$.

Demostración.

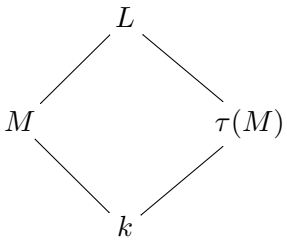
(1) $\Rightarrow$ (2): Sea $\tau\ :\ M \to L$ un monomorfismo tal que $\tau|_k = id$. Queremos probar que $\tau(M) = M$. Sea $\alpha \in M$ y sea $p(x) = Irr(\alpha, k) \in k[x]$. Entonces,

$$0 = p(\alpha) = \tau(p(\alpha)) = p(\tau(\alpha)),$$

ya que los coeficientes de $p(x)$ están en k y $\tau|_k = id$.
Así, $\tau(\alpha) \in L$ es una raíz de $p(x)$ también. Ahora, como M/k es normal por hipótesis y $p(x) \in k[x]$ es irreducible con $\alpha \in M$ una raíz de $p(x)$, entonces todas las raíces de $p(x)$ deben estar en M. En particular $\tau(\alpha) \in M$. Así,

$$\tau(M) \subseteq M.$$

Finalmente, en el diagrama siguiente

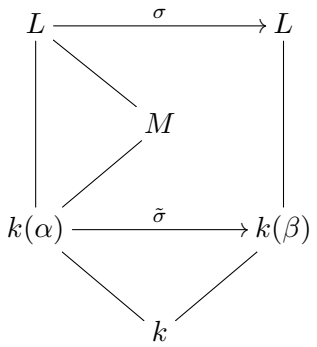


como la función $\tau \ : \ M \to \tau(M) \subseteq M$ es k-lineal e inyectiva, entre k-espacios vectoriales de dimensión finita, entonces de

$$dim_k(M) = dim_k\tau(M) < \infty \quad \text{y} \quad \tau(M) \subseteq M$$

se sigue que $\tau(M) = M$, i.e., $\tau \in Aut(M/k)$.

(2) $\Rightarrow$ (1): Sea $p(x) \in k[x]$ irreducible tal que tiene una raíz $\alpha \in M$. Como $\alpha \in M \subseteq L$ y L/k es normal, entonces $p(x)$ se descompone en L.
Ahora, si $\beta \in L$ es una raíz cualquiera de $p(x)$, consideremos el diagrama



donde, como α y β son raíces del mismo irreducible $p(x) \in k[x]$, existe un k-isomorfismo

$$\tilde{\sigma} \ : \ k(\alpha) \to k(\beta)$$

tal que $\tilde{\sigma}(\alpha) = \beta$.
Ahora, como L/k es normal y finita, entonces por (2,2,16), L es el campo de descomposición de un polinomio $f(x) \in k[x]$. Así, ciertamente, L es el campo de descomposición de $f(x)$ considerado ahora como polinomio en $k(\alpha)$ ó $k(\beta)$. Entonces, por (2,2,6) existe un isomorfismo

$$\sigma \ : \ L \to L$$

tal que $\sigma|_{k(\alpha)} = \tilde{\sigma}$ y así $\sigma(\alpha) = \beta$. Pero $\alpha \in M$, y así

$$\beta = \sigma(\alpha) = \sigma|_M(\alpha);$$

y como $\sigma|_M \ : \ M \to L$ es un monomorfismo tal que $(\sigma|_M)|_k = id$, por hipótesis se debe tener que $\sigma|_M(M) = M$, i.e., $\beta = \sigma|_M(\alpha) \in M$, i.e., todas las raíces de $p(x)$ están en M.

□

Lemma 2.3.3. *Sean L/k una extensión finita, normal y separable y M un campo intermedio. Sea $\tau \in Gal(L/k)$. Entonces:*

$$S(\tau M) = \tau S(M)\tau^{-1}$$

donde $S(M) = Gal(L/M)$.

Demostración. Sea $\gamma \in S(M)0subseteqGal(L/k)$ cualquier elemento y sea $x' \in \tau(M)$ arbitrario. Así, $x' = \tau(x)$ para algún $x \in M$. Entonces

$$\begin{aligned} \tau\gamma\tau^{-1}(x') &= \tau\gamma\tau^{-1}(\tau(x)) \\ &= \tau\gamma(x) \\ &= \tau(x) \quad \text{ya que } x \in M \text{ y } \gamma \in Gal(L/M) \\ &= x', \end{aligned}$$

i.e., $\tau\gamma\tau^{-1} : L \to L$ deja fijo a $\tau(M)$, i.e., para todo $\gamma \in S(M) = Gal(L/M)$ se tiene que

$$\tau\gamma\tau^{-1} \in Gal(L/\tau(M)) = S(\tau(M))$$

i.e.,

$$\tau S(M)\tau^{-1} \subseteq S(\tau(M)).$$

Recíprocamente, tomando $S(\tau(M))$ en lugar de $S(M)$ se tiene que

$$\tau^{-1}(S(\tau(M)))\tau \subseteq S(M)$$

y así

$$S(\tau(M)) \subseteq \tau S(M)\tau^{-1}.$$

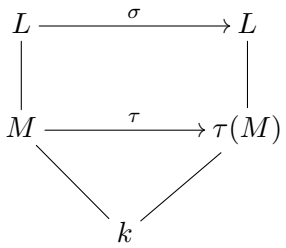
□

Con estos dos lemas, se puede finalizar la demostración del teorema principal.

(4) Sea M un campo intermedio con M/k normal:
Queremos probar que $S(M) := Gal(L/M) \lhd Gal(L/k)$, i.e., queremos mostrar que para todo $\tau \in Gal(L/k)$ se tiene que $\tau S(M)\tau^{-1} = S(M)$.
Ahora, por el lema (2,3,3), $\tau S(M)\tau^{-1} = S(\tau(M))$, y así lo que debemos probar es que $\tau(M) = M$.
Pero como $\tau : L \to L$ es un k-automorfismo entonces $\tau|_M : M \to L$ es un monomorfismo que deja fijo a k. Y como por hipótesis M/k es normal, se sigue del lema (2,3,2) que $\tau(M) = M$ como se quería.

Supongamos ahora que $S(M) \lhd Gal(L/k)$ es un subgrupo normal. Queremos

probar que M/k es normal usando el lema (2,3,2), y para ésto sea $\tau : M \to L$ un k-monomorfismo con L/k finita normal y consideremos el diagrama siguiente:



y observemos que como L/k es finita, normal y separable, por (2,2,16), L es campo de descomposición de un polinomio separable $p(x) \in k[x]$, y así también es campo de descomposición de $p(x)$ considerado ahora como polinomio en $M[x]$. Ahora, como $\tau|_k = id$, entonces $\tau(p(x)) = p(x)$, y así, L es campo de descomposición de $p(x) \in \tau(M)[x]$. Por la unicidad de los campos de descomposición (2,1,6), se sigue que existe un isomorfismo $\sigma : L \to L$ tal que $\sigma|_M = \tau$ y por lo tanto $\sigma|_k = id$, y así $\sigma \in Gal(L/k)$.
Ahora, como $S(M) \lhd Gal(L/k)$, entonces

$$\sigma S(M)\sigma^{-1} = S(M),$$

pero, por el lema (2,3,3), $\sigma S(M)\sigma^{-1} = S(\sigma M) = S(\tau M)$, la última igualdad porque $\sigma|_M = \tau$. Se sigue que

$$S(M) = S(\tau M),$$

y como S es inyectiva por la parte (2) del teorema principal, entonces $M = \tau M$ para todo k-monomorfismo $\tau : M \to L$, y así por el lema (2,3,2), M/k es normal.

(5) Sea M un campo intermedio de L/k tal que M/k es normal. Queremos probar que $Gal(M/k) \approx Gal(L/k)/Gal(L/M)$. Para esto, sea

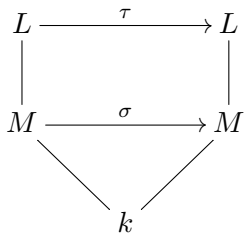
$$\phi : Gal(L/k) \to Gal(M/k)$$

definida por

$$\phi(\tau) := \tau|_M$$

y obsérvese que como M/k es normal, entonces por el lema (2,3,2) se sigue que $\tau|_M$ es en efecto un k-automorfismo de M, i.e., $\tau|_M \in Gal(M/k)$. Claramente, ϕ es un homomorfismo de grupos. Probaremos que ϕ es suprayectiva con núcleo $Gal(L/M)$.

(i) ϕ es suprayectivo: Sea $\sigma \in Gal(M/k)$ y consideremos el diagrama



Como L/k es finita, normal y separable, por el teorema (2,2,16), L es el campo de descomposición de un polinomio separable $p(x) \in k[x]$. Así, ciertamente, L también es el campo de descomposición de $p(x)$ considerado ahora como polinomio en $M[x]$. Y como $\sigma|_k = id$, entonces para $p(x) \in k[x]$ se tiene que $\sigma(p(x)) = p(x)$. Entonces, por la unicidad de los campos de descomposición (2,2,6) existe un isomorfismo $\tau : L \to L$ tal que $\tau|_M = \sigma$, y así $\tau|_k = \sigma|_k = id$, i.e., $\tau \in Gal(L/k)$ y entonces $\phi(\tau) = \tau|_M = \sigma$.

(ii) Finalmente,

$$\begin{aligned} ker\ \phi &= \{\tau \in Gal(L/k) : \tau|_M = id\} \\ &= \{\tau : L \to L \ \ isomorfismo : \tau|_M = id\} \\ &= Gal(L/M). \end{aligned}$$

□

2.4. Extensiones de Galois infinitas

Sea Ω/k una extensión de Galois posiblemente infinita. En primer lugar, esta la observación de que Ω es la unión de extensiones de Galois finitas de k, o bien:

Lemma 2.4.1. *Cada subextensión finita de Ω/k puede ser cubierta por una subextensión de Galois.*

Demostración. Por el teorema del elemento finito, cada subextensión finita es de la forma $f(\alpha)$, para algún elemento α apropiado. Entonces, cubriremos a $k(\alpha)$ con el campo separable del polinomio minimo de α, que es Galois sobre k. □

Definición 2.4.2. *Un sistema inverso de grupos $(G_\alpha, \phi_{\alpha\beta})$ consiste de:*

- *un conjunto parcialmente ordenado $(\Lambda, \leq)$ tal que para todo $(\alpha, \beta) \in \Lambda$ existe algún $\gamma \in \Lambda$ tal que $\alpha \leq \gamma$, $\beta \leq \gamma$;*

- *para cada $\alpha \in \Lambda$, existe el grupo G_α;*
- *para cada $\alpha \leq \beta$ existe un homomorfismo $\phi_\beta^\alpha : G_\beta \to G_\alpha$ tal que $\phi_\gamma^\alpha = \phi_\beta^\alpha \circ \phi_\gamma^\beta$ para $\alpha \leq \beta \leq \gamma$.*

El limite inverso del sistema está definido como el subgrupo de los productos directos $\prod_{\alpha\in\Lambda} G_\alpha$ que consisten de las sucesiones (g_α) tal que $\phi_\beta^\alpha(g_\beta) = g_\alpha$ para toda $\alpha \leq \beta$. Se denota por $\varprojlim G_\alpha$;

Definición 2.4.3. *Un grupo profinito es el limite inverso de un sistema (inverso) de grupos finitos. Para un número primo p, un pro-p-grupo es el límite inverso de p-grupos finitos.*

Ejemplos.

(1) Todo grupo finito es profinito; es el límite inverso del sistema $(G_\alpha, \phi_\beta^\alpha)$ con $G_\alpha = G$ y $\phi_\beta^\alpha = id_G$.

(2) Tomando $\mathbb{Z}$, sea Λ el conjunto $\mathbb{Z}_{>0}$, ya que cada subgrupo de índice finito está generado por algún entero positivo m. El orden parcial está inducido por la relación de división: $m|n$ si y sólo si $m\mathbb{Z} \supset n\mathbb{Z}$.

Proposición 2.4.1. *Sea Ω/k una extensión de Galois de campos. Los grupos de Galois de subextensiones finitas de Ω/k junto con los homomorfismos $\phi_L^M : Gal(M/k) \to Gal(L/k)$ forman un sistema inverso cuyo límite inverso es isomorfo a $Gal(\Omega/k)$. En particular, $Gal(\Omega/k)$ es un grupo profinito.*

Demostración. Solamente necesitamos probar la parte de los isomorfismos. Para esto, definimos un homomorfismo de grupos $\phi : Gal(\Omega/k) \to \prod Gal(L/k)$ (donde el producto es sobre todas las subextensiones finitas de Galois L/k) como sigue: tomamos un k-automorfismo σ de Ω y lo mandamos al producto directo de sus reestricciones a los subcampos L. Entonces $\sigma(L) \subset L$ para toda L (como resultado de la teoría finita de Galois). El morfismo ϕ es inyectivo, ya que si un automorfismo σ no fija un elemento α de k_s, entonces su restricción a una subextensión finita de Galois que contiene a $k(\alpha)$ es no-trivial (dicha extensión siempre existe). Por otro lado, el teorema fundamental de la teoría de Galois asegura que la imagen de ϕ está contenida en $\varprojlim Gal(\Omega/k)$. Veremos ahora que $Im(\phi) = \varprojlim Gal(\Omega/k)$: tomamos un elemento $(\sigma_L) \in \varprojlim Gal(L/k)$ y definimos un k-automorfismo σ de Ω poniendo $\sigma(\alpha) = \sigma_L(\alpha)$ con algunas extensiones de Galois finitas L que contienen a $k(\alpha)$. El hecho de que σ está bien definido se sigue del hecho de que

por hipótesis, σ_L forma un sistema compatible de automorfismos; finalmente, σ manda a $(\sigma_L) \in \varprojlim Gal(L/k)$ por contrucción. □

Los grupos profinitos están dotados con una topología natural como sigue: si G es un limite inverso de un sistema de grupos finitos $(G_\alpha, \phi_{\alpha\beta})$, dotamos a G_α con la topología discreta, su producto con la topología producto y el subgrupo $G \subset \prod G_\alpha$ con el subespacio topológico. Se sigue de esta construcción que las proyección naturales $G \to G_\alpha$ son continuas y sus nucleos forman una base de vecindades abiertas del 1 en G.

Lemma 2.4.4. *Sea $(G_\alpha, \phi_{\alpha\beta})$ un sistema inverso de grupos equipados con la topología discreta. El límite inverso $\varprojlim G_\alpha$ es un subgrupo topológicamente cerrado del producto $\prod G_\alpha$.*

Demostración. Tomamos un elemento $g = (g_\alpha) \in \prod G_\alpha$. Si $g \notin \varprojlim G_\alpha$, tenemos que mostrar que tiene una vecindad abierta que no intersecta con $\varprojlim G_\alpha$. Por hipótesis, para algunos α y β tenemos que $\phi^\alpha_\beta(g_\beta \neq g_\alpha$. Ahora tomamos el subgrupo de $\prod G_\alpha$ que consiste de todos los elementos que en la componente α tengan a g_α y en la componente β tengan a g_β. Es abierto porque G_α tiene la topología discreta y la definición del producto topológico, y además, contiene a g pero no intersecta a $\varprojlim G_\alpha$. □

Corolario 2.4.5. *Un grupo profinito es compacto y totalmente disconexo (i.e., los únicos subconjuntos conexos son los subconjuntos de un sólo elemento). Más aún, los subgrupos abiertos son precisamente los subgrupos cerrados de indice finito.*

Teorema 2.4.6. ***(Krull).*** *Sea L una subextensión de la extensión de Galois Ω/k. Entonces $Gal(\Omega/L)$ es un subgrupo cerrado de $Gal(\Omega/k)$. Más aún, los morfismos*

$$L \mapsto H := Gal(\Omega/L) \quad y \quad H \mapsto L := \Omega^H$$

definen una biyección includiva-recursiva entre los subcampos $\Omega \supset L \supset k$ y los subgrupos cerrados $H \subset G$. Una subextensión L/k es Galois sobre k si y sólo si $Gal(\Omega/L)$ es normal en $Gal(\Omega/k)$; en este caso existe un isomorfismo natural $Gal(L/k) \simeq Gal(\Omega/k)/Gal(\Omega/L)$.

Demostración. Tomemos una extensión finita separable L/k contenida en Ω. Usando el lema (2,4,1), cubrimos a L/k en una extensión finita de Galois M/k contenida en Ω. Entonces $Gal(M/k)$ es uno de los cocientes finitos estándar de $Gal(\Omega/k)$, y contiene a $Gal(M/L)$ como subgrupo. Sea U_L la imagen inversa de $Gal(M/L)$ por la proyección narutal $Gal(\Omega/k) \to Gal(M/k)$. Como la proyección es continua y $Gal(M/k)$ tiene la topología discreta, U_L es abierto. Demostraremos que

$U_L = Gal(\Omega/L)$. De hecho, tenemos que $U_L \subset Gal(\Omega/L)$, ya que cada elementos de U_L fija a L; por otro lado, la imagen de $Gal(\Omega/L)$ por la proyección $Gal(\Omega/k) \to Gal(M/k)$ está contenido en $Gal(M/L)$, de dónde se concluye que $Gal(\Omega/L) \subset U_L$. Ahora, si L/k es una subextensión arbitraria de Ω/k, la escribimos como una unión de subextensiones finitas L_α/k. Por lo que acabamos de probar, cada $Gal(\Omega/L_\alpha)$ es un subgrupo abierto de $Gal(\Omega/k)$, de dónde también es cerrado (corolario (2,4,5)). Su intersección es precisamente $Gal(\Omega/L)$ que es entonces un subgrupo cerrado; su campo fijo es exactamente L, ya que Ω es Galois sobre L.
Conversamente, dado un subgrupo cerrado $H \subset G$, éste fija alguna extensión L/k y por lo tanto está contenido en $Gal(\Omega/L)$. Para mostrar la igualdad, sea σ un elemento de $Gal(\Omega/L)$, y tomamos una vecindad fundamental abierta U_M de la identidad en $Gal(\Omega/L)$, correspondiente a una extensión de Galois M/L. Ahora, $H \subset Gal(\Omega/L)$ se proyecta en $Gal(M/L)$ por la proyección natural; efectivamente, de otro modo su imágen en $Gal(M/L)$ fijaría un subcampo de M estrictamente mas grande que L de acuerdo con la teoría finita de Galois, lo que contradecería nuestra hipótesis de que cada elemento de M/L es movido por algún elemento de H. En particular, algunos elementos de H deben caer (bajo isomorfismo) al mismo elemento en $Gal(M/L)$ como σ. Por lo tanto, H contiene un elemento del *coset* σU_M y, como U_M es arbitrario, esto implica que σ está en la cerradura de H en $Gal(\Omega/L)$. Pero H es cerrado por hipótesis, de donde se concluye el teorema.
Finalmente, la relación entre subextensiones de Galois y subgrupos normales se demuestra exactamente igual al caso finito. □

Ejemplos.

(1) La extensión $\mathbb{Q}(\sqrt{2})$ es una extensión de Galois finita, para verlo solo se tiene que comprobar que esta extensión es el campo de descomposición del polinomio $x^2 - 2$.

(2) La cerradura algebraica de $\mathbb{Z}_p$ es una extensión de Galois finita sobre $\mathbb{Z}_p$ para p primo.

(3) La extensión $\mathbb{C}$ sobre $\mathbb{R}$ es una extensión infinita de Galois.

Capítulo 3

Cohomología de Grupos

El origen del álgebra cohomológica se encuentra en el descubrimiento, por Hurewiez en 1930's, que si X es un espacio asférico conexo, entonces todos los grupos de homología y cohomología de X están determinados por el grupo fundamental $\pi = \pi_1(X)$. Pero fue el teorema de Hopf en 1944, acerca de acciones de grupos fundamentales, que llevaron a definir y desarrollar las ideas básicas de cohomología de grupos. [2] Para desarrollar esta sección usaremos los conocimientos mínimos requeridos, los cuales son teoría de módulos, teoría de grupos y las definiciones de resoluciones proyectivas e inyectivas.

3.1. Grupos de cohomología

Si G es un grupo arbitrario y M es un grupo abeliano, diremos que M es un G-módulo si M es un $\mathbb{Z}G$-módulo, donde $\mathbb{Z}G$ es el anillo de grupos generado por G, es decir, $\mathbb{Z}G$ consiste de los elementos de la forma $\sum_{\sigma \in G} n_\sigma \sigma$ con $n_\sigma \in \mathbb{Z}$ y las sumas son finitas; las operaciones de $\mathbb{Z}G$ son las naturales.
Similarmente, si M y N son G-módulos, un G-morfismo $\phi : M \to N$ es un $\mathbb{Z}G$-morfismo. Se usará la notación $Hom_G(M, N) := Hom_{\mathbb{Z}G}(M, N)$.
Ahora, dado un G-módulo M, consideremos el submódulo de M formado por aquellos elementos que quedan fijos bajo la acción de G:

$$M^G := \{x \in M : \sigma \cdot x = x \text{ para todo } \sigma \in G\};$$

claramente M^G es un submódulo de M y es el mayor submódulo de M donde G actúa trivialmente, es decir, si $N \subseteq M$ es cualquier submódulo con una acción trivial de G, entonces $N \subseteq M^G$.

Lemma 3.1.1. *Sea G un grupo y consideremos la función $()^G : G - M\acute{o}d \to Ab$ que a cada G-módulo M le asocia el grupo abeliano M^G, donde $G - M\acute{o}d$ es la categoría de G-módulos izquierdos y Ab denota a la categoría de grupos abelianos. Entonces,*

(1) Si $\theta : M \to N$ es un G-morfismo, entonces la restricción de θ a M^G tiene su imagen en N^G y por lo tanto induce $\widetilde{\theta} : M^G \to N^G$. Se tiene así un funtor covariante

$$(\ )^G : G - M\acute{o}d \to Ab$$

(2) Más aún, el funtor $(\ )^G$ es exacto izquierdo y por lo tanto aditivo.

(3) Existe un isomorfismo natural

$$(\ )^G \to Hom_G(\mathbb{Z},\ ),$$

donde $\mathbb{Z}$ es un G-módulo trivial i.e., $\sigma x = x$ para todo $x \in \mathbb{Z}$ y todo $\sigma \in G$.

Demostración. (1): Dado $x \in M^G$, para $\theta(x) \in N$ y para todo $\sigma \in G$, se tiene que $\sigma \cdot (\theta(x)) = \theta(\sigma \cdot x) = \theta(x)$, la primera igualdad porque θ es G-morfismo y la segunda igualdad porque $\sigma x = x$. Se sigue que $\theta(x) \in N^G$ y se verifica que $(\ )^G$ es un funtor covariante.

(2): Dada una sucesión exacta de G-módulos $0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$, queremos mostrar que la sucesión

$$0 \to M'^G \xrightarrow{\widetilde{\phi}} M^G \xrightarrow{\widetilde{\psi}} M''^G$$

es exacta.
Para comenzar, $\widetilde{\phi}$ es inyectivo ya que es la restricción de ϕ que es inyectivo. La inclusión $Im(\widetilde{\phi}) \subseteq Ker(\widetilde{\psi})$ es porque $\widetilde{\psi} \circ \widetilde{phi} = \psi \circ \phi = 0$ (la primera igualdad porque las funciones son reestricciones y la segunda igualdad por la exactitud de la sucesión inicial).
Finalmente, $Ker(\widetilde{\psi}) \subseteq Im(\widetilde{\phi})$ ya que si $x \in Ker(\widetilde{\psi}) \subseteq M^G$ entonces $0 = \widetilde{\psi}(x) = \psi(x)$ y así $x \in Ker(\psi) = Im(\phi)$ y por lo tanto existe un $y \in M'$ tal que $x = \phi(y)$.
Mostraremos que $y \in M'^G$. En efecto, para todo $\sigma \in G$

$$\phi(y) = x = \sigma \cdot x = \sigma \cdot \phi(y) = \phi(\sigma \cdot y),$$

(la última igualdad porque ϕ es G-morfismo), y como ϕ es inyectiva se sigue que $\phi \cdot y = y$.

(3): Sea M un G-módulo y definamos $\eta_M : Hom_G(\mathbb{Z}, M) \to MG$ mediante $\eta_M(\phi) = \theta(1)$. Entonces,

(i): $\phi(1) \in M^G$ ya que para toda $\sigma \in G$ se tiene que $\sigma \cdot \phi(1) = \phi(\sigma \cdot 1) = \phi(1)$, la primera igualdad porque ϕ es G-morfismo y la segunda igualdad porque $\sigma x = x$ para toda $x \in \mathbb{Z}$, en particular $\sigma \cdot 1 = 1$.

(ii): Claramente η_M es un homomorfismo de grupos abelianos.

(iii): η_M es inyectivo ya que si $\phi(1) = \eta_M(\phi) = 0$ entonces para todo $n \in \mathbb{Z}$, $\phi(n) = \phi(n \cdot 1) = n \cdot \phi(1) = n \cdot 0 = 0$ i.e, $\phi = 0$.

(iv): η_M es suprayectivo ya que si $x \in M^G$, definimos $\phi_x : \mathbb{Z} \to M$ mediante $\phi_x(1) := x$ y lo extendemos linealmente a todo $\mathbb{Z}$, en particular $\phi_x(m) = \phi_x(m \cdot 1) = m\phi_x(1) = mx$. Se tiene que ϕ_x es un G-morfismo ya que si $\sigma \in G$ y $m \in \mathbb{Z}$, entonces

$$\phi_x(\sigma m) = \phi_x(m) = mx = m(\sigma x) = \sigma(mx) = \sigma\phi_x(m),$$

la primera igualdad porque $\sigma m = m$ y la tercera porque $x \in M^G$.

□

Definición 3.1.2. *Si M es un G-módulo y $q \geq 0$ es un entero, el $q-$ésimo grupo de cohomología de G con coeficientes en M es*

$$H^q(G, M) := R^q Hom_G(\mathbb{Z}, M) = Ext^q_{\mathbb{Z}G}(\mathbb{Z}, M)$$

Así, los funtores $Ext^q_{\mathbb{Z}G}(\mathbb{Z}, \ )$ son los funtores derivados derechos del funtor $Hom_G(G, \ )$ por lo que los grupos de cohomología $H^q(G, M)$ se calculan tomando una resolución proyectiva del G-módulo $\mathbb{Z}$ (o una resolución inyectiva del módulo M), digamos

$$\mathcal{P} : \cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

después se descabeza el complejo $\mathcal{P}$ eliminando el módulo $\mathbb{Z}$ y se aplica el funtor contravariante $Hom_G(\ , M)$ a este complejo descabezado para formar el nuevo complejo de grupos abelianos:

$$Hom_G(P_0, M) \xrightarrow{d_1^*} Hom_G(P_1, M) \xrightarrow{d_2^*} Hom_G(P_2, M) \xrightarrow{d_3^*} \ldots,$$

cuya cohomología es por definición

$$H^q(G,M) := Ext^q_{\mathbb{Z}G}(\mathbb{Z},M) := Ker(d^*_{q+1})/Im(d^*_q).$$

Observación. Las propiedades usuales de los funtores derivados se traducen a este contexto como sigue:

(1): $H^0(G,M) \simeq Hom_G(\mathbb{Z},M) \simeq M^G$.

(2): $H^q(G,M) = 0$ para toda $q \geq 1$ si M es un G-módulo inyectivo.

(3): Dada cualquier sucesión exacta corta de G-módulos

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0,$$

se tiene asociada la sucesión larga de cohomología:

$$0 \to M'^G \xrightarrow{\phi} M^G \xrightarrow{\psi} M''^G \xrightarrow{\delta} H^1(G,M') \xrightarrow{\phi^*} H^1(G,M) \xrightarrow{\psi^*}$$

$$\xrightarrow{\psi^*} H^1(G,M'') \xrightarrow{\delta} \dots$$

donde los morfismos de conexión δ dependen funtorialmente de la sucesión exacta de G-módulos dada.

Resoluciones. Como un ejemplo importante consideraremos la resolución proyectiva (de hecho, libre) de $\mathbb{Z}$ dada como sigue: se toma como P_n al $\mathbb{Z}$-módulo libre con base el conjunto de $(n+1) - adas(\sigma_0,\dots,\sigma_n)$ de elementos de G y donde el grupo G actúa en P_n mediante traslaciones, i.e., para $\sigma \in G$

$$\sigma \cdot (\sigma_0,\dots,\sigma_n) = (\sigma\sigma_0,\dots,\sigma\sigma_n),$$

y así, los P_n son, en efecto, G-módulos y de hecho son G-módulos libres con una base dada por las $(n+1) - adas$ de la forma $(1,\sigma_1,\dots,\sigma_n) \in G^{n+1}$.
Los morfismos $d_n : P_n \to P_{n-1}$ se definen, en los generadores, mediante la fórmula

$$d_n(\sigma_0,\dots,\sigma_n) = \sum_{j=0}^{n}(-1)^j(\sigma_0,\dots,\widehat{\sigma_j},\dots,\sigma_n),$$

donde el símbolo $\widehat{\sigma_j}$ indica el elemento correspondiente que ha sido omitido. Finalmente, el morfismo $\varepsilon : P_0 \to \mathbb{Z}$ se define enviando cada generador (σ_0) de P_0 a $\varepsilon(\sigma_0) = 1$. Observemos que $P_0 = \mathbb{Z}G$ y el morfismo $\varepsilon : P_0 = \mathbb{Z}G \to \mathbb{Z}$ está dado por $\varepsilon(\sum_{\sigma\in G} m_\sigma \cdot \sigma) = \sum_{\sigma\in G} m_\sigma$, i.e., es el morfismo de aumentación. Más aún, $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$ es claramente un epimorfismo de anillos y su núcleo $I_G \subseteq \mathbb{Z}G$ es un ideal bilateral de $\mathbb{Z}G$ llamado el ideal de aumentación.

Proposición 3.1.1. *La sucesión de $\mathbb{Z}$ de G-módulos libres*

$$\mathcal{P} : \ldots \xrightarrow{d_{i+1}} P_i \xrightarrow{d_i} P_{i-1} \xrightarrow{d_{i-1}} \ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

es exacta.

Demostración. Primero veremos que es un complejo, i.e., que $\varepsilon \circ d_1 = 0$ y $d_{n-1} \circ d_n = 0$. En efecto, para todo generador $(\sigma_0, \sigma_1) \in P_1$ se tiene que $\varepsilon d_1(\sigma_0, \sigma_1) = \varepsilon[(-1)^0(\widehat{\sigma_0}, \sigma_1) + (-1)^1(\sigma_0, \widehat{\sigma_1})] = \varepsilon[(\sigma_1) - (\sigma_0)] = 1 - 1 = 0$.
Ahora, si $n \geq 2$,

$$\begin{aligned} d_{n-1} \circ d_n(\sigma_0, \ldots, \sigma_n) &= d_{n-1}\left[\sum_{j=0}^{n} (-1)^j(\sigma_0, \ldots, \widehat{\sigma_j}, \ldots, \sigma_n)\right] \\ &= \sum_{j=0}^{n} (-1)^j d_{n-1}(\sigma_0, \ldots, \widehat{\sigma_j}, \ldots, \sigma_n) \\ &= \sum_{j=0}^{n} (-1)^j \Big[\sum_{i=0}^{j-1} (-1)^i(\sigma_0, \ldots, \widehat{\sigma_i}, \ldots, \widehat{\sigma_j} \ldots, \sigma_n) \\ &\quad + \sum_{i=j+1}^{n} (-1)^{i-1}(\sigma_0, \ldots, \widehat{\sigma_j}, \ldots, \widehat{\sigma_i}, \ldots, \sigma_n)\Big] \end{aligned}$$

(nótese que recorrimos un lugar los índices en la segunda suma, por eso aparece el exponente $i - 1$ en el (-1)).
Observamos ahora que los sumandos con los pares omitidos $\widehat{\sigma_i}$ y $\widehat{\sigma_j}$ ocurren en la primera suma con el coeficiente $(-1)^j(-1)^i = (-1)^{i+j}$ y ocurren en la segunda suma con el coeficiente $(-1)^j(-1)^{i-1} = (-1)^{i+j-1}$ y por lo tanto se cancelan. Se sigue que $d_{n-1} \circ d_n$=0.
Finalmente, para probar que el complejo $\mathcal{P}$ es exacto es suficiente probar que el morfismo identidad $1_{\mathcal{P}}$ es nulhomótopo, i.e., que en el diagrama siguiente

$$\begin{array}{ccccccccccccccc} P_{n+1} & \xrightarrow{d_{n+1}} & P_n & \xrightarrow{d_n} & P_{n-1} & \longrightarrow \cdots \longrightarrow & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & \mathbb{Z} & \longrightarrow & 0 \\ \downarrow{\scriptstyle 1} & \swarrow{\scriptstyle s_n} & \downarrow{\scriptstyle 1} & \swarrow{\scriptstyle s_{n-1}} & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle 1} & \swarrow{\scriptstyle s_0} & \downarrow{\scriptstyle 1} & \swarrow{\scriptstyle s_{-1}} & \downarrow{\scriptstyle 1} & & \\ P_{n+1} & \xrightarrow[d_{n+1}]{} & P_n & \xrightarrow[d_n]{} & P_{n-1} & \longrightarrow \cdots \longrightarrow & P_1 & \xrightarrow[d_1]{} & P_0 & \xrightarrow[\varepsilon]{} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

existen morfismos $s_n : P_n \to P_{n+1}$ con las propiedades siguientes:

$$\begin{aligned} s_{n-1} \circ d_n + d_{n+1} \circ s_n &= 1 \\ s_{-1} \circ \varepsilon + d_1 \circ s_0 &= 1 \\ \varepsilon \circ s_{-1} &= 1 \end{aligned}$$

Los morfismos s_n se definen como sigue: $s_{-1} : \mathbb{Z} \to P_0$ está dado por: $1 \mapsto 1$, donde el segundo 1 es la identidad de G.
Para $n \geq 0$, $s_n : P_n \to P_{n+1}$ está dado por: $(\sigma_0, \ldots, \sigma_n) \mapsto (1, \sigma_0, \ldots, \sigma_n)$.
Ahora veremos que efectivamente las propiedades se cumplen:

(1): $(s_{n-1} \circ d_n + d_{n+1} \circ s_n)(\sigma_0, \ldots \sigma_n)$

$$= s_{n-1}(\sum_{j=0}^{n}(-1)^j(\sigma_0, \ldots, \widehat{\sigma_j}, \ldots, \sigma_n)) + d_{n+1}(1, \sigma_0, \ldots, \sigma_n)$$
$$= \sum_{j=0}^{n}(-1)^j(1, \sigma_0, \ldots, \widehat{\sigma_j}, \ldots, \sigma_n) + (\sigma_0, \ldots, \sigma_n)$$
$$+ \sum_{j=0}^{n}(-1)^{j+1}(1, \sigma_0, \ldots, \widehat{\sigma_j}, \ldots, \sigma_n)$$
$$= (\sigma_0, \ldots, \sigma_n)$$

(2): $(s_{-1} \circ \varepsilon + d_1 \circ s_0)(\sigma_0) = s_{-1}(1) + d_1(1, \sigma_0)$

$$= 1 + \sigma_0 - 1 = \sigma_0$$

(3): $(\varepsilon \circ s_{-1})(1) = \varepsilon(1) = 1$

□

El paso siguiente es identificar los $Hom_G(P_i, M)$ pra los P_i anteriores: un elemento $\phi \in Hom_G(P_i, M)$ está determinado por sus valores en los generadores $(\sigma_0, \ldots, \sigma_n)$ de P_i y como ϕ debe ser un G-morfismo, entonces debe ser G-covariante, i.e., para todo $\sigma \in G$

$$\phi(\sigma(\sigma_0, \ldots, \sigma_n)) = \sigma\phi(\sigma_0, \ldots, \sigma_n).$$

Los morfismos $d_i : P_i \to P_{i-1}$ inducen homomorfismos

$$d_i^* : Hom_G(P_{i-1}, M) \to Hom_G(P_i, M)$$

dados por:

$$\phi \mapsto (d_i^*\phi)(\sigma_0, \ldots, \sigma_n) = \phi d_i(\sigma_0, \ldots, \sigma_n) = \sum_{j=0}^{i}(-1)^j\phi(\sigma_0, \ldots, \widehat{\sigma_j}, \ldots, \sigma_i).$$

Por lo visto anteriormente, una i-cocadena $\phi \in Hom_G(P_i, M)$ está determinada por sus valores en los generadores $(\sigma_0, \ldots, \sigma_n)$ de P_i, y como también debe ser G-covariante entonces

$$\phi(\sigma_0, \ldots, \sigma_n) = \phi(\sigma_0(1, \sigma_0^{-1}\sigma_1, \ldots, \sigma_0^{-1}\sigma_i)) = \sigma_0\phi(1, \sigma_0^{-1}\sigma_1, \ldots, \sigma_0^{-1}\sigma_i),$$

es decir, ϕ está determinada por sus valores en los generadores de P_i de la forma $(1, \sigma_1, \ldots, \sigma_i)$. Esto nos lleva a considerar otra resolución $\mathbb{Z}G$-libre de $\mathbb{Z}$ mediante coordenadas no homogéneas dada como sigue: si $n > 0$ sea Q_n el $\mathbb{Z}G$-módulo libre con base las n-adas $[\sigma_1, \ldots, \sigma_n]$ de G^n; y si $n = 0$ sea Q_0 el G-módulo libre generado por un símbolo denotado por [ ].

Lemma 3.1.3. *Para toda $n \geq 0$, $P_n \simeq Q_n$ como $\mathbb{Z}G$-módulos.*

Demostración. Sea $\phi_n : Q_n \to P_n$ dado por:

$$\phi_n[\sigma_1, \ldots, \sigma_n] := (1, \sigma_1, \sigma_1\sigma_2, \sigma_1\sigma_2\sigma_3, \ldots, \sigma_1\sigma_2 \cdots \sigma_n);$$

así, ϕ_n manda un básico de Q_n a un básico de P_n. La inversa de ϕ_n es el morfismo $\psi_n : P_n \to Q_n$ dado por:

$$\psi_n(\sigma_0, \ldots, \sigma_n) := \sigma_0[\sigma_0^{-1}\sigma_1, \sigma_1^{-1}\sigma_2, \ldots, \sigma_{n-1}^{-1}\sigma_n].$$

Si aplicamos la composición directamente se ve que estos morfismos son inversos uno del otro. □

Corolario 3.1.4. *Existen morfismos únicos $\delta_n : Q_n \to Q_{n-1}$ para toda $n \geq 1$, tales que los diagramas siguientes conmutan:*

$$\begin{array}{ccc} P_n & \xrightarrow{d_n} & P_{n-1} \\ {\scriptstyle \phi_n}\uparrow & & \downarrow{\scriptstyle \psi_{n-1}} \\ Q_n & \xrightarrow[\delta_n]{} & Q_{n-1} \end{array}$$

es decir, $\delta_n = \psi_{n-1} \circ d_n \circ \phi_n$ (ya que $\psi_n^{-1} = \phi_n$).
Explícitamente, los morfismos δ_n están dados por la fórmula:

$$\delta_n[\sigma_1, \ldots, \sigma_n] = \sigma_1[\sigma_2, \ldots, \sigma_n] + \sum_{i=1}^{n-1}(-1)^i[\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_n] +$$

$$+(-1)^n[\sigma_1, \ldots \sigma_{n-1}].$$

En particular,

$$\delta_1[\sigma] = \sigma[\,] - [\,],$$

$$\delta_2[\sigma, \sigma'] = \sigma[\sigma'] - [\sigma\sigma'] + [\sigma'],$$

y

$$\delta_3[\sigma, \sigma', \sigma''] = \sigma[\sigma', \sigma''] - [\sigma\sigma', \sigma''] + [\sigma, \sigma'\sigma''] - [\sigma, \sigma'].$$

Demostración. Sólo necesitamos verificar que $\delta_n = \psi_{n-1} \circ d_n \circ \phi_n$ nos da la fórmula deseada. En efecto,

$$\begin{aligned}
\delta_n[\sigma_1, \ldots, \sigma_n] &= \psi_{n-1} \circ d_n \circ \phi_n[\sigma_1, \ldots, \sigma_n] \\
&= \psi_{n-1} \circ d_n(1, \sigma_1, \sigma_1\sigma_2, \ldots, \sigma_1\sigma_2 \cdots \sigma_n) \\
&= \psi_{n-1}\left(\sum_{j=0}^{n}(-1)^j(1, \sigma_1, \ldots, \widehat{\sigma_1 \cdots \sigma_j}, \ldots, \sigma_1 \cdots \sigma_n)\right) \\
&= \psi_{n-1}((\sigma_1, \ldots, \sigma_1 \cdots \sigma_n) \\
&+ \sum_{j=1}^{n-1}(-1)^j(1, \ldots, \widehat{\sigma_1 \cdots \sigma_j}, \ldots, \sigma_1, \cdots, \sigma_n) \\
&+ (-1)^n(\sigma_1, \ldots, \sigma_1 \cdots \sigma_{n-1}) \\
&= \psi_{n-1}(\sigma_1, \ldots, \sigma_1 \cdots \sigma_n) \\
&+ \sum_{j=1}^{n-1}(-1)^j\psi_{n-1}(1, \ldots, \widehat{\sigma_1 \cdots \sigma_j}, \ldots, \sigma_1 \cdots \sigma_n) \\
&+ (-1)^n\psi_{n-1}(1, \ldots, \sigma_1 \cdots \sigma_n \\
&= \sigma_1[\sigma_1^{-1}\sigma_1\sigma_2, (\sigma_1\sigma_2)^{-1}\sigma_1\sigma_2\sigma_3, \ldots, (\sigma_1 \cdots \sigma_{n-1})^{-1}\sigma_1 \cdots \sigma_n] \\
&+ \sum_{j=1}^{n-1}(-1)^j 1[\sigma_1, \sigma_1^{-1}(\sigma_1\sigma_2), \ldots, (\sigma_1 \cdots \sigma_{j-1})^{-1}\sigma_1 \cdots \sigma_{j+1}, \ldots \\
&(\sigma_1 \cdots \sigma_{n-1})^{-1}\sigma_1 \cdots \sigma_n] \\
&+ (-1)^n[\sigma_1, \sigma_1^{-1}(\sigma_1\sigma_2, \ldots, (\sigma_1 \cdots \sigma_{n-2}^{-1}\sigma_1 \cdots \sigma_{n-1}] \\
&= \sigma_1[\sigma_2, \ldots, \sigma_n] + \sum_{j=1}^{n-1}(-1)^j[\sigma_1, \ldots, \sigma_j\sigma_{j+1}, \ldots, \sigma_n] \\
&+ (-1)^n[\sigma_1, \ldots, \sigma_{n-1}].
\end{aligned}$$

□

Proposición 3.1.2. *La sucesión de $\mathbb{Z}G$- módulos libres*

$$\mathcal{Q} : \cdots \to Q_n \xrightarrow{\delta_n} Q_{n-1} \to \cdots \to Q_1 \xrightarrow{\delta_1} Q_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

es una resolución proyectiva de $\mathbb{Z}$.

Demostración. $\mathcal{Q}$ es un complejo de cadena ya que $\varepsilon \circ \delta_1 = 0$ y para toda $n \geq 2$ se tiene que

$$\begin{aligned}
\delta_{n-1} \circ \delta_n &:= (\psi_{n-2} \circ d_{n-1} \circ \phi_{n-1}) \circ (\psi_{n-1} \circ d_n \circ \phi_n) \\
&= \psi_{n-2} d_{n-1} d_n \phi_n \qquad \text{ya que } \phi_{n-1}\psi_{n-1} = 1 \\
&= \psi_{n-2}(0)\phi_n \qquad\quad \text{ya que } d_{n-1}d_n = 0 \\
&= 0.
\end{aligned}$$

Finalmente, como por definición de δ_n los cuadrados del corolario previo conmutan, entonces se tiene un morfismo de complejos de cadena $\psi = (\psi_n) : \mathcal{P} \to \mathcal{Q}$ que es un isomorfismo con inverso $\phi = (\phi_n)$, y que por lo tanto induce isomorfismos en la cohomología de los complejos $\mathcal{P}$ y $\mathcal{Q}$, pero como $\mathcal{P}$ es exacto, entonces $H^n(\mathcal{Q}) \simeq H^n(\mathcal{P}) = 0$ para toda $n \geq 0$, es decir, $\mathcal{Q}$ es una sucesión exacta. □

Observación. Para el complejo $\mathcal{Q}$ anterior, las n-cocadenas $\phi \in Hom_G(\mathcal{Q}_n, M)$ son funciones G-covariantes $\phi : Q_n \to M$ determinadas por sus valores en los generadores $[\sigma_1, \ldots, \sigma_n]$ de Q_n y por lo tanto las podemos ver como funciones G-covariantes $\phi : G \times \cdots \times G \to M$. Entonces, los $\delta_n : Q_n \to Q_{n-1}$ inducen las cofronteras

$$\delta_n^* : Hom_G(Q_{n-1}, M) \to Hom_G(Q_n, M)$$

dadas por la fórmula (para $\phi \in Hom_G(Q_{n-1}, M)$):

$$\begin{aligned}
\delta_n^*[\sigma_1, \ldots, \sigma_n] &= \phi \circ \delta_n[\sigma_1, \ldots, \sigma_n] \\
&= \phi(\sigma_1[\sigma_2, \ldots, \sigma_n] + \sum_{i=1}^{n-1}(-1)^i[\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_n] \\
&+ (-1)^n[\sigma_1, \ldots, \sigma_{n-1}] \\
&= \sigma_1\phi[\sigma_2, \ldots, \sigma_n] + \sum_{i=1}^{n-1}(-1)^i[\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_n] \\
&+ (-1)^n\phi[\sigma_1, \ldots, \sigma_{n-1}].
\end{aligned}$$

El grupo $H^1(G, M)$. Para calcular este grupo, consideremos la parte del complejo inducido por $\mathcal{Q} = \{(Q_n, \delta_n)\}$ que nos interesa:

$$\cdots \to Hom_G(Q_0, M) \xrightarrow{\delta_1^*} Hom_G(Q_1, M) \xrightarrow{\delta_2^*} Hom_G(Q_2, M) \to \cdots$$

donde los δ_n^* están dados por la fórmula anterior. Así, para $n = 1$, para que una 1-cocadena $\phi \in Hom_G(Q_1, M)$ sea un 1-cociclo, es decir, $\delta_2^*(\phi) = 0$, se requiere que la función $\phi : Q_1 \to M$ satisfaga la condición

$$0 = \delta_2^*(\phi) \in Hom_G(Q_2, M),$$

es decir,

$$0 = \delta_2^*(\phi)[\sigma, \sigma'] = \sigma\phi[\sigma'] + (-1)^1\phi[\sigma\sigma'] + (-1)^2\phi[\sigma]$$

$$= \sigma\phi[\sigma'] - \phi[\sigma\sigma'] + \phi[\sigma],$$

y por lo tanto la función $\phi : G \to M$ satisface la identidad

$$\phi(\sigma\sigma') = \sigma\phi(\sigma') + \phi(\sigma).$$

Se suele llamar a una tal función $\phi : G \to M$ un morfismo cruzado.

Finalmente, un 1-cociclo $\phi \in Hom_G(Q_1, M)$, i.e., un morfismo cruzado $\phi : G \to M$, es una 1-cofrontera si y sólo si $\phi = \delta_1^*\phi'$ con $\phi' \in Hom_G(Q_0, M) = Hom_G(\mathbb{Z}G, M)$, y como $Q_0 = \mathbb{Z}G$ está generado por $[\ ]$ entonces ϕ' está determinado por su valor en este generador $\phi'[\ ] =: x \in M$. Ahora, como $\phi = \delta_1^*\phi' \in Hom_G(Q_1, M)$ está dado por

$$\phi[\sigma] = \delta_1^*\phi'[\sigma] = \phi'\delta_1[\sigma] = \phi'(\sigma[\ ] - [\ ]) = \sigma\phi'[\ ] - \phi'[\ ] = \sigma x - x,$$

entonces

$$\phi(\sigma) = \sigma x - x \qquad \text{para algún } x \in M,$$

es decir, un 1-cociclo $\phi \in Hom_G(Q_1, M)$ es una 1-cofrontera si y sólo si existe $x \in M$ tal que $\phi(\sigma) = \sigma x - x$ para todo $\sigma \in G$. Esto nos describe completamente el grupo $H^1(G, M)$ = { 1-cociclos }/{ 1-cofronteras }.

Como un caso particular observamos que, si G opera trivialmente en M, es decir, si $\sigma x = x$ para todo $\sigma \in G$ y todo $x \in M$, entonces $\phi \in Hom_G(Q_1, M)$ es un 1-cociclo si y sólo si $\phi : G \to M$ satisface

$$\phi(\sigma\sigma') = \sigma\phi(\sigma') + \phi(\sigma) = \phi(\sigma') + \phi(\sigma),$$

(ya que $\sigma\phi(\sigma') = \phi(\sigma')$ porque la acción es trivial), es decir,

$$\phi(\sigma\sigma') = \phi(\sigma) + \phi(\sigma'),$$

para todos los $\sigma, \sigma' \in G$ y por lo tanto $\phi : G \to M$ es un homomorfismo de grupos y así $Ker(\delta_2^*) = Hom(G, M)$.
Pero $Im(\delta_1^*) = 0$ ya que para todo $\phi' \in Hom(G, M)$ se tiene que $\delta_1^*\phi' \in Hom_G(Q_1, M)$ satisface

$$\delta_1^*\phi'[\sigma] = \sigma x - x = x - x = 0$$

(ya que $\sigma x = x$ porque la acción es trivial). Se sigue que

$$H^1(G, M) = Ker(\delta_2^*/Im(\delta_1^*) \simeq Hom(G, M).$$

El grupo $H^2(G, M)$ y extensiones de grupos. Para calcular este grupo, consideremos la parte del complejo inducido por $\mathcal{Q} = \{(Q_n, \delta_n)\}$ que nos interesa:

$$\cdots \to Hom_G(Q_1, M) \xrightarrow{\delta_2^*} Hom_G(Q_2, M) \xrightarrow{\delta_3^*} Hom_G(Q_3, M) \to \cdots$$

donde los δ_n^* están dados por la fórmula previa. Así, para $n = 2$, una 2-cocadena $\phi \in Hom_G(Q_2, M)$ es un 2-cociclo, es decri, $\delta_3^*(\phi) = 0$, si la función $\phi : Q_2 \to M$ satisface la condición

$$0 = \delta_3^*(\phi) \in Hom_G(Q_3, M),$$

es decir,

$$\begin{aligned} 0 &= \delta_3^*(\phi)[\sigma, \sigma', \sigma''] \\ &= \sigma\phi[\sigma', \sigma''] + (-1)^1\phi[\sigma\sigma', \sigma''] + (-1)^2\phi[\sigma, \sigma'\sigma''] + (-1)^3\phi[\sigma, \sigma'] \\ &= \sigma\phi[\sigma', \sigma''] - \phi[\sigma\sigma', \sigma''] + \phi[\sigma, \sigma'\sigma''] - \phi[\sigma, \sigma'] \end{aligned}$$

Y por lo tanto la función $\phi : : G \times G \to M$ satisface la identidad

$$\sigma\phi[\sigma', \sigma''] - \phi[\sigma\sigma', \sigma''] + \phi[\sigma, \sigma'\sigma''] - \phi[\sigma, \sigma'] = 0.$$

Se suele llamar a una función $\phi : G \times G \to M$ un conjunto factor. Para explicar esto, usando los conceptos involucrados, sería de la siguiente forma: dado el grupo (no necesariamente abeliano) G y el grupo abeliano M, ¿qué grupos E existen tales que contienen a M como un subgrupo normal y además el grupo cociente E/M es

G? En otras palabras, lo que queremos es que E esté en una sucesión exacta corta de la forma:

$$\varepsilon \ : \qquad 1 \to M \xrightarrow{i} E \xrightarrow{\rho} G \to 1,$$

donde además hay una acción de G en M. Notamos además que como $G = E/M$, la acción de G en M está daad por conjugación, i.e., para todo $\sigma \in G$ y $x \in M$ se tiene que $\sigma \cdot x = \widetilde{\sigma} x \widetilde{\sigma}^{-1}$, donde $\widetilde{\sigma} \in E$ es una preimagen, bajo ρ, de $\sigma \in G$.
A la sucesión ε se le llama una extensión de M con cociente G. Un ejemplo de una tal extensión está dada por

$$1 \to M \to M \rtimes G \to G \to 1,$$

donde $M \rtimes G$ es el producto semidirecto de G con M, i.e., los elementos de $M \rtimes G$ son de la forma $x\sigma$ con $x \in M,\ \sigma \in G$ y la ley de composición está dada por

$$(x\sigma)(z\tau) = x(z)^{\sigma}\sigma\tau$$

donde z^{σ} denota la acción de $\sigma \in G$ sobre $z \in M$. El morfismo $i \ : \ M \to M \rtimes G$ es la inclusión $i(x) = x \cdot 1$ y el morfismo $\rho \ : \ M \rtimes G \to G$ es $\rho(x\sigma) = \sigma$.

Se dice que dos extensiones $\varepsilon, \varepsilon'$ de M con cociente G son equivalentes (denotado $\varepsilon \sim \varepsilon'$), si existe un diagrama conmutativo de la forma:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{\rho} & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \phi} & & \| & & \\ 1 & \longrightarrow & M & \xrightarrow[i']{} & E' & \xrightarrow[\rho']{} & G & \longrightarrow & 1 \end{array}$$

i.e., si existe un morfismo $\phi \ : \ E \to E'$ que hace conmutativo el diagrama anterior. Nótese que, por el lema del quinto, ϕ necesriamente resulta ser un isomorfismo. Se sigue que la relación $\varepsilon \sim \varepsilon'$ es una relación de equivalencia en el conjunto de extensiones de M por G. Denotemos con $Ext(M, G)$ al conjunto cociente. La extensión dada por el producto semidirecto $M \rtimes G$ nos da un elemento distinguido en el conjutno $Ext(M, G)$.

El teorema siguiente nos dice que $Ext(M, G)$ es un grupo abeliano isomorfo a $H^2(G, M)$:

Teorema 3.1.5. *Si G es un grupo (no necesariamente abeliano) y M es un grupo abeliano con una acción de G, entonces se tiene una biyección*

$$H^2(G, M) \simeq Ext(M, G)$$

que manda el elemento neutro de $H^2(G, M)$ en el elemento distinguido de $Ext(M, G)$.

Demostración. Primero definimos una función $\Phi : Ext(M,G) \to H^2(G,M)$ como sigue: dada una clase $[\varepsilon] \in Ext(M,G)$ representada por la sucesión exacta $\varepsilon : \quad 1 \to M \xrightarrow{i} E \xrightarrow{\rho} G \to 1$, sea $s : G \to E$ una sección i.e., una función (que, en general no es un homomorfismo) tal que $\rho \circ s = id_G$. Nótese que como $G = E/M$, entonces s es un sistema de representantes de las clases laterales de $G = E/M$, por lo que, pensando a M como un subgrupo de E, todo elemento $\gamma \in E$ se puede escribir en forma única como

$$\gamma = xs(\sigma) \qquad \text{con } x \in M \text{ y } \sigma \in G \tag{3.1}$$

y se tiene que para $\sigma \in G$ y $x\ inM$:

$$s(\sigma)x = (s(\sigma)xs(\sigma)^{-1})s(\sigma) = x^{s(\sigma)}s(\sigma), \tag{3.2}$$

donde $x^{s(\sigma)} = s(\sigma)xs(\sigma)^{-1}$ es el conjugado de x por $s(\sigma)$.
Ahora, si $\sigma, \tau \in G$ consideremos su producto $\sigma\tau \in G$ y los elementos $s(\sigma), s(\tau), s(\sigma\tau)$ de E correspondientes. En general, s no es un homomorfismo, sin embargo, $s(\sigma)s(\tau)$ y $s(\sigma\tau)$ están en la misma clase lateral de E módulo M, ya que

$$\rho(s(\sigma)s(\tau)) = \rho s(\sigma)\rho s(\tau) = \sigma\tau = \rho s(\sigma\tau)$$

por lo que $s(\sigma)s(\tau)M = s(\sigma\tau)M$ y por lo tanto existe un elemento $x(\sigma,\tau) \in M$ tal que

$$s(\sigma)s(\tau) = x(\sigma,\tau)s(\sigma\tau), \tag{3.3}$$

y la función $x : G \times G \to M$ así definida satisface que $x(\sigma,\tau) = 1 = x(1,\sigma)$ ya que $s(1) = 1$ y $\sigma \cdot 1 = \sigma = 1 \cdot \sigma$.
La asociatividad del producto en E implica que $x : G \times G \to M$ es un 2-cociclo ya que, por (3):

$$(s(\sigma)s(\tau))s(\theta) = x(\sigma,\tau)s(\sigma\tau)s(\theta) = x(\sigma,\tau)x(\sigma\tau,\theta)s(\sigma\tau\theta)$$

y,

$$s(\sigma)(s(\tau)s(\theta)) = s(\sigma)x(\tau,\theta)s(\tau\theta) = x(\tau,\theta)^{s(\sigma)}s(\sigma)s(\tau\sigma) = x(\tau,\theta)^{s(\sigma)}x(\sigma,\tau\theta)s(\sigma\tau\theta),$$

donde en la penúltima igualdad se uso (2). Igualando las dos expresiones anteriores y cancelando el factor común, obtenemos

$$x(\sigma,\tau)x(\sigma\tau,\theta) = x(\tau,\theta)^{s(\sigma)}x(\sigma,\tau\theta),$$

i.e.,

$$x(\tau,\theta)^{s(\sigma)}x(\sigma,\tau\theta)x(\sigma\tau,\theta)^{-1}x(\sigma,\tau)^{-1} = 1,$$

i.e., $x(\ ,\ )$ es un conjunto factor, en notación multiplicativa, ya que la acción de G en $x(\tau,\sigma)$ está dada por $\sigma x(\tau,\sigma) = x(\tau,\sigma)^{s(\sigma)}$, i.e., x es un 2-cociclo.
Se obtiene así una clase de cohomología $[x] \in H^2(G,M)$ y queremos definir $\Phi[\varepsilon] = [x] \in H^2(G,M)$. Para que esta sea una buena definición, necesitados dos hechos:

(A). La clase $[x]$ no depende de la elección de la sección $s : G \to E$, i.e., no depende de la elección del sistema de representantes de $G = E/M$.

(B). La clase $[x]$ no depende de la elección del representante ε de la clase de equivalencia $[\varepsilon] \in Ext(M,G)$.

La demostración es como sigue:

(A). Si $s' : G \to E$ es otra sección de ρ, entonces para cualquier $\sigma \in G$, $\rho s'(\sigma) = \sigma = \rho s(\sigma)$ en $G = E/m$, por lo que existe $y(\sigma) \in M$ tal que

$$s'(\sigma) = y(\sigma)s(\sigma). \tag{3.4}$$

Ahora, usando la sección s' y dados $\sigma,\tau \in G$, procedemos como antes para probar (3), de tal forma que existe un elemento $z(\sigma,\tau) \in M$ tal que

$$s'(\sigma)s'(\tau) = z(\sigma,\tau)s'(\sigma,\tau), \tag{3.5}$$

lo cual define de la misma manera un 2-cociclo $z : G \times G \to M$ y se tiene que:

$$\begin{aligned}
s'(\sigma)s'(\tau) &= z(\sigma,\tau)s'(\sigma\tau) \\
&= z(]\sigma,\tau)y(\sigma\tau)s(\sigma\tau) \quad \text{por (4)} \\
&= z(\sigma,\tau)y(\sigma\tau)x(\sigma,\tau)^{-1}s(\sigma)s(\tau) \quad \text{por (3)} \\
&= z(\sigma,\tau)y(\sigma\tau)x(\sigma,\tau)^{-1}y(\sigma)^{-1}s'(\sigma)y(\tau)^{-1}s'(\tau) \quad \text{por (4)} \\
&= z(\sigma,\tau)x(\sigma.\tau)^{-1}y(\sigma\tau)y(\sigma)^{-1}s'(\sigma)y(\tau)^{-1}s'(\tau) \\
&\text{ ya que } M \text{ es abeliano y } x(\sigma,\tau), y(\sigma,\tau) \in M \\
&= z(\sigma,\tau)x(\sigma,\tau)^{-1}y(\sigma\tau)y(\sigma)^{-1}s'(\sigma)y(\tau)^{-1}s'(\sigma)^{-|}s'(\sigma)s'(\tau) \\
&= z(\sigma,\tau)x(\sigma,\tau)^{-1}y(\sigma\tau)y(\sigma)^{-1}\left(y(\tau)^{s'(\sigma)}\right)^{-1}s'(\sigma)s'(\tau),
\end{aligned}$$

de donde, cancelando $s'(\sigma)s'(\tau)$ y poniendo $w(\sigma,\tau) := y(\tau)^{s'(\sigma)}y(\sigma)y(\sigma\tau)^{-1}$ se tiene que $1 = z(\sigma,\tau)x(\sigma,\tau)^{-1}w(\sigma,\tau)^{-1}$, .i.e,

$$z(\sigma,\tau) = x(\sigma,\tau)w(\sigma,\tau),$$

donde $w(\sigma,\tau)$ es una 2-cofrontera por la segunda fórmula particular de (3,1,4) en notación multiplicativa. Se sigue que

$$[z(\sigma,\tau)] = [x(\sigma\tau)],$$

como se quería.

(B). Si $\varepsilon \sim \varepsilon' \;:\; 1 \to M \to E' \to G \to 1$, entonces existe un diagrama conmutativo

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \xrightarrow{i} & E & \underset{\rho}{\overset{s}{\rightleftarrows}} & G & \longrightarrow & 1 \\ & & \| & & \downarrow \phi & & \| & & \\ 1 & \longrightarrow & M & \xrightarrow[i']{} & E' & \underset{s'}{\overset{\rho'}{\rightleftarrows}} & G & \longrightarrow & 1 \end{array}$$

y así, $s' = \phi \circ s$, por lo que para todo $\sigma \in G$ se tiene que $s'(\sigma) = \phi s(\sigma)$. Entonces para la clase de cohomología $[x]$ contruida usando la extensión ε y la sección s, y para toda $\sigma,\tau \in G$ se tiene que $s'(\sigma) = \phi s(\sigma)$. Entonces, para la clase de cohomología $[x]$ construida usando la extensión ε y la sección s, y para $\sigma,\tau \in G$ se tiene que

$$\begin{aligned} s'(\sigma)s'(\tau) &= \phi s(\sigma)\phi s(\tau) = \phi(s(\sigma)s(\tau)) \\ &= \phi(x(\sigma,\tau)s(\sigma\tau)) \\ &= \phi(x(\sigma,\tau))\phi s(\sigma\tau) \\ &= x(\sigma,\tau)s'(\sigma\tau), \end{aligned}$$

la última igualdad porque ϕ restringida a $M]$ es la identidad por la conmutatividad del cuadrado izquierdo del diagrama anterior, y porque $s' = \phi \circ s$. Se sigue que

$$s'(\sigma)s'(\tau) = x(\sigma,\tau)s'(\sigma\tau)$$

que es precisamente la igualdad que se usa para definir la clase de cohomología asociada a ε' y s'. Por lo tanto las extensiones ε y ε' dan lugar al mismo 2-cociclo x.

Para mostrar que Φ es biyectiva, construiremos su inversa

$$\Psi \;:\; H^2(G,M) \to Ext(M,G)$$

como sigue: toda clase de cohomología $c \in H^2(G,M)$ contiene un 2-cociclo normalizado $x(\sigma,\tau)$, esto es, un 2-cociclo tal que $x(\sigma,1) = 1 = x(1,\sigma)$, para ver esto, si $x(\sigma,\tau)$ es un 2-cociclo arbitrario en c, entonces de la igualdad

$$x(\sigma\tau,\theta)x(\sigma,\tau) = x(\sigma,\tau\theta)x(\tau,\theta)^{\sigma}$$

se sigue que, para $\tau = 1 = \theta, x(\sigma,1)x(\sigma,1) = x(\sigma,1)x(1,1)^\sigma$ y por lo tanto

$$x(\sigma,1) = x(1,1)^\sigma \tag{3.6}$$

y para $\sigma = 1 = \tau$ se tiene que $x(1,\theta)x(1,1) = x(1,\theta)x(1,\theta)^1$ y por lo tanto

$$x(1,1) = x(1,\theta). \tag{3.7}$$

Poniendo $y(\sigma) := x(1,1)$ para todo $\sigma \in G$, se obtiene una 2-cofrontera

$$y(\sigma,\tau) := y(\sigma)y(\sigma\tau)^{-1}y(\tau)^\sigma \tag{3.8}$$

y el 2-cociclo

$$x'(\sigma,\tau) := x(\sigma,\tau)y(\sigma,\tau)^{-1}.$$

que está en la misma clase de cohomología que $x(\sigma,\tau)$; está normalizado ya que:

$$\begin{aligned} x'(\sigma,1) &= x(\sigma,1)y(\sigma,1)^{-1} \\ &= x(\sigma,1)\left(y(\sigma)y(\sigma)^{-1}y(1)^\sigma\right)^{-1} \\ &= x(\sigma,1)(x(1,1)^\sigma)^{-1} \quad \text{por definición } y(1) = x(1,1) \\ &= x(1,1)^\sigma(x(1,1)^\sigma)^{-1} \quad \text{por (6)} \\ &= 1, \end{aligned}$$

y también

$$\begin{aligned} x'(1,\tau) &= x(1,\tau)y(1,\tau)^{-1} \\ &= x(1,\tau)\left(y(1)y(\tau)^{-1}y(\tau)^1\right)^{-1} \\ &= x(1,\tau)\left(x(1,1)\right)^{-1} \quad \text{por definición } y(1) = x(1,1) \\ &= x(1,1)(x(1,1)^{-1} \quad \text{por (7)} \\ &= 1. \end{aligned}$$

Así, podemos elegir un 2-cociclo normalizado $x(\sigma,\tau)$ en la clase $c \in H^2(G,M)$. Consideremos ahora el conjunto $M \times G$ con la multiplicación definida mediante:

$$(a,\sigma)(b,\tau) := (x(\sigma,\tau)ab^\sigma, \sigma\tau).$$

(i) Este producto es asociativo. En efecto,

$$\begin{aligned} ((a,\sigma)(b,\tau))(c,\theta) &= (x(\sigma,\tau)ab^\sigma, \sigma\tau)(c,\theta) \\ &= (x(\sigma\tau,\theta)x(\sigma,\tau)ab^\sigma c^{\sigma\tau}, \sigma\tau\theta) \end{aligned}$$

y

$$\begin{aligned}(a,\sigma)((b,\tau)(c,\theta)) &= (a,\sigma)(x(\tau,\theta)bc^{\tau},\tau\theta)\\ &= (x(\sigma,\tau\theta)a(x(\tau,\theta)bc^{\tau})^{\sigma},\sigma\tau\theta)\\ &= (x(\sigma\tau,\theta)x(\sigma,\tau)ab^{\sigma}c^{\sigma\tau},\sigma\tau\theta)\end{aligned}$$

la última igualdad porque M es abeliano y $x(\tau,\theta), a \in M$. Se sigue que $((a,\sigma)(b,\tau))(c,\theta) = (a,\sigma)((b,\tau)(c,\theta))$.

(ii) El $(1,1) \in M \times G$ es neutro para el producto anterior, ya que:

$$(a,\sigma)(1,1) = (x(\sigma,1)a \cdot 1^{\sigma}, \sigma \cdot 1) = (x(\sigma,1)a,\sigma) = (a,\sigma)$$

porque $x(\sigma,1) = 1$ ya que x está normalizado.

(iii) Si $(a,\sigma) \in M \times G$ entonces $\left(((x(\sigma,\sigma^{-1})a)^{-1})^{\sigma^{-1}}, \sigma^{-1}\right)$ es su inverso, ya que

$$\begin{aligned}(a,\sigma)(((x(\sigma,\sigma^{-1})a)^{-1})^{\sigma^{-1}},\sigma^{-1}) &= (x(\sigma,\sigma^{-1})a(((x(\sigma,\sigma^{-1})a)^{-1})^{\sigma^{-1}})^{\sigma},\sigma\sigma^{-1})\\ &= (x(\sigma,\sigma^{-1})ax(\sigma,\sigma^{-1})a)^{-1},1)\\ &= (x(\sigma,\sigma^{-1})aa^{-1}(x(\sigma,\sigma^{-1}))^{-1},1)\\ &= (1,1).\end{aligned}$$

Así, $M \times G$ es un grupo con la operación anterior y lo denotaremos mediante $M\hat{\times}G$; observando que se tienen morfismos $M \to M\hat{\times}G$ dado por $a \mapsto (a,1)$ y $M\hat{\times}G \to G$ dado por $(a,\sigma) \mapsto \sigma$, de tal forma que la sucesión siguiente es exacta:

$$\hat{\mathcal{G}}: \qquad 1 \to M \to M\hat{\times}G \to G \to 1.$$

Observamos también que G actúa en el grupo M como sigue: se tiene una sección $s : G \to M\hat{\times}G$ dada por $s(\sigma) := (1,\sigma)$ y, por definición del inverso en $M\hat{\times}G$, se tiene que $s(\sigma)^{-1} = ((s(\sigma,\sigma^{-1})^{-1})^{\sigma^{-1}},\sigma^{-1})$ y así, para cualquier $a \in M$, como $M \subseteq M\hat{\times}G$ identificamos a $a = (a,1) \in M\hat{\times}G$ y se tiene entonces:

$$\begin{aligned}s(\sigma)(a,1)s(\sigma)^{-1} &= (1,\sigma)(a,1)((x(\sigma,\sigma^{-1})^{-1})^{\sigma^{-1}},\sigma^{-1})\\ &= (x(\sigma,1)a^{\sigma},\sigma)((x(\sigma,\sigma^{-1})^{-1})^{\sigma^{-1}},\sigma^{-1})\\ &= (x,(\sigma,\sigma^{-1})x(\sigma,1)a^{\sigma}((x(\sigma,\sigma^{-1})^{-1})^{\sigma^{-1}})^{\sigma},1)\\ &= (a^{\sigma},1) \quad \text{ya que } x(\sigma,1) = 1\end{aligned}$$

es decir, G actúa en M por conjugación. Se sigue que $\hat{\mathcal{G}}$ es un elemento de $Ext(M,G)$ y la idea es definir

$$\Psi(c) := [\hat{\mathcal{G}}] \in Ext(M,G),$$

y para ver que ésta es una buena definición debemos probar que no depende de la elección del 2-cociclo normalizado en la clase de cohomología c.
En efecto, si $x'(\sigma,\tau)$ es otro cociclo normalizado en c, entonces $x'(\sigma,\tau)x(\sigma,\tau)y(\sigma,\tau)^{-1}$ con $y(\sigma,\tau) = y(\sigma)y(\sigma\tau)]^{-1}y(\tau)^{\sigma}$ una 2-cofrontera. Sea $M\tilde{\times}G$ el conjunto $M\times G$ con la operación de grupo definida usando el cociclo $x'(\sigma,\tau)$ y definamos la función

$$f \ : \ M\hat{\times}G \to M\tilde{\times}G$$

mediante $f(a,\sigma) := (y(\sigma)a,\sigma)$. Entonces, f es un homomorfismo de grupos (Observando que $y(1) = 1$ ya que $1 = x'(1,\sigma) = x(1,\sigma)y(1)^{-1} = y(1)^{-1}$), y el diagrama siguiente conmuta:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \xrightarrow{i} & M\hat{\times}G & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow f & & \| & & \\ 1 & \longrightarrow & M & \longrightarrow & M\tilde{\times}G & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

se sigue que $[\hat{\mathcal{G}}] = [\tilde{\mathcal{G}}]$ en $Ext(M,G)$ y por lo tanto Ψ está bien definida.
Finalmente, Ψ es inversa de Φ ya que si

$$1 \longrightarrow M \xrightarrow{i} E \underset{\rho}{\overset{s}{\leftrightarrows}} G \longrightarrow 1$$

es una extensión de M por G y si $x(\sigma,\tau)$ es el 2-cociclo correspondiente a la sección s, i.e., $\Phi[\varepsilon] = [x(\sigma,\tau)]$, sea $M\hat{\times}G$ la extensión asociada a $x(\sigma,\tau)$. Entonces, la función $f : M\hat{\times}G \to E$ dada por $f(a,\sigma) := i(a)s(\sigma)$, es un homomorfismo que hace equivalentes las extensiones ε y $M\hat{\times}G$ y por lo tanto $\Psi\circ\Phi[\varepsilon] = [M\hat{\times}G] = [\varepsilon]$. □

En general, no se tienen interpretaciones concretas, como en los casos de $H^0(G,M)$, $H^1(G,M)$ y $H^2(G,M)$ para los otros grupos de cohomología $H^n(G,M)$, con $n \geq 3$, y sin embargo todos estos grupos nos dan información algebraica que puede ser usada en problemas concretos, digamos de la aritmética. [5]

3.2. Cambio de grupos

Si $f : G' \to G$ es un homomorfismo de grupos y M es un G-módulo entonces M es un G'-módulo por cambio de anillos ya que el morfismo $f : G' \to G$ se extiende a un morfismo de anillos $f : \mathbb{Z}G' \to \mathbb{Z}G$ de la forma esperada: $\sum m_\sigma \cdot \sigma \mapsto \sum m_\sigma \cdot f(\sigma)$, y para el $\mathbb{Z}G$-módulo M y el morfismo de anillos $f : \mathbb{Z}G' \to \mathbb{Z}G$ definimoos, para toda $x \in M$ y para todo $a' \in \mathbb{Z}G'$, la acción $a'x := f(a')x$, se puede apreciar que M con esta acción es un $\mathbb{Z}G$-módulo. Algunas veces se usará la notación $f^*(M)$ para denotar esta estructura de $\mathbb{Z}G'$-módulo de M, y en otras ocasiones se usará simplemente M para denotar ambs estructuras si no hay lugar a confusión.
Observemos ahora que, como subgrupos abelianos, se tiene una inclusión $M^G \subseteq (f^*(M))^{G'}$, ya que si $x \in M^G$ entonces para todo $\sigma' \in G'$ se tiene que

$$\sigma' x = f(\sigma')x = x,$$

la primera igualdad por la definición de la acción de G' y la segunda igualdad porque $x \in M^G$ y $f(\sigma') \in G$.
De esta observación se sigue que:

$$H^0(G, M) = M^G \subseteq (f^*(M))^{G'} = H^0(G', f^*(M)),$$

y por la propiedad universal de los funtores derivados, el morfismo anterior se extiende a un morfismo de funtores de cohomología:

$$H^q(G, M) \xrightarrow{f^*} H^q(G', f^*(M)),$$

al cual llamamos el morfismo inducido por el cambio de grupos $f : G' \to G$.
Ahora veremos unos ejemplos de morfismos para cambios de grupos:

El morfismo de restricción. Si $H \subseteq G$ es un subgrupo e $i : H \hookrightarrow G$ es el morfismo dado por la inclusión, por cambio de grupos obtenemos morfismos

$$i^* : H^q(G, M) \to H^q(H, M),$$

llamados morfismos de restricción y a los que denotaremos por $i^* = Res^G_H$.
Si $K \subseteq H \subseteq G$ son subgrupos, entonces $Res^G_H \circ Res^H_K = Res^G_K$. Sea $\sigma \in Res^G_H \circ Res^H_K$, entonces, el morfismo σ es de la forma

$$\sigma : H^q(G, M) \to H^q(H, M) \to H^q(K, M)$$

en particular, se tiene que

$$\sigma : H^q(G, M) \to H^q(K, M)$$

por lo que $\sigma \in Res^G_K$. Por otro lado, sea $\phi \in Res^G_K$, entonces

$$\phi \ : \ H^q(G, M) \to H^q(K, M)$$

Como ϕ es el morfismo de restricción y $K \subseteq H$, entonces se puede restringir a ϕ de la siguiente manera:

$$\phi^* \ : \ H^q(H, M) \to H^q(K, M)$$

De igual manera, como $H \in G$, se puede reestringir a ϕ aún más, para que

$$\phi^{**} \ : \ H^q(G, M) \to H^q(H, M)$$

Utilizando las 2 ecuaciones anteriores, se concluye que $\phi \in Res^G_H \circ Res^H_K$ y por lo tanto $Res^G_H \circ Res^H_K = Res^G_K$ i.e., el morfismo de restricción es transitivo.

La construcción del morfismo inducido por el cambio de grupos se suele generalizar considerando un homomorfismo de grupos $f \ : \ G' \to G$ y un morfismo de grupos abelianos $g \ : \ M \to M'$ tal que M es un G-módulo y M' es un G'-módulo; en esta situación diremos que f y g son compatibles si para toda $x \in M$ y todo $\sigma' \in G'$ se tiene que $g(f(\sigma') \cdot x) = \sigma' \cdot g(x)$ i.e., si g es un G'-morfismo de $f^*(M)$ en M'. Se sigue que el G'-morfismo $g \ : \ f^*(M) \to M'$ induce morfismos

$$H^q(G', f^*(M)) \to H^q(G', M'),$$

y por cambio de grupos el homomorfismo $f \ : \ G' \to G$ induce morfismos

$$H^q(G, M) \to H^q(G', f^*(M)),$$

y componiendo estos dos morfismos inducidos, obtenemos morfismos

$$H^q(G, M) \to H^q(G', M'),$$

a los cuales denotaremos algunas veces por $(f, g)^*$ y diremos que son los morfismos inducidos por el par (f, g).

El morfismo de inflación. Si $H \lhd G$ es un subgrupo normal, consideremos el epimorfismo canónico $f \ : \ G \to G/H$; y si M es un G-módulo observemos que M^H es un (G/H)-módulo mediante la acción $(\sigma H)x := \sigma x$ donde basta observar que si $x \in M^H$, entonces $(\sigma H)x = \sigma x \in M^H$ ya que para toda $h \in H$, $h(\sigma x) = (h\sigma)x = (\sigma h')x = \sigma x$ donde usamos que $\sigma H = H\sigma$ por lo que $\sigma h = h'\sigma$ para un $h' \in H$; así podemos considerar la inclusión de grupos abelianos

$g : M^H \hookrightarrow M$ y observamos que los morfismos (f, g) son compatibles ya que si $x \in M^H$ y $\sigma' \in G$, entonces

$$\begin{aligned} g(f(\sigma') \cdot x) &= g((\sigma' H) \cdot x) \\ &= g(\sigma' \cdot x) \quad \text{por definición de la acción de } G/H \text{ en } M^H \\ &= \sigma' \cdot x \quad \text{ya que } g \text{ es la inclusión} \\ &= \sigma' \cdot g(x) \quad \text{ya que } x \in M^H \text{ y } g \text{ es la inclusión.} \end{aligned}$$

Se sigue que el par (f, g) induce morfismos

$$H^q(G/H, M^H) \to H^q(G.M)$$

a los que se les llama morfismos de inflación y se denotan por $(f, g)^* = Inf_G^{G/H}$.

Conjugación. Otro ejemplo esta dado tomando $G = G', M = M'$, el homomorfismo $f = f_\sigma : G \to G$ la conjugación por σ, i.e., $f_\sigma(s) := \sigma s \sigma^{-1}$ y el homomorfismo de grupos abelianos $g = g_\sigma : M \to M$ dado por $g_\sigma := \sigma^{-1} x$. Observamos que (f_σ, g_σ) son compatibles ya que si $s \in G$ y $x \in M$, entonces

$$g_\sigma(f_\sigma(s) \cdot x) = \sigma^{-1}(f_\sigma(s) \cdot x) = \sigma^{-1}(\sigma s \sigma^{-1} \cdot x) = s\sigma^{-1} \cdot x = s \cdot g_\sigma(x).$$

Se sigue que el par (f_σ, g_σ) induce morfismos

$$c_\sigma := (f_\sigma, g_\sigma)^* : H^q(G, M) \to H^q(G, M),$$

y se tiene que:

Proposición 3.2.1. *Los morfismos c_σ inducidos por la conjugación, son la identidad.*

Demostración. Por inducción sobre $q \geq 0$. Para $q = 0$ se tiene

$$c_\sigma : M^G = H^0(G, M) \to H^0(G, M) = M^G,$$

es tal que si $x \in M^G$,

$$c_\sigma(x) = g_\sigma(x) = \sigma^{-1} x = x = id(x),$$

la penúltima igualdad porque $\sigma^{-1} \in G$ y $x \in M^G$.
Supongamos que el resultado es válido para $q > 0$. Sea Q un $\mathbb{Z}G$-módulo inyectivo tal que M se sumerge en Q y sea N el cociente. Se tiene entonces una sucesión exacta corta $0 \to M \to Q \to N \to 0$, y considerando el morfismo $g_\sigma : M \to M$

tenemos el diagrama siguiente:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & Q & \longrightarrow & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g_\sigma} & & \vdots{\scriptstyle g'_\sigma} & & \vdots{\scriptstyle g''_\sigma} & & \\ 0 & \longrightarrow & M & \longrightarrow & Q & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

donde, si definimos el morfismo g'_σ mediante $g'_\sigma(x) = \sigma^{-1}x$, entonces el cuadrado de la izquierda conmuta y por paso al cociente definimos g''_σ de tal forma que el cuadrado de la derecha también conmuta.
Este diagrama conmutativo induce una escalera conmutativa:

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & H^q(G,N) & \xrightarrow{\delta} & H^{q+1}(G,M) & \longrightarrow & H^{q+1}(G,Q) & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle c''_\sigma} & & \downarrow{\scriptstyle c_\sigma} & & \downarrow{\scriptstyle c'_\sigma} & & \\ \cdots & \longrightarrow & H^q(G,N) & \xrightarrow[\delta]{} & H^{q+1}(G,M) & \longrightarrow & H^{q+1}(G,Q) & \longrightarrow & \cdots \end{array}$$

donde $H^{q+1}(G,Q) = 0$ ya que Q es inyectivo y donde $c''_\sigma = id$ por hipótesis de inducción. Se sigue que $c_\sigma = id \ : \ H^{q+1}(G,M) \to H^{q+1}(G,M)$. □

3.3. La sucesión inflación-restricción

Si $H \lhd G$ es un subgrupo normal, hemos definido los morfismos

$$Res \ : \ H^q(G,M) \to H^q(H,M)$$

e

$$Inf \ : \ H^q(G/H, M^H) \to H^q(G,M)$$

para toda $q \geq 0$.

Proposición 3.3.1. *La sucesión siguiente es exacta:*

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

Demostración. El morfismo Inf es inyectivo ya que si $f \ : \ G/H \to M^H$ es un 1-cociclo tal que $Inf(f) = 0 \in H^1(G,M)$, entonces $Inf(f) \ : \ G \to M$ es una 1-cofrontera i.e., existe $x \in M$ tal que para todo $\sigma \in G$, $Inf(f)(\sigma) = \sigma x - x$. Mostraremos que $x \in M^H$ y así f será cohomólogo a 0 en $H^1(G, M^H)$ como se requiere. Para ver que $x \in M^H$, observemos que

$$Inf(f) \ : \ G \to G/H \xrightarrow{f} M^H \hookrightarrow M$$

y así

$$\sigma x - x = Inf(f)(\sigma) = f(\sigma H) = f(\sigma h H) = \sigma h x - x$$

para todo $h \in H$ (ya que depende sólo de la clase lateral mod H); se sigue que $\sigma x - x = \sigma h x - x$ para todo $h \in H$ i.e., $\sigma x = \sigma h x$ para todo $h \in H$, i.e., $x = hx$ para todo $h \in H$, i.e., $x \in M^H$.
Mostraremos ahora que $Res \circ Inf = 0$. En efecto, sea $f : G/H \to M$ un 1-cociclo en $Ker(Res)$, i.e., $Res(f)$ es una 1-cofrontera en $H^1(H, M)$, i.e., existe $x \in M$ tal que $f(h) = hx - x$ para todo $h \in H$. Sea $g : G \to M$ la cofrontera dada por $g(\sigma)\sigma x - x$ para todo $\sigma \in G$ (usando la misma x anterior). Notamos entonces que $(f - g)(h) = 0$ para toda $h \in H$ y así pordemos suponer, sin perder generalidad, que $f(h) = 0$ para toda $h \in H$.
Observemos ahora que, para toda $\sigma \in G$ y para toda $h \in H$,

$$f(\sigma h) = f(\sigma) + \sigma f(h) = f(\sigma)$$

ya que f es un 1-cociclo y $f(h) = 0$. Se sigue que $f(\sigma H) = f(\sigma)$ y así f induce un morfismo $\tilde{f} : G/H \to M$.
Ahora, como $\sigma H = H\sigma$ entonces

$$f(h\sigma) = f(\sigma h') = f(\sigma),$$

(la primera igualdad para algún $h' \in H$ y la segunda igualdad por la fórmula del párrafo anterior)]. Y como

$$f(h\sigma) = hf(\sigma) + f(h) = hf(\sigma)$$

ya que $f(h) = 0$, entonces

$$hf(\sigma) = f(h\sigma) = f(\sigma)$$

para toda $h \in H$; es decir, $f(\sigma) \in M^H$. Se sigue que en realidad $\tilde{f} : G/H \to M^H$, y es claro que $Inf(\tilde{f}) = f$. □

Para poder generalizar esta sucesión necesitaremos una clase de módulos que, como los módulos inyectivos, son tales que $H^*(G, \ ) = 0$, pero son más manejables.

Definición 3.3.1. *Sean G un grupo, $H \subseteq G$ un subgrupo y N un H-módulo. Se define*

$$Ing_G^H(N) = \{f : G \to N : f \text{ es una función y } f(h\sigma) = hf(\sigma) \forall h \in H\}.$$

Nótese que $Ind_G^H(N)$ es un grupo abeliano con la suma usual de funciones (usando la suma de M). Más aún, $Ind_G^H(N)$ tiene una estructura de G-módulo izquierdo mediante la acción siguiente: si $f \in Ind_G(N)$ y $\sigma \in G$, entonces $\sigma \cdot f : G \to N$ es la función dada por

$$(\sigma \cdot f)(\tau) := f(\tau\sigma) \qquad \text{para toda } \tau \in G.$$

En el caso particular cuando $H = \{1\}$ es el subgrupo trivial, usaremos la notación $Ind_G(N) = Ind_G^1(N)$, notando que en este caso un $\{1\}$-módulo N es sólo un grupo abeliano. Un G-módulo Q se llama G-coinducido si tiene la forma:

$$Q \simeq Ind_G(N).$$

para algún grupo abeliano N. Los factores directos de un módulo coinducido se llaman módulos relativamente inyectivos.

La primera parte del lema siguiente es un análogo de recirpocidad de Frobenius y la segunda parte identifica como un Hom a los módulos coinducidos:

Lemma 3.3.2. *Sean $H \subseteq G$ un subgrupo, M un G-módulo y N un H-módulo.*

(1) Se tiene un isomorfismo natural

$$Hom_G(M, Ind_G^H(N)) \xrightarrow{\sim} Hom_H(M, N),$$

donde a la derecha M es visto como un H-módulo por el cambio de anillos dado por la inclusión $H \subseteq G$.

(2) En particular, para $M = \mathbb{Z}G$, se tiene

$$Ind_G^H(N) \simeq Hom_H(\mathbb{Z}G, N),$$

de tal forma que si $H = \{1\}$, se tiene que

$$Ind_G(N) \simeq Hom_{\mathbb{Z}}(\mathbb{Z}G, N).$$

Demostración. Definimos $\Phi : Hom_G(M, Ind_G^H(N)) \to Hom_H(M, N)$ mediante: si $g \in Hom_G(M, Ind_G^H(N))$, entonces para todo $x \in M$, $g(x) \in Ind_G^H(N)$, y así, para cualquier $\tau \in G$, $g(x)(\tau) \in N$, por lo que si $\tau \in H \subseteq G$ se tiene que $g(x)(\tau) = g(x)(\tau \cdot 1) = \tau g(x)(1)$ por definición de $Ind_G^H(N)$. Se define entonces $(\Phi(g))(x) := g(x)(1)$. Se tiene que $\Phi(g) : M \to N$ es H-covariante ya que si $\tau \in H$, entonces $\Phi(g)(\tau x) = g(\tau x)(1) = \tau g(x)(1) = \tau\Phi(g)(x)$. Para ver que Φ es un isomorfismo, definimos su inversa $Psi : Hom_H(M, N) \to$

$Hom_G(M, Ind_G^H(N))$ como sigue: sea $g \in Hom_H(M,N)$; entonces $\Psi(g) \in Hom_G(M, Ind_G^H(N))$ está dado por $(\Psi(g)(x))(\tau) := g(\tau x)$. Al momento de hacer composición, se puede verificar que Ψ y Φ son inversas una de la otra.
La segunda parte se sigue de los isomorfismos naturales

$$Ind_G^H(N) \simeq Hom_{\mathbb{Z}G}(\mathbb{Z}G, Ind_G^H(N)) \simeq Hom_{\mathbb{Z}H}(\mathbb{Z}G, N),$$

donde el segundo isomorfismo es el de la parte (1). □

Observación. El G-isomorfismo $Ind_G(N) \simeq Hom_{\mathbb{Z}}(\mathbb{Z}G, N)$ nos dice, en particular, que $Hom_{\mathbb{Z}}(\mathbb{Z}G, N)$ es un G-módulo izquierdo mediante la G-acción dada por $(\sigma \cdot f)(\tau) := f(\tau\sigma)$ correspondiente a la G-acción en $Ind_G(N)$.

Proposición 3.3.2. *Para todo G-módulo M existe un G-módulo coinducido Q y un G-monomorfismo $\phi : M \hookrightarrow Q$.*

Demostración. Sea $Q := Ind_G(M)$ considerando a M sólo como grupo abeliano, y definamos $\phi : M \to Q$ mediante la regla: para todo $x \in M$ sea $\phi(x) : G \to M$ dado por $\phi(x)(\sigma) := \sigma \cdot x$. Se puede demostrar (similarmente como en el lema anterior) que ϕ es un G-morfismo, y es inyectivo ya que si $\phi(x) = 0 : G \to M$, en particular para el $1 \in G$ se tiene que $0 = \phi(x)(1) = 1 \cdot x = x$, i.e., $x = 0$. □

Proposición 3.3.3. *Sea G un grupo. Si Q es un G-módulo relativamente inyectivo, entonces*

$$H^q(G, Q) = 0 \qquad \textit{para todo } q \geq 1.$$

Demostración. Como $H^q(G, \ )$ es un funtor aditivo, basta probar la proposición en el caso cuando Q es un módulo coinducido, i.e., cuando $Q := Ing_G(M)$. En este caso se tienen isomorfismos naturales de funtores:

$$\begin{aligned} Hom_G(\ , Q) &= Hom_G(\ , Ind_G(M)) \\ &\simeq Hom_{\mathbb{Z}}(\ , M), \quad \text{por el lema (3,3,2).} \end{aligned}$$

Ahora, sea $(P)_{\mathbb{Z}} : \cdots \to P_i \to \cdots \to P_1 \to P_0 \to \mathbb{Z} \to 0$ una resolución del G-módulo $\mathbb{Z}$. Aplicando el funtor $Hom_{\mathbb{Z}G}(\ , Q) \simeq Hom_{\mathbb{Z}}(\ , M)$ y descabezando se obtiene:

$$\begin{array}{ccccccccc} Hom_G(P_0, Q) & \longrightarrow & Hom_G(P_1, Q) & \longrightarrow & \cdots & \longrightarrow & Hom_G(P_i, Q) & \longrightarrow & \cdots \\ \downarrow \simeq & & \downarrow \simeq & & & & \downarrow \simeq & & \\ Hom_{\mathbb{Z}}(P_0, M) & \longrightarrow & Hom_{\mathbb{Z}}(P_1, M) & \longrightarrow & \cdots & \longrightarrow & Hom_{\mathbb{Z}}(P_i, M) & \longrightarrow & \cdots \end{array}$$

donde los cuadrados conmutan por la naturalidad de los isomorfismos verticales. Se sigue que, para toda $q \geq 1$,

$$\begin{aligned} H^q(G, Q) &= H^q(Hom_G(\mathcal{P}_{\mathbb{Z}}, Q) \\ &\simeq H^q(Hom_{\mathbb{Z}}(\mathcal{P}_{\mathbb{Z}}, M) \\ &= Ext^q_{\mathbb{Z}}(\mathbb{Z}, M) = 0 \end{aligned}$$

(la última igualdad porque $\mathbb{Z}$ es $\mathbb{Z}$-proyectivo). □

Corolario 3.3.3. *Si $0 \to M \to Q \to N \to 0$ es una sucesión exacta de G-módulos con Q coinducido, entonces*

$$H^q(G, N) \simeq H^{q+1}(G, M) \quad \textit{para todo } q \geq 1.$$

Demostración. La sucesión larga de cohomología asociada a la sucesión exacta corta dada tiene la forma:

$$\cdots \to H^q(G, Q) \to H^q(G, N) \xrightarrow{\delta} H^{q+1}(G, M) \to H^{q+1}(G, Q) \to \cdots,$$

donde los grupos de los extremos son nulos por la proposición anterior. Se sigue que δ es un isomorfismo para $q \geq 1$. □

Lemma 3.3.4. *Si $H \subseteq G$ es un subgrupo entonces $\mathbb{Z}G$ es libre como $\mathbb{Z}H$-módulo.*

Demostración. Escojamos un sistema de representantes $\{\sigma_i\}$ de las clases laterales izquierdas de G/H. Así, el conjunto G es la unión disjunta de las clases laterales izquierdas $\sigma_i H$. La parte de $\mathbb{Z}G$ expandida linealmente por la clase lateral $\sigma_i H$, para i fijo, es un H-módulo isomorfo a $\mathbb{Z}H$. Se sigue que el H-módulo $\mathbb{Z}G$ es una suma directa de submódulos cada uno de ellos isomorfo a $\mathbb{Z}H$. □

Proposición 3.3.4. *Si $H \subseteq G$ es un subgrupo y Q es un G-módulo coinducido, entonces Q es un H-módulo coinducido. Si además $H \lhd G$, entonces Q^H es G/H-coinducido.*

Demostración. Como $\mathbb{Z}G$ es un $\mathbb{Z}H$-módulo libre, se puede escribir de laa forma:

$$\mathbb{Z}G \simeq \mathbb{Z}H \otimes_{\mathbb{Z}} M,$$

para algún grupo abeliano M, y como Q es G-coinducido, entonces $Q \simeq Ind_G(N)$ para algún grupo abeliano N y así

$$\begin{aligned} Q \simeq Ind_G(N) &\simeq Hom_{\mathbb{Z}}(\mathbb{Z}G, N) \quad \text{por el lema (3,3,2)(2)} \\ &\simeq Hom_{\mathbb{Z}}(\mathbb{Z}H \otimes_{\mathbb{Z}} M, N) \\ &\simeq Hom_{\mathbb{Z}}(\mathbb{Z}H, Hom_{\mathbb{Z}}(M, N)) \quad \text{por la adjunción entre } \otimes \text{ y } Hom, \end{aligned}$$

y así, Q es H-coinducido.
Finalmente, como Q es G-coinducido, $Q \simeq Hom_{\mathbb{Z}}(\mathbb{Z}G, N)$, entonces Q^H es G/H-coinducido ya que

$$\begin{aligned} Q^H &\simeq \{f \in Hom_{\mathbb{Z}}(\mathbb{Z}G, N) \ : \ \tau f = f, \quad \text{para toda } \tau \in H\} \\ &= \{f \in Hom_{\mathbb{Z}}(\mathbb{Z}G, N) \ : \ \tau f(\sigma) = f(\sigma), \quad \text{para toda } \tau \in H, \ \sigma \in G\} \\ &= \{f \in Hom_{\mathbb{Z}}(\mathbb{Z}G, N) \ : \ f(\tau\sigma) = f(\sigma), \quad \text{para toda } \tau \in H, \ \sigma \in G\} \\ &= \{f \in Hom_{\mathbb{Z}}(\mathbb{Z}G, N) \ : \ f(\sigma H) = f(\sigma), \quad \text{para toda } \sigma \in G\} \\ &= Hom_{\mathbb{Z}}(\mathbb{Z}[G/H], N) \\ &\simeq Ind_{G/H}(N). \end{aligned}$$

□

Podemos ahora generalizar la sucesión inflación-restricción (3,3,1) anterior:

Proposición 3.3.5. *Sean $H \lhd G$ un subgrupo normal y M un G-módulo. Sea $q \geq 0$ un entero y supongamos que*

$$H^i(H, M) = 0 \qquad \textit{para todo } i = 1, \ldots, q-1.$$

Entonces, la sucesión siguiente es exacta:

$$0 \to H^q(G/H, M^H) \xrightarrow{Inf} H^q(G, M) \xrightarrow{Res} H^q(H, M).$$

Demostración. Por inducción sobre q, el caso $q = 1$ es la proposición anterior. Supongamos ahora que $q > 1$ y sea Q un módulo G-coinducido tal que $M \hookrightarrow Q$. Consideremos la sucesión exacta corta de G-módulos

$$0 \to M \hookrightarrow Q \to Q/M \to 0$$

y recordemos que, como H-módulo , Q es coinducido también. Ahora, la sucesión larga de cohomología asociada a la sucesión corta anterior y el hecho de que $H^1(H, M) = 0$ por hipótesis, implican que la sucesión siguiente es exacta:

$$0 \to M^H \hookrightarrow Q^H \to (Q/M)^H \to 0.$$

Consideremos entonces el diagrama

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^{q-1}(G/H, (Q/M)^H) & \xrightarrow{Inf} & H^{q-1}(G, Q/M) & \xrightarrow{Res} & H^{q-1}(H, Q/M) \\ & & \downarrow \delta & & \downarrow \delta & & \downarrow \delta \\ 0 & \longrightarrow & H^q(G/H, M^H) & \xrightarrow{Inf} & H^q(G, M) & \xrightarrow{Res} & H^q(H, M) \end{array}$$

el cual es conmutativo ya que Inf y Res son morfismos de funtores de cohomología. Los morfismos de conexión δ (de las correspondientes sucesiones largas de cohomología) son isomorfismos ya que arriba y abajo de las flechas verticales están grupos de cohomología $H^*(\ )$ con coeficientes Q^H, Q, Q, respectivamente donde Q es G-coinducido por hipótesis, Q es H-coinducido y Q^H es G/H-coinducido por (3,3,4), y por lo tanto los grupos de cohomología correspondientes se anulan.

Observamos ahora que $H^1(H, Q/M) = 0$ para $1 \leq i \leq q-2$ ya que de la sucesión larga de cohomología asociada a la sucesión corta:

$$0 \to M \to Q \to Q/M \to 0$$

se obtiene la sucesión larga de cohomología:

$$\cdots \to H^i(H, Q) \to H^i(H, Q/M) \to H^{i+1}(H, M) \to \cdots$$

como Q es H-coinducido entonces $H^i(H, Q) = 0$ para toda $i \geq 1$, y por hipótesis de inducción $H^{i+1}(H, M) = 0$ para $i+1 \leq q-1$, i.e., para $i \leq q-2$. Se sigue que el grupo de enmedio $H^i(H, Q/M) = 0$ para $q \leq i \leq q-2$, es decir, Q/M satisface la hipótesis de inducción con $q-1$ en lugar de q y por lo tanto la sucesión de arriba en el diagrama anterior es exacta y consecuentemente la de abajo también. □

Corolario 3.3.5. *Si $H^i(H, M) = 0$ para $1 \leq i \leq q-1$, entonces*

$$Inf : H^i(G/H, M^H) \to H^i(G, M)$$

es un isomorfismo para $i \leq q-1$.

Demostración. Se sigue directo del diagrama en la demostración anterior. □

3.4. Restricción y correstricción

Sea $H \subseteq G$ un subgrupo de índice finito $n = [G : H]$. Sea M un G-módulo, al cual también pordemos considerar como un H-módulo por cambio de anillos. Nuestro objetivo ahora es definir morfismos

$$Cor : H^q(H, M) \to H^q(G, M) \qquad \text{para toda } q \geq 0,$$

que van en la dirección opuesta a la natural, i.e., en la dirección opuesta a la del morfismo restricción

$$Res : Hq(G, M) \to H^q(H, M)$$

inducido por la incllusión $H \subseteq G$.
Para definir el morfismo Cor procedemos como sigue: sea

$$G = \bigcup_{i=1}^{n} \sigma_i H$$

una descomposición de G en clases laterales izquierdas de H en G. Definiremos $Cor \ : \ H^q(H, M) \to H^q(G, M)$ inductivamente.

(1). Para $q = 0$, se define

$$Cor \ : \ M^H = H^0(H, M) \to H^0(G, M) = M^G,$$

para $x \in M^H$, como

$$Cor^0(x) = N_{G/H}(x) := \sum_{\sigma_i H \in G/H} \sigma_i x.$$

Entonces,

(i) Cor^0 no depende de los representantes σ_i de las clases laterales $\sigma_i H$ de G/H, ya que si tomamos otros representantes, digamos $\tau_i \in \sigma_i H$, entonces $\tau_i = \sigma_i h_i$ con $h_i \in H, 1 \leq i \leq n$, y así, para toda $x \in M^H$, se tiene que

$$\sum_i \tau_i x = \sum_i (\sigma_i h_i)x = \sum_i \sigma_i (h_i x) = \sum_i \sigma_i x$$

(ya que $h_i \in H$ y $x \in M^H$).

(ii) $Cor^0 \in M^G$, i.e., es G-invariante. Esto es porque si $\sigma \in G$, entonces

$$\sigma \cdot Cor^0(x) = \sigma \cdot \sum_i \sigma_i x = \sum_i (\sigma\sigma_i)x = Cor^0(x),$$

ya que $\sigma\sigma_i H$ recorre G/H cuando $\sigma_i H$ lo hace.

(iii) $Cor^0 \ : \ M^H \to M^G$ es un homomorfismo de grupos abelianos. En efecto, si $x, y \in M^H$, entonces

$$Cor^0(x + y) = \sum_i \sigma_i (x + y) = \sum_i \sigma_i x + \sum_i \sigma_i y = Cor^0(x) + Cor^0(y).$$

(2). Sea $q \geq 1$ y supongamos que $Cor^i(x)$ está definido para toda $i \leq q$. Sea Q un G-módulo coinducido tal que $M \hookrightarrow Q$. Consideremos la sucesión exacta corta

$$0 \to M \to Q \to Q/M \to 0$$

y las sucesiones largas de cohomología asociadas a $H^*(H,\ )$ y $H^*(G,\ )$ en el diagraama siguiente:

$$\begin{array}{ccccccccccc}
\cdots \longrightarrow & H^{q-1}(H,Q) & \longrightarrow & H^{q-1}(H,Q/M) & \xrightarrow{\delta} & H^q(H,M) & \longrightarrow & H^q(H,Q) & \longrightarrow \cdots \\
& \downarrow 0 & & \downarrow Cor^{q-1} & & \downarrow Cor^q & & \downarrow 0 & \\
\cdots \longrightarrow & H^{q-1}(G,Q) & \longrightarrow & H^{q-1}(G,Q/M) & \xrightarrow[\delta]{} & H^q(G,M) & \longrightarrow & H^q(G,Q) & \longrightarrow \cdots
\end{array}$$

En este diagrama los cuatro grupos de los extremos son nulos ya que Q es Gcoinducido y por lo tanto H-coinducido también. Se sigue que los morfismos δ son isomorfismos, y como Cor^{q-1} está definido por hipótesis de inducción, la conmutatividad del diagrama define Cor^q.

La propiedad principal del morfismo de correstricción es el siguiente:

Teorema 3.4.1. *Sea $H \subseteq G$ un subgrupo de índice finito $n = [G\ :\ H]$. Entonces para todo G-módulo M y para todo $q \geq 0$, la composición $Cor \circ Res = n$ es multiplicación por $n = [G\ :\ H]$ en $H^q(G,M)$, i.e., el diagrama siguiente conmuta para toda $q \geq 0$:*

$$\begin{array}{ccc}
H^q(G,M) & \xrightarrow{\qquad n \qquad} & H^q(G,M) \\
& {\scriptstyle Res}\searrow \quad \nearrow{\scriptstyle Cor} & \\
& H^q(H,M) &
\end{array}$$

Demostración. Por inducción sobre $q \geq 0$. Si $q = 0$, la composición

$$M^G \xhookrightarrow{Res} M^H \xrightarrow{Cor} M^G,$$

es tal que, para toda $x \in M^G$, se tiene que

$$Cor^0 \circ Res(x) = Cor^0(x) = \sum_{i=1}^{n} \sigma_i x = \sum_{i=1}^{n} x = nx,$$

(la última igualdad porque $x \in M^G$.
Sea $q \geq 1$ y supongamos el resultado cierto para $q-1$. Escojamos un G-módulo coinducido Q tal que $M \hookrightarrow Q$ y consideremos las sucesiones largas de cohomología asociadas a la sucesión exacta corta

$$0 \to M \to Q \to M/Q \to 0 :$$

$$\begin{array}{ccccccccc} 0 = H^{q-1}(G,Q) & \longrightarrow & H^{q-1}(G,Q/M) & \xrightarrow{\delta} & H^q(G,M) & \longrightarrow & H^q(G,Q) = 0 \\ \downarrow 0 & & \downarrow Cor^{q-1}\circ Res & & \downarrow Cor^q\circ Res & & \downarrow 0 \\ 0 = H^{q-1}(G,Q) & \longrightarrow & H^{q-1}(G,Q/M) & \xrightarrow[\delta]{} & H^q(G,M) & \longrightarrow & H^q(G,Q) = 0 \end{array}$$

Entonces los morfismos δ son isomorfos, y como por hipótesis de inducción $Cor^{q-1} \circ Res = n$, por conmutatividad se sigue que $Cor^q \circ Res = n$. □

Corolario 3.4.2. *Si G es un grupo finito de orden n, entonces*

$$n \cdot H^q(G, M) = 0$$

para todo $q \geq 1$ y todo G-módulo M.

Demostración. Sea $H = \{1\} \subseteq G$ el subgrupo trivial. Entonces $[G : H] = n$ y por el teorema anterior el diagrama siguiente conmuta

$$\begin{array}{ccc} H^q(G,M) & \xrightarrow{\quad n \quad} & H^q(G,M) \\ & {\scriptstyle Res}\searrow \quad \nearrow{\scriptstyle Cor} & \\ & H^q(\{1\},M) & \end{array}$$

para toda $q \geq 0$. Pero $H^q(\{1\}, M) = 0$ para toda $q \geq 1$. Se sigue que $n = Cor \circ Res = 0$, i.e., multiplicación por n es igual a cero. □

3.5. Homología de grupos

Sea M un G-módulo y sea $I_G M \subseteq M$ el subgrupo (abeliano) de M generado por todos los elementos de la forma $\sigma x - x$ con $x \in M$ y $\sigma \in G$.

Lemma 3.5.1. *(1) El grupo cociente $M_G := M/I_G M$ es un G-módulo (con la estructura inducida por la del G-módulo M) donde G actúa trivialmente.*

(2) Más aún, M_G es el mayor cociente de M en el cual G actúa trivialmente.

(3) Existe un isomorfismo natural

$$M_G \simeq \mathbb{Z} \otimes_{\mathbb{Z}G} M$$

y así el funtor $(\ )_G$ es exacto derecho y por lo tanto aditivo.

En el producto tensorial de la parte (3) se considera a $\mathbb{Z}$ como un G-módulo derecho trivial.
El morfismo $M_G \to \mathbb{Z} \otimes_{\mathbb{Z}G} M$ dado por $x + I_G M \mapsto 1 \times x$ es el isomorfismo requerido en (3).

Definición 3.5.2. *Si M es un G-módulo y $q \geq 0$ es un entero, el q-ésimo grupo de homología de G con coeficientes en M es*

$$H_q(G, M) := L_q(\mathbb{Z} \otimes_{\mathbb{Z}G} M) = Tor_q^{\mathbb{Z}G}(\mathbb{Z}, M).$$

Se tienen las propiedades usuales:

(1): $H_0(G, M) \simeq \mathbb{Z} \otimes_{\mathbb{Z}G} M \simeq M_G$.

(2): $H_q(G, M) = 0$ para toda $q \geq 1$ si M es un G-módulo proyectivo.

(3): Dada cualquier sucesión excta corta de G-módulos

$$0 \to M' \xrightarrow{\Phi} M \xrightarrow{\Psi} M'' \to 0.$$

se tiene asociada una sucesión larga de homología:

$$\cdots \xrightarrow{\delta} H_1(G, M') \xrightarrow{\Phi_*} H_1(G, M) \xrightarrow{\Psi_*} H_1(G, M'') \xrightarrow{\delta} M'_G \xrightarrow{\Phi_*} M_G \xrightarrow{\Psi_*} M''_G \to 0$$

en forma funtorial.

Dual a la definición de módulo coinducido (un G-módulo M es coinducido si y sólo si es de la forma $M \simeq Hom_{\mathbb{Z}}(\mathbb{Z}G, X)$ con X un grupo abeliano) tenemos la definición siguiente:

Definición 3.5.3. *Un G-módulo M se llama inducido si es de la forma*

$$\mathbb{Z}G \otimes_{\mathbb{Z}} X,$$

donde X es un grupo abeliano. Un sumando directo de un G-módulo inducido se llama un G-módulo relativamente proyectivo.

Observación. $\mathbb{Z}G \otimes_{\mathbb{Z}} X$ tiene estructura de G-módulo izquierdo mediante la acción: $\sigma \cdot (\tau \otimes x) := (\sigma\tau) \otimes x$, para $\sigma \in G$ y $\tau \otimes x \in \mathbb{Z}G \otimes_{\mathbb{Z}} X$.

Proposición 3.5.1. *Un G-módulo M es inducido si y sólo si M contiene un subgrupo X tal que*

$$M \simeq \bigoplus_{\sigma \in G} \sigma \cdot X.$$

Duales a los resultados correspondientes para módulos coinducidos se tiene:

Proposición 3.5.2. *(1) Todo G-módulo M es cociente de un G-módulo inducido.*

(2) Si Q es un G-módulo relativamente proyectivo entonces $H_q(G, Q) = 0$ para toda $q \geq 1$.

Duales a las construcciones de los morfismos de inflación y correstricción en cohomología tenemos los correspondientes para homología:

Si $H \subseteq G$ es un subgrupo cualquiera, la inclusión $H \hookrightarrow G$ induce morfismos

$$Cor \ : \ H_q(H, M) \to H_q(G, M)$$

llamados morfismos de correstricción, que en dimensión 0 son las inclusiones

$$Cor \ : \ H_0(H, M) = M_H = M/I_H M \hookrightarrow M/I_G M = M_G = H_0(G, M).$$

Y si $H \subseteq G$ es un subgrupo de índice finito, tenemos morfismos

$$Res \ : \ H_q(G, M) \to H_q(H, M)$$

llamados de restricción o de transferencia, que en dimensión $q = 0$ están definidos como sigue: dado $x \in M$, si $\sigma H = \tau H$ en G/H, entonces $\sigma^{-1}x = \tau^{-1}x$ en M_H, ya que podemos escribir $\sigma = \tau h$, con $h \in H$, y por lo tanto

$$\sigma^{-1}x = h^{-1}\tau^{-1}x = \tau^{-1}x,$$

ya que H actúa trivialmente en M_H. Se sigue que la expresión

$$N'_{G/H}(x) := \sum_{\sigma \in \sigma H \in G/H} \sigma^{-1}x$$

estáa bien definida en M_H. Se tiene así un morfismo $N' \ : \ M \to M_H = M/I_G M$; para ver que pasa al cociente y define un morfismo de M_G a M_H, observemos que en el diagrama siguiente:

$$\begin{array}{ccc} \mathbb{Z} \otimes_{\mathbb{Z}G} M & \simeq & M/I_G M \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle V} \\ \mathbb{Z} \otimes_{\mathbb{Z}H} M & \simeq & M/I_H M \end{array}$$

donde

$$T(m \otimes x) := \sum_{\sigma_i H \in G/H} (m\sigma_i \otimes \sigma_i^{-1}x) = \sum_{\sigma_i H \in G/H} (m \otimes \sigma_i^{-1}x)$$

y

$$V(x + I_G M) := \sum_{\sigma_i H \in G/H} \sigma_i^{-1} x + I_H M,$$

son tales que el diagrama conmuta ya que los isomorfismos horizontales mandan $m \otimes x \in \mathbb{Z} \otimes_G M$ a $mx + I_G M$ (y el otro similarmente), y así se tiene que:

$$T(m \otimes x) = \sum_{\sigma_i H \in G/H} (m \otimes \sigma_i^{-1} x) \mapsto \sum_{\sigma_i H \in G/H} m\sigma_i^{-1} x + I_H M$$

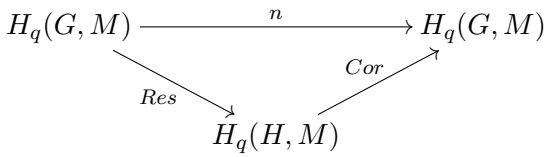
y por otro lado

$$V(m \otimes x) = V(mx + I_G M) = \sum_{\sigma_i H \in G/H} \sigma_i^{-1} mx + I_H M = \sum_{\sigma_i H \in G/H} m\sigma_i^{-1} x + I_H M,$$

que es igual a $T(m \otimes x)$. Se tiene así un homomorfismo $N'_{G/H} \ : \ M_G \to M_H$, y éste es el morfismo de restricción en dimensión $q = 0$:

$$Res_0 = N'_{G/H} \ : \ H_0(G, M) = M_G \to M_H = H_0(H, M).$$

Teorema 3.5.4. *Sea $H \subseteq G$ un subgrupo de índice finito $n = [G \ : \ H]$. Entonces, para todo G-módulo M y para toda $q \geq 0$, la composición $Cor \circ Res = n$ es multiplicación por $n = [G \ : \ H]$ en $H_q(G, M)$, i.e., el diagrama siguiente conmuta para toda $q \geq 0$:*



Se tiene también los análogos de la sucesión inflación-restricción y traslación de dimensión.

Lemma 3.5.5. *Sea G cualquier grupo y sea $I_G := Ker(\varepsilon \ : \ \mathbb{Z}G \to \mathbb{Z})$ el ideal de aumentación de G. Entonces, el grupo aaditivo de I_G es libre con base $\{\sigma - 1 \ : \ 1 \neq \sigma \in G\}$.*

Demostración. Por definición

$$I_G := Ker(\varepsilon \ : \ \mathbb{Z}G \to \mathbb{Z}) = \left\{ \sum_\sigma m_\sigma \cdot \sigma \ : \ \sum_\sigma m_\sigma = 0 \right\},$$

y por lo tanto los elementos de la forma $\sigma - 1$ están en I_G.
Observemos ahora que el conjunto $\{\sigma - 1 \ : \ 1 \neq \sigma \in G\}$ genera al grupo abeliano I_G, ya que si $u = \sum m_\sigma \sigma \in I_G$ entonces $\sum m_\sigma = 0$ y por lo tanto

$$u = u - \left(\sum m_\sigma \right) \cdot 1 = \sum m_\sigma \cdot \sigma - \sum m_\sigma \cdot 1 = \sum m_\sigma \cdot (\sigma - 1),$$

i.e., cada $u \in I_G$ es combinación lineal de los elementos de la forma $\sigma - 1$. Finalmente, observamos que el conjunto $\{\sigma - 1 \ : \ 1 \neq \sigma \in G\}$ es linealmente independiente sobre $\mathbb{Z}$ ya que si

$$\sum m_\sigma(\sigma - 1) = 0 \qquad \text{con } m_\sigma \in \mathbb{Z}$$

entonces

$$\sum m_\sigma \cdot \sigma - \sum m_\sigma \cdot 1 = 0 \qquad \text{en } \mathbb{Z}G.$$

Pero $\mathbb{Z}G$, como grupo abeliano, es libre con base G y como $\sigma, 1 \in G$ entonces la igualdad anterior es una combinación lineal en $\mathbb{Z}G$ con coeficientes en $\mathbb{Z}$ y por lo tanto todos los $m_\sigma = 0$. □

Proposición 3.5.3. *Si la acción de G en $\mathbb{Z}$ es trivial, entonces $H_1(G, \mathbb{Z}) \simeq G^{ab}$, donde $G^{ab} = G/G'$ es la abelianización del grupo G.*

Demostración. De la sucesión exacta corta $0 \to I_G \to \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \to 0$ y del hecho de que $\mathbb{Z}G$ es inducido se sigue que el morfismo de conexión de la sucesión larga de cohomología asociada es un isomorfismo:

$$\delta \ : \ H_1(G, \mathbb{Z}) \to H_0(G, I_G) = I_G/I_G^2.$$

Finalmente, se tiene un isomorfismo $G^{ab} = G/G' \to I_G/I_G^2$ dado como sigue: definimos $\Psi \ : \ I_G \to G/G'$ en los generadores (2,2,2) de I_G mediante $\Psi(\sigma - 1) := \sigma \cdot G'$. Se aprecia que Ψ es suprayectiva (recorre todas las clases laterales) y como

$$(\sigma - 1)(\tau - 1) = (\sigma\tau - 1) - (\sigma - 1) - (\tau - 1)$$

entonces Ψ para al cociente para definir

$$\tilde{\Psi} \ : \ I_G/I_G^2 \to G/G'.$$

Por otra parte, definimos $\Phi \ : \ G \to I_G/I_G^2$ mediante $\phi(\sigma) := (\sigma - 1) + I_G^2$; entonces Φ es un epimorfismo que pasa al cociente para definir:

$$\tilde{\Phi} \ : \ G/G' \to I_G/I_G^2.$$

Donde $\tilde{\Psi}$ y $\tilde{\Phi}$ son inversas una de la otra por como estan definidas dentro de las clases de equivalencia ($\Phi \circ \Psi(\sigma - 1) = \Phi(\sigma) = \sigma - 1$, utilizando las respectivas clases de equivalencia de G/G' y I_G/I_G^2 y similarmente, $\Psi \circ \Phi(\sigma) = \sigma$)). □

Capítulo 4

Cohomología de Grupos Finitos

Proposición 4.0.1. *Si G es un grupo finito, entonces para todo grupo abeliano X existe un G-isomorfismo*

$$Ind_G(X) \simeq Hom_{\mathbb{Z}}(\mathbb{Z}G, X) \simeq \mathbb{Z}G \otimes_{\mathbb{Z}} X.$$

Demostración. El primer isomorfismo es el del lema (3,3,2). Ahora, definamos $\Phi : Hom_{\mathbb{Z}}G, X) \to \mathbb{Z}G \otimes_{\mathbb{Z}} X$ mediante

$$f \mapsto \Phi(f) := \sum_{\sigma \in G} \sigma \otimes f(\sigma^{-1}).$$

La suma es finita porque G lo es y Φ es aditivo por la definición de la suma en Ind_G. Es G-morfismo ya que si $\tau \in G$ entonces

$$\begin{aligned}
\Phi(\tau \cdot f) &= \sum_{\sigma \in G} \sigma \otimes (\tau \cdot f)(\sigma^{-1}) \\
&= \sum_{\sigma \in G} \sigma \otimes f(\sigma^{-1}\tau) \quad \text{(definición de la acción en } Ind_G(X)) \\
&= \sum_{\sigma \in G} \tau\tau^{-1}\sigma \otimes f(\sigma^{-1}\tau) \\
&= \sum_{\sigma \in G} \tau(\sigma^{-1}\tau)^{-1} \otimes f(\sigma^{-1}\tau) \\
&= \tau \left(\sum_{\sigma \in G} (\sigma^{-1}\tau)^{-1} \otimes f(\sigma^{-1}\tau) \right) \quad \text{definición de la acción en el } \otimes) \\
&= \tau \cdot \Phi(f), \quad \text{porque } \sigma^{-1}\tau \text{ recorre } G \text{ cuando } \sigma \text{ lo hace.}
\end{aligned}$$

□

Corolario 4.0.1. *Si G es un grupo finito, entonces un G-módulo M es inducido si y sólo si es coinducido.*
Más aún, M es relativamente inyectivo si y sólo si M es relativamente proyectivo.

4.1. Cohomología de Tate

Los grupos de cohomología de Tate son un artificio para tener en un sólo concepto los grupos de cohomología y de homología de un grupo finito.[5]

Su construcción es como sigue: sea G un grupo finito. La norma de G es el elemento de $\mathbb{Z}G$ dado por

$$N_G := \sum_{\sigma \in G} \sigma \in \mathbb{Z}G.$$

Si M es un G-módulo, la norma anterior define un endomorfismo de M, denotado también con $N_G : M \to M$, mediante la fórmula:

$$N_G(x) := \sum_{\sigma \in G} \sigma \cdot x.$$

Lemma 4.1.1. *Si $I_G \subseteq \mathbb{Z}G$ es el ideal de aumentación, entonces*

$$I_G \cdot M \subseteq Ker(N_G) \tag{4.1}$$

y

$$Im(N_G) \subseteq M^G. \tag{4.2}$$

Demostración. (1): Por (3,5,5) el ideal I_G está generado por los elementos de la forma $\tau - 1$ y así, para $(\tau - 1)x \in I_G \cdot M$ se tiene que

$$N_G((\tau - 1)x) = \sum_{\sigma \in G} \sigma(\tau - 1)x = \sum_{\sigma \in G} \sigma\tau x - \sum_{\sigma \in G} \sigma x = N_G(x) - N_G(x) = 0.$$

(2): Para todo $\tau \in G$ se tiene que

$$\tau \cdot N_G(x) = \tau \sum_{\sigma \in G} \sigma x = \sum_{\sigma \in G} \tau\sigma x = N_G(x).$$

□

Se sigue que el morfismo $N_G : M \to M$ tiene imagen en M^G y su núcleo contiene a $I_G M$ y así define, por paso al cociente, un morfismo

$$N_G^* : M_G = M/I_G M \to M^G$$

y como

$$H_0(G, M) \simeq M_G$$

y

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

entonces $N_G \ : \ M \to M$ induce un morfismo

$$N_G^* \ : \ H_0(G, M) \to H^0(G, M).$$

Definición 4.1.2. *Sea G un grupo finito y M un G-módulo. Se definen*

$$\widehat{H}_0(G, M) := Ker(N_G^*)$$

y

$$\widehat{H}^0(G, M) := Coker(N_G^*).$$

Observemos que $Ker(N_G^*) = Ker(N_G)/I_G M$ y así, poniendo ${}_{N_G}M := Ker(N_G \ : \ M \to M)$, se tiene que

$$\widehat{H}_0(G, M) =_{N_G} M/I_G M$$

y

$$\widehat{H}^0(G, M) = M^G/N_G(M).$$

Proposición 4.1.1. *Si G es un grupo finito y M un G-módulo relativamente proyectivo, entonces:*

$$\widehat{H}_0(G, M) = 0 = \widehat{H}^0(G, M).$$

Demostración. Probaremos la proposición para $\widehat{H}^0(G, M)$ y observamos que basta probarla cuando M es inducido, en cuyo caso M es de la forma

$$M = \bigoplus_{\sigma \in G} \sigma \cdot X$$

con X un subgrupo de M. Así, cada $z \in M$ se puede escribir de manera única como

$$z = \sum_{\sigma \in G} \sigma x_\sigma$$

con $x_\sigma \in X$.
Además, $z \in M^G$ si y sólo si todos los x_σ son iguales, ya que: si todos los $x_\sigma = x$ entonces

$$z = \sum_{\sigma \in G} \sigma x_\sigma = \sum_{\sigma \in G} \sigma x = N_G(x) \in M^G$$

por la parte (2) del lema anterior. Recíprocamente, si $z \in M^G$ entonces, para toda $\tau \in G$:

$$\sum_{\sigma \in G} \sigma x_\sigma = z = \tau z = \tau \sum_{\sigma \in G} \sigma x_\sigma = \sum_{\sigma \in G} \tau(\sigma x_\sigma),$$

y por la unicidad de la expresión anterior para z, se sigue que todos los x_σ deben ser iguales.
Se sigue que $z \in M^G$ si y sólo si $z = N_G(x)$ para algún $x \in X \subseteq M$, i.e.,

$$M^G = Im(N_G) = N_G M,$$

y por lo tanto

$$\widehat{H}^0(G, M) = M^G / N_G M = 0.$$

□

Podemos ahora definir los grupos de cohomología de Tate:

Definición 4.1.3. *Sea G un grupo finito, M un G-módulo y $q \in \mathbb{Z}$ Los grupos de cohomología de Tate de G con coeficientes en M son los grupos*

$$\widehat{H}^q(G, M) := \begin{cases} H^q(G, M) & \text{si } q \geq 1 \\ \widehat{H}^0(G, M) = M^G / N_G M & \text{si } q = 0 \\ \widehat{H}_0(G, M) =_{N_G} M / I_G M & \text{si } q = -1 \\ H_{-1-q}(G, M) & \text{si } q \leq 2. \end{cases}$$

De esta definición y como una consecuencia inmediata de (4,1,1), (4,0,1) y los resultados correspondientes para homología y cohomología tenemos:

Corolario 4.1.4. *Sea G un grupo finito y M un G-módulo relativamente proyectivo (inyectivo). Entonces, $\widehat{H}^q(G, M) = 0$ para todo $q \in \mathbb{Z}$.*

Teorema 4.1.5. *Sea G un grupo finito. Para toda sucesión exacta corta de G-módulos*

$$0 \to M' \to M \to M'' \to 0$$

se tiene una sucesión larga de cohomología de Tate, que se extiende en ambas direcciones:

$$\cdots \to \widehat{H}^q(G, M') \to \widehat{H}^q(G, M) \to \widehat{H}^q(G, M'') \xrightarrow{\delta} \widehat{H}^{q+1}(G, M') \to \cdots$$

Demostración. Para $q \geq 1$ ó $q \leq -2$ no hay nada que probar: son las sucesiones largas de homología y cohomología correspondientes.

Ahora, asociado a la sucesión exacta corta de G-módulos dada, consideremos el diagraama siguiente:

$$\begin{array}{ccccccccc} H_1(G,M'') & \xrightarrow{\delta} & H_0(G,M') & \longrightarrow & H_0(G,M) & \longrightarrow & H_0(G,M'') & \longrightarrow & 0 \\ \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle N^*_{M'}} & & \downarrow{\scriptstyle N^*_{M}} & & \downarrow{\scriptstyle N^*_{M''}} & & \downarrow{\scriptstyle 0} \\ 0 & \longrightarrow & H^0(G,M') & \longrightarrow & H^0(G,M) & \longrightarrow & H^0(G,M'') & \xrightarrow{\delta} & H^1(G,M') \end{array}$$

donde el morfismo N^*_M es el morfismo N^*_G correspondiente a M y similarmente para M' y M''. Los dos cuadrados intesnos conmutan y la conmutatividad de los cuadrados exteriores se sigue de la definición de los correspondientes morfismos δ. La conmutatividad de este diagrama y el lema de la serpiente (sucesión núcleo-conúcleo) implican la existencia de un morfismo de conexión canónico:

$$\delta \ : \ Ker(N^*_{M''}) \to Coker(N^*_{M'})$$

y como $\widehat{H}^{-1}(G,M'') = \widehat{H}_0(G,M'') := Ker(N^*_{M''})$ y $\widehat{H}^0(G,M') := Coker(N^*_{M'})$, entonces hemos definico un morfismo de conexión

$$\delta \ : \ \widehat{H}_0(G,M'') \to \widehat{H}^0(G,M'),$$

la sucesión núcelo-conúcleo

$$Ker(N^*_{M'}) \to Ker(N^*_M) \to Ker(N^*_{M''}) \xrightarrow{\delta} Coker(N^*_{M'}) \to$$

$$\to Coker(N^*_M) \to Coker(N^*_{M''})$$

es exacta. La exactitud faltante en la sucesión del teorema es directa. □

Observación. El morfismo $\delta \ : \ \widehat{H}_0(G,M'') \to \widehat{H}^0(G,M'')$ está dado como sigue: si $c \in Ker(N^*_{M''})$, levantamos a c a un elemento $b \in M$; el elemento $N^*_M(b)$ proviene de un $a \in A^G$ y la imagen de a en $Coker(N^*_{M'})$ es por definición $\delta(c)$.

Corolario 4.1.6. *Si* $0 \to M \to Q \to N \to 0$ *es una sucesión exacta de* G*-módulos con* Q *coinducido, entonces*

$$\widehat{H}^q(G,N) \simeq \widehat{H}^{q+1}(G,M)$$

para todo $q \in \mathbb{Z}$.
Similarmente, si $0 \to N \to P \to M \to 0$ *es una sucesión exacta de* G*-módulos con* P *inducido, entonces*

$$\widehat{H}^{q-1}(G,M) \simeq \widehat{H}^q(G,N)$$

para todo $q \in \mathbb{Z}$.

Los grupos de cohomología de Tate son de hecho los grupos de cohomología de un complejo; en efecto, si $\mathcal{P} = \{P_n, d_n\}$ es una resolución de $\mathbb{Z}$ formada por G-módulos libres finitamente generados y si $\mathcal{P}^* = \{Hom(P_n, \mathbb{Z}), d_n^*)$ es su dual, se tiene sucesiones exactas:

$$\cdots \to P_2 \to P_1 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

y

$$0 \to \mathbb{Z} \xrightarrow{\varepsilon^*} P_1^* \to P_2^* \to \cdots,$$

(donde la sucesión dual es exacta ya que cada P_n es $\mathbb{Z}$-libre). Poniendo entonces

$$P_{-n} = P_n^*$$

y pegando las dos sucesiones exactas de arriba (i.e., pegando con el morfismo $\varepsilon^* \circ \varepsilon$), obtenemos una sucesión exacta larga:

$$\mathcal{L} \qquad \cdots \to P_2 \to P_1 \to P_{-1} \to P_{-2} \to \cdots$$

a la cual llamaremos una resolución completa de G.

Proposición 4.1.2. *Sea M un G-módulo. Los grupos de cohomología de Tate son los grupos de cohomología*

$$H^q(Hom_G(\mathcal{L}, M))$$

donde $\mathcal{L}$ es el complejo anterior.

Demostración. Si $q \geq 1$ no hay nada que probar. Si $q \leq -2$ observemos que si N es un G-módulo libre finitamente generado y $N^* := Hom(N, \mathbb{Z})$ es su dual, entonces se tiene un G-isomorfismo:

$$\Phi \ : \ N \otimes M \to Hom(N^*, M)$$

dado por $n \otimes m \mapsto (f \mapsto f(n) \cdot m)$, para $n \in N$, $m \in M$, $f \in N^*$. Por lo tanto, la composición

$$\theta \ : \ N \otimes_G M = (N \otimes M)_G \xrightarrow{N^*} (N \otimes M)^G \xrightarrow{\Phi} (Hom(N^*, M))^G = Hom_G(N^*, M)$$

es un isomorfismo. (Aquí N^* es un isomorfismo ya que por (4,1,1) el núcleo y el conúcleo del morfismo N^* son nulos porque $N \otimes M$ es un G-módulo inducido). Se sigue que

$$Hom_G(P_{-n}, M) \simeq P_n \otimes_G M,$$

y por lo tanto $H^{-q}(Hom_G(\mathcal{L}, M)) = H_q(G, M)$, para $q \geq 2$.
Finalmente, para los casos $q = 0, 1$, observemos que el morfismo

$$Hom_G(P_{-1}, M) \to Hom_G(P_1, M) \tag{4.3}$$

es inducido por la composición $P_1 \xrightarrow{\varepsilon} \mathbb{Z} \xrightarrow{\varepsilon^*} P_{-1}$. Ahora, si identificamos $Hom_G(P_{-1}, M)$ con $P_1 \otimes_G M$ mediante el isomorfismo θ, el morfismo (3) se vuelve un morfismo

$$P_1 \otimes_G M \to Hom_G(P_1, M),$$

y éste se puede factorizar como

$$P_1 \otimes_G M \to M_G \xrightarrow{N^*} M^G \to Hom_G(P_1, M),$$

donde las flechas de los extremos son las inducidas por ε. Se sigue que

$$H^q(Hom_G(\mathcal{L}, M)) = \widehat{H}^q(G, M),$$

para $q = 0, 1$. □

4.2. Restricción y Correstricción

Si $H \subseteq G$ es un subgrupo del grupo (finito) G y M es un G-módulo, tomando las definiciones de los morfismos de restricción para cohomología para definir los morfismos de reestricción en la cohomología de Tate:

$$Res \ : \ \widehat{H}^q(G, M) \to \widehat{H}^q(H, M)$$

para $q \geq 1$. Como estos morfismos conmutan con los morfismos de conexión δ, entonces por traslación de dimensión los tenemos definidos en cohomología de Tate para toda $q \in \mathbb{Z}$.
Recordemos que para $q = 0$ el morfismo de reestricción es la inclusión

$$M^G \hookrightarrow M^H;$$

y como $N_G M \subseteq N_H M$, pasando al cociente obtenemos el morfismo de restricción

$$Res \ : \ \widehat{H}^0(G, M) = M^G / N_G M \to M^H / N^H M = \widehat{H}^0(H, M).$$

Para $\widehat{H}^{-q}$ y $q \geq 2$ se tiene que $\widehat{H}^{-q} = H_{q-1}$ y el morfismo Res es el correspondiente en homología.

Para $q = -1$, como $\widehat{H}^{-1} = H_0$, se verifica que el morfismo de restricción de homología en dimensión cero:

$$Res_0 \ : \ H_0(G, M) = M_G \to M_H = H_0(H, M),$$

inducido por el morfismo $N'_{G/H} \ : \ M_G \to M_H$ dado por

$$N'_{G/H}(x) := \sum_{\sigma \in \sigma H \in G/H} \sigma^{-1} x,$$

se restringe para definir

$$Res \ : \ \widehat{H}_0(G, M) =_{N_G} M/I_G M \to_{N_H} M/I_H M = \widehat{H}_0(H, M).$$

Similarmente se define el morfismo de correstricción

$$Cor \ : \ \widehat{H}^q(H, M) \to \widehat{H}^q(G, M),$$

que en dimensión 0 es inducido por el paso al cociente del morfismo

$$N_{G/H} \ : \ M^H \to M^G,$$

dado por $x \mapsto \sum_{\sigma \in \sigma H \in G/H} \sigma x$.
Similarmente, para $q = -1$, como $\widehat{H}^{-1} = H_0$, el morfismo de correstricción

$$Cor \ : \ \widehat{H}^{-1}(H, M) = H_0(H, M) \to \widehat{H}^{-1}(G, M) = H_0(G, M)$$

está inducido por la inclusión $M_H \hookrightarrow M_G$.

Proposición 4.2.1. *(1) Los morfismos de restricción forman un morfismo de funtores de cohomología i.e., conmutan las cofronteras.*

(2) Similarmente, los morfismos de corestricción forman un morfismo de funtores de cohomología.

Demostración. (1): Sea $0 \to A \xrightarrow{\phi} B \xrightarrow{\psi} C \to 0$ una sucesión exacta de G-módulos. Probraremos que los diagramas siguientes conmutan:

$$\begin{array}{ccc} \widehat{H}^q(G, C) & \xrightarrow{\delta} & \widehat{H}^{q+1}(G, A) \\ {\scriptstyle Res}\downarrow & & \downarrow{\scriptstyle Res} \\ \widehat{H}^q(H, C) & \xrightarrow{\delta} & \widehat{H}^{q+1}(H, A) \end{array}$$

Para $q \geq 0$ esto se sigue de la definición de Res de grupos de cohomología.
Para $q \leq -2$ se sigue de la definición de Res de grupos de homología.
En el caso restante, $q = -1$, debemos probar que el diagrama siguiente conmuta:

$$\begin{array}{ccc} \widehat{H}_0(G,C) & \xrightarrow{\delta} & \widehat{H}^0(G,A) \\ {\scriptstyle Res}\downarrow & & \downarrow{\scriptstyle Res} \\ \widehat{H}_0(H,C) & \xrightarrow{\delta} & \widehat{H}^0(H,A) \end{array}$$

donde $\widehat{H}^{-1}(G,C) = \widehat{H}_0(G,C) =_{N_G} C/I_GC,^0 (G,A) = A^G/N_GA$, etc.
Esto se prueba explícitamente: sea $c \in_{N_G} C$ un representante de la clase $\tau \in_{N_G} C/I_GC = \widehat{H}^0(G,C)$ de tal forma que $N_G(c) = 0$. Levantamos c a un elemento $b \in B$ y consideremos a $N_G(b) \in B$. Obsérvese que $\Psi(N_G(b)) = 0$ (porque $N_G(c) = 0$ y así $N_G(b) \in Ker(\psi) = Im(\phi)$, es decir, existe un único $a \in A$ tal que $\phi(a) = N_G(b)$. Se puede demostrar que a es G-invariante, y así $a \in A^G \subseteq A^H$. Más aún, la clase de a módulo N_GA es $\delta(\bar{c})$ y por lo tanto la clase de a módulo N_HA es $Res \circ \delta(\bar{c})$.
Por otra parte, $Res(\bar{c})$ es la clase módulo I_HC de $N'_{G/H}(c) \in C_H$ y como arriba este elemento se puede levantar a un $N'_{G/H}(b)$ el cual a su vez proviene de $a \in A^G$ de tal forma que $\delta \circ Res(\bar{c})$ está representado por la clase de a módulo N_HA, como se quería probar.
La parte (2) se demuestra similarmente. □

Teorema 4.2.1. *Sea $H \subseteq G$ un subgrupo de índice finito $n = [G : H]$. Entonces, para todo G-módulo M y para toda $q \in \mathbb{Z}$, la composición $Cor \circ Res$ es multiplicación por $n = [G : H]$ en $\widehat{H}^q(G,M)$, i.e., el diagrama siguiente conmuta para toda $q \in \mathbb{Z}$:*

$$\begin{array}{ccc} \widehat{H}^q(G,M) & \xrightarrow{\quad n \quad} & \widehat{H}^q(G,M) \\ & {\scriptstyle Res}\searrow \quad \nearrow{\scriptstyle Cor} & \\ & \widehat{H}^q(H,M) & \end{array}$$

Demostración. Se sigue de las proposiciones correspondientes para cohomología y homología y de las definiciones correspondientes para $q = 0$ y $q = -1$. □

Corolario 4.2.2. *Si G es un grupo finito de orden n, entonces*

$$n \cdot \widehat{H}^q(G,M) = 0$$

para todo $q \in \mathbb{Z}$ y todo G-módulo M.

Corolario 4.2.3. *Si M es un G-módulo el cual es finitamente generado como grupo abeliano, entonces los $\widehat{H}^q(G, M)$ son grupos finitos.*

Demostración. La definición de los grupos $\widehat{H}^q(G, M)$ en términos de cadenas y cocadenas, y como M es finitamente generado, muestra que estos grupos son finitamente generados también y por el corolario anterior son de torsión; se sigue que deben ser finitos. □

Corolario 4.2.4. *Sean G un grupo finito, p un entero primo, G_p un p-subgrupo de Sylow de G y M un G-módulo. Entonces, para todo entero $n \in \mathbb{Z}$ el morfismo*

$$Res \ : \ \widehat{H}^n(G, M) \to \widehat{H}^n(G_p, M)$$

es inyectivo en la componente p-primaria de $\widehat{H}^n(G, M)$.

Corolario 4.2.5. *Sean G un grupo finito, M un G-módulo y $n \in \mathbb{Z}$. Si $x \in \widehat{H}^n(G, M)$ es tal que para todo primo p se tiene que $Res(x) = 0$ en $\widehat{H}^n(G_p, M)$, donde G_p es el correspondiente p-subgrupo de Sylow de G, entonces $x = 0$.*
Se sigue que, si para todo primo p se tiene que $\widehat{H}^n(G_p, M) = 0$, donde G_p es el correspondiente p-subgrupo de Sylow de G, entonces $\widehat{H}^n(G, M) = 0$.

Corolario 4.2.6. *Sea G un grupo finito, M un G-módulo y $m, q \in \mathbb{Z}$ tales que $m \geq 0$, $q > 0$. Supongamos que:*

(1) $H^i(H, M) = 0$ para todo $0 < i < q$ y todos los subgrupos $H \subseteq G$.

(2) Si $H' \subseteq H \subseteq G$ son subgrupos tales que H' es normal en H y H/H' es cíclico de orden primo, entonces el orden de $\widehat{H}^q(H/H', M^H)$ divide a $[H \ : \ H']^m$.

Entonces, el orden de $\widehat{H}^q(G, M)$ divide a $|G|^m$.

4.3. Productos en cohomología

Consideremos G-módulos (izquierdos) M, N y sea $M \otimes_{\mathbb{Z}} N$ su producto tensorial; $M \otimes_{\mathbb{Z}} N$ se vuelve un G-módulo definiendo la acción de G mediante:

$$\sigma \cdot (a \otimes b) := \sigma \cdot a \otimes \sigma \cdot b$$

y extendiendo linealmente.

Teorema 4.3.1. *Si G es un grupo finito, existe una y solo una familia de homomorfismos (llamados productos):*

$$\widehat{H}^m(G,M) \otimes_{\mathbb{Z}} \widehat{H}^n(G,N) \to \widehat{H}^{m+n}(G, M \otimes_{\mathbb{Z}} N),$$

denotados por $a \otimes b \mapsto a \cdot b$, definidos para todos los pares de enteros (m,n) y todos los G-módulos M, N, tales que estos productos satisfacen las cuatro propiedades siguientes:

(1) Estos productos son funtoriales en M y N.

(2) Para $m = 0 = n$, el producto $a \cdot b$ se obtiene mediante el paso al cociente del morfismo narutal:

$$M^G \otimes N^G \to (M \otimes N)^G.$$

(3) Si $0 \to M' \to M \to M'' \to 0$ es una sucesión exacta de G-módulos y N es tal que la sucesión

$$0 \to M' \otimes_{\mathbb{Z}} N \to M \otimes_{\mathbb{Z}} N \to M'' \otimes_{\mathbb{Z}} N \to 0$$

también es exacta, entonces para todo $x'' \in \widehat{H}^m(G, M'')$ y para todo $y \in \widehat{H}^n(G,N)$ se tiene que:

$$(\delta x'') \cdot y = \delta(x'' \cdot y),$$

donde ambos lados de esta igualdad se ven en $\widehat{H}^{m+n+1}(G, M' \otimes_{\mathbb{Z}} N)$.

(4) Si $0 \to N' \to N \to N'' \to 0$ es una sucesión exacta de G-módulos y M es tal que la sucesión

$$0 \to M \otimes_{\mathbb{Z}} N' \to M \otimes_{\mathbb{Z}} N \to M \otimes_{\mathbb{Z}} N'' \to 0$$

también es exacta, entonces para todo $x \in \widehat{H}^m(G,M)$ y para todo $y'' \in \widehat{H}^n(G,N'')$ se tiene que:

$$x \cdot \delta(y'') = (-1)^m \delta(x \cdot y''),$$

donde ambos lados de esta igualdad se ven en $\widehat{H}^{m+n+1}(G, M \otimes_{\mathbb{Z}} N')$.

Las propiedades siguientes del producto que hemos definido se prueban utilizando traslación de dimensión:

Proposición 4.3.1. *Se tiene las siguientes fórmulas:*

(1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *módulo la identificación* $(A \otimes B) \otimes C \simeq A \otimes (B \otimes C)$.

(2) $a \cdot b = (-1)^{dim(a) \cdot dim(b)} b \cdot a$ *módulo* $A \otimes B \simeq B \otimes A$.

(3) $Res(a \cdot b) = Res(a) \cdot Res(b)$.

(4) $Cor(a \cdot Res(b)) = Cor(a) \cdot b$.

(5) $Inf(a \cdot b) = Inf(a) \cdot Inf(b)$.

Algunas veces tendremos oportunidad de usar productos de un tipo un poco más general; consideremos G-módulos A, B, C y un G-morfismo $\phi \ : \ A \otimes B \to C$. Si componemos el producto que hemos definido anteriormente con el morfismo inducido $\phi^* \ : \ \widehat{H}^*(G, A \otimes B) \to \widehat{H}^*(G, C)$, obtenemos la aplicación

$$\widehat{H}^m(G, A) \otimes \widehat{H}^n(G, B) \to \widehat{H}^{m+n}(G, C);$$

$$a \otimes b \mapsto \phi^*(a \cdot b),$$

a lo que llamamos el producto de a con b relativo a ϕ.

4.4. Cohomología de grupos cíclicos finitos

Para calcular la cohomología de Tate de un grupo cíclico finito usaremos la siguietne resolución G-libre de $\mathbb{Z}$:

Proposición 4.4.1. *Sea G un grupo cíclico finito de orden n con generador $\sigma \in G$. Consideremos los siguientes dos elementos en el anillo de grupo $\mathbb{Z}G$:*

$$D := \sigma - 1 \quad y \quad N_G := 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1},$$

y pongamos $L_j = \mathbb{Z}G$ para toda j.
Entonces, la sucesión siguiente es una resolución G-libre completa de G:

$$\cdots \xrightarrow{N} L_{2n} \xrightarrow{D} L_{2n-1} \xrightarrow{N_G} L_{2n-2} \xrightarrow{D} L_{2n-3} \xrightarrow{N_G} \cdots \tag{4.4}$$

donde D y N_G denotan multiplicaciones por D y N_G respectivamente.

Demostración. Observémos que como G es abeliano entonces el anillo $\mathbb{Z}G$ es conmutativo y por lo tanto la multiplicación por elementos de $\mathbb{Z}G$ es un G-morfismo. La sucesión (4) es un complejo ya que:

(1) $D \circ N_G = DN_G = (\sigma - 1)(1 + \sigma + \cdots + \sigma^{n-1}) = 0$ ya que $\sigma^n = 1$.

(2) $N_G \circ D = N_G D = 0$ similarmente.

(3) $Ker(D) \subseteq Im(N_G)$: en efecto, sea

$$u = \sum_{i=0}^{n-1} m_i \sigma^i \in Ker(D)$$

Entonces,

$$\begin{aligned} 0 = Du = (\sigma - 1)(\sum m_i \sigma^i) &= \sum_{i=0}^{n-1} m_i \sigma^{i+1} - \sum_{i=0}^{n-1} m_i \sigma^i \\ &= m_0\sigma^1 + m_1\sigma^2 + \cdots + m_{n-1}\sigma^n - m_0\sigma^0 - m_1\sigma^1 - \cdots - m_{n-1}\sigma^{n-1} \\ &= (m_0 - m_1)\sigma + \cdots + (m_{n-2} - m_{n-1})\sigma^{n-1} + (m_{n-1} - m_0)\sigma^0. \end{aligned}$$

(ya que $\sigma^n = \sigma^0 = 1$). Se sigue que $m_0 = m_1 = \cdots = m_{n-1}$, y por lo tanto

$$u = \sum_{i=0}^{n-1} m_i \sigma^i = \sum_{i=0}^{n-1} m_0 \sigma^i = m_0 \sum_{i=0}^{n-1} \sigma^i = m_0 N_G \in Im(N_G).$$

(4) Similarmente se prueba que $Ker(N_G) \subseteq Im(D)$.

□

Como consecuencia de esta proposición tenemos que los grupos $\widehat{H}^n(G, M)$ dependen solo de la paridad de n:

Corolario 4.4.1. *Sea G un grupo cíclico finito de orden n y sea M un G-módulo. Pongamos ${}_{N_G}M := \{x \in M \ : \ N_G x = 0\}$. Entonces*

$$\widehat{H}^q(G, M) = \begin{cases} {}_{N_G}M/DM & \textit{si } q \equiv 1 \textit{mód } (2) \\ M^G/N_G M & \textit{si } q \equiv 0 \textit{mód } (2) \end{cases} \tag{4.5}$$

Aquí DM y $N_G M$ son las imágenes de las multiplicaciones por D y N_G respectivamente.

Demostración. Apliquemos el funtor $Hom_G(\ , M)$ a la resolución (4) de la proposición anterior para obtener:

$$\cdots \xrightarrow{N_G^*} Hom_G(\mathbb{Z}G, M) \xrightarrow{D^*} Hom_G(\mathbb{Z}G, M) \xrightarrow{N_G^*} Hom_G(\mathbb{Z}G, M) \xrightarrow{D^*} \cdots,$$

y recordemos que como G es abeliano entonces $\mathbb{Z}G$ es conmutativo y así N_G^* y D^* también son multiplicativos por N_G y D respectivamente.
Ahora, en la resolución (4), el morfismo D tiene dominio un L_i con índice par y N_G tiene dominio un L_i con índice impar, entonces N_G^* tiene dominio par y D^* tiene dominio impar. Así:

(1) Si $q = 2m + 1$, entonces

$$\widehat{H}^{2m+1}(G, M) = Ker(N_G^*)/Im(D^*),$$

pero $Ker(N_G^*) =_{N_G} M$ e $Im(D^*) = DM$, y por lo tanto

$$\widehat{H}^{2m+1}(G, M) =_{N_G} M/DM.$$

(2) Si $q = 2m$, entonces

$$\widehat{H}^{2m}(G, M) = Ker(D^*)/Im(N_G^*), \tag{4.6}$$

donde

$$\begin{aligned} Ker(D^*) &= \{x \in M \ : \ Dx = 0\} \\ &= \{x \in M \ : \ (\sigma - 1)x = 0\} \quad \text{ya que } D = \sigma - 1 \\ &= \{x \in M \ : \ \sigma x = x\} \\ &= \{x \in M \ : \ \sigma^i x = x\} \\ &= M^G, \end{aligned}$$

(la penúltima igualdad por iteración ya que $\sigma x = x$ implica $\sigma^2 x = \sigma x = x$, etc.) Se sigue que

$$\widehat{H}^{2m}(G, M) = M^G/N_G M.$$

□

Observación. Los isomorfismos del corolario anterior dependen de la elección del generador σ de G ya que los operadores D y N_G dependen de este σ.

Corolario 4.4.2. *Si G es un grupo cíclico finito de orden n y M es un G-módulo trivial, entonces*

$$\widehat{H}^q(G, M) = \begin{cases} {}_N M & \textit{si } q \equiv 1 \textit{mód } (2) \\ M/nM & \textit{si } q \equiv 0 \textit{mód } (2) \end{cases}$$

Ejemplo. Si G es cíclico finito de orden n y $M = \mathbb{Z}$ como G-módulo trivial, entonces

$$\widehat{H}^q(G, \mathbb{Z}) = \begin{cases} 0 & \text{si } q \equiv 1 \text{mód } (2) \\ \mathbb{Z}/n\mathbb{Z} & \text{si } q \equiv 0 \text{mód } (2) \end{cases}$$

lo único que necesita observarse es que ${}_n\mathbb{Z} = \{x \in \mathbb{Z} \ : \ nx = 0\} = \{0\}$.

Proposición 4.4.2. *Sea G un grupo cíclico finito de orden n que actúa trivialmente en $\mathbb{Z}$. Sea θ un generador de $H^2(G,\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}$. Entonces, multiplicación por θ induce un isomorfismo*

$$\widehat{H}^q(G,M) \xrightarrow{\simeq} \widehat{H}^{q+2}(G,M)$$

para todo $q \in \mathbb{Z}$ y todo G-módulo M.

Demostración. Las sucesiones largas de cohomología asociadas a las sucesiones exactas cortas de G-módulos:

$$0 \to I_G \hookrightarrow \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \to 0 \tag{4.1}$$

y

$$0 \to \mathbb{Z} \xrightarrow{N_G} \mathbb{Z}G \xrightarrow{D} I_G \to 0 \tag{4.2}$$

dan lugar a isomorfismos

$$\widehat{H}^0(G,\mathbb{Z}) \xrightarrow{\delta}{\simeq} H^1(G,I_G) \xrightarrow{\delta}{\simeq} H^2(G,\mathbb{Z}).$$

Y como las sucesiones (1) y (2) se escinden como $\mathbb{Z}$-módulos, entonces permanecen exactas cuando se tensoran con M:

$$0 \to I_G \otimes_{\mathbb{Z}} M \hookrightarrow \mathbb{Z}G \otimes_{\mathbb{Z}} M \to \mathbb{Z} \otimes_{\mathbb{Z}} M \simeq M \to 0, \tag{4.3}$$

$$0 \to \mathbb{Z} \otimes_{\mathbb{Z}} M \simeq M \to \mathbb{Z}G \otimes_{\mathbb{Z}} M \to I_G \otimes_{4t\mathbb{Z}} M \to 0 \tag{4.4}$$

y estas dos últimas sucesiones exactas cortas dan lugar a isomorfismos (ya que $\mathbb{Z}G \otimes_{\mathbb{Z}} M$ es inducido y por lo tanto cohomológicamente trivial):

$$\widehat{H}(G,M) \xrightarrow{\delta}{\simeq} H^1(G, I_G \otimes_{\mathbb{Z}} M) \xrightarrow{\delta}{\simeq} H^2(G,M).$$

Así, lo que debemos probar es que el producto por un generador de $\widehat{H}^0(G,\mathbb{Z})$ induce un automorfismo de $\widehat{H}^q(G,M)$.
Por traslación de dimensión se reduce nuevamente al caso $q = 0$. Y como $\widehat{H}^0(G,\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}$, un generador θ de $\widehat{H}^0(G,\mathbb{Z})$ está representado por un entero t coprimo con n y el producto por θ es multiplicación por t. Ahora, como $mcd(t,n) = 1$ entonces existe un entero s tal que $ts \equiv 1\ m\acute{o}d(n)$ y como por (4,2,2) el entero n anula a $\widehat{H}^0(G,M)$ y $ts = 1 + rn$ entonces multiplicación por t es un automorfismo de $\widehat{H}^0(G,M)$. □

4.5. El cociente de Hebrand

Sea G un grupo cíclico finito y M un G-módulo. Para $q = 0, 1$ denotemos con $h_q(M)$ el orden del grupo $\widehat{H}^q(G, M)$ siempre que éste sea un grupo finito. Si ambos grupos son finitos, se define el cociente de Herbrand:

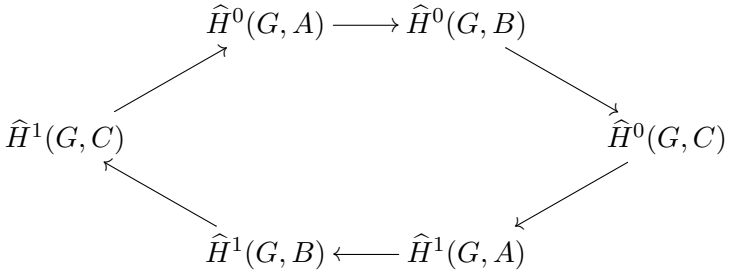
$$h(M) := h_0(M)/h_1(M).$$

Dada la periodicidad $mod(2)$ de la cohomología de Tate de un grupo cíclico finito, el cociente de Herbrand es el análogo a una característica de Euler-Poincaré.

Proposición 4.5.1. *Sea G un grupo cíclico finito y sea $0 \to A \to B \to C \to 0$ una sucesión exacta de G-módulos. Si dos de los tres cocientes de Herbrand $h(A), h(B), h(C)$ están definidos, entonces el tercero también está definido y se tiene que:*

$$h(B) = h(A)h(C).$$

Demostración. Debido a la periodicidad de los $\widehat{H}^q$, la sucesión larga de cohomología puede verse como un hexágono exacto:



Supongamos ahora que $h(A)$ y $h(B)$ están definidos, i.e., que $\widehat{H}^0(G, A), \widehat{H}^1(G, A)$ y $\widehat{H}^0(G, B), \widehat{H}^1(G, B)$ son finitos. Sean M_1 la imagen de $\widehat{H}^0(G, A)$ en $\widehat{H}^0(G, B)$, M_2 la imagen de $\widehat{H}^0(G, B)$ en $\widehat{H}^0(G, C)$ y así sucesivamente en el hexágono en sentido contrario a las manecillas del reloj. Entonces, la sucesión

$$0 \to M_2 \to \widehat{H}^0(G, C) \to M_3 \to 0$$

es exacta, donde los grupos M_2 Y M_3 son finitos ya que M_2 es imagen de $\widehat{H}^0(G, B)$ y M_3 es subgrupo de $\widehat{H}^1(G, A)$. Se sigue que $\widehat{H}^0(G, C)$ es finito; y similarmente $\widehat{H}^1(G, C)$ es finito también.
Finalmente, los órdenes de los grupos $\widehat{H}^0(G, A), \ldots, \widehat{H}^1(G, C)$ son respectivamente $m_6m_1, m_1m_2, \ldots, m_5m_6$, donde m_i es orden de M_i. Por ejemplo, para $\widehat{H}^0(G, A)$, del hexágono anterior se tiene la sucesión exacta corta

$$0 \to M_6 \to \widehat{H}^0(G, A) \to M_1 \to 0$$

de donde se sigue que $h_0(A) = m_6 m_1$. Similarmente para los otros órdenes. Con esto se llega a que:

$$\begin{aligned} h(A)h(C) = \frac{h_0(A)}{h_1(A)}\frac{h_0(B)}{h_1(B)} &= \frac{m_6 m_1}{m_3 m_4}\frac{m_2 m_3}{m_5 m_6} \\ &= \frac{m_1 m_2}{m_4 m_5} \\ &= \frac{h_0(B)}{h_1(B)} \\ &= h(B). \end{aligned}$$

□

Proposición 4.5.2. *Sea G un grupo cíclico finito. Si A es G-módulo finito, entonces $h(A) = 1$.*

Demostración. Se tienen sucesiones exactas

$$0 \to A^G \to A \xrightarrow{D} A \to A_G \to 0.$$

y

$$0 \to \widehat{H}^1(G, A) \to A_G \xrightarrow{N_G^*} A^G \to \widehat{H}^0(G, A) \to 0.$$

La primera sucesión muestra que A^G y A_G tienen el mismo orden, y por lo tanto la segunda implica que $\widehat{H}^0(G, A)$ y $\widehat{H}^1(G, A)$ tienen el mismo orden $h_0(A) = h_1(A)$. □

En las demostraciones anteriores hemos usado el hecho de que en una sucesión exacta de grupos finitos, con extremos los grupos triviales, se tiene que el producto de los órdenes de los grupos involucrados, con exponentes $+1$ ó -1 alternados es igual a 1. Esto se prueba descomponiendo la sucesión exacta dada en sucesiones exactas cortas.

Corolario 4.5.1. *Sea G un grupo cíclico finito y consideremos G-módulos A, B y $f : A \to B$ un G-morfismo con núcleo y conúcleo finitos. Entonces, si $h(A)$ ó $h(B)$ está definido, el otro también lo está y de hecho son iguales.*

Demostración. Supongamos que $h(A)$ está definido. De la sucesión exacta

$$0 \to Ker(f) \to A \to f(A) \to 0$$

donde $h(A)$ está definido y $h(Ker(f)) = 1$ se sigue de la proposición (4,5,1) que $h(f(A))$ está definido y además

$$h(A) = h(f(A)) \cdot 1.$$

Similarmente, de la sucesión exacta

$$0 \to f(A) \to B \to Coker(f) \to 0$$

donde ahora $h(f(A))$ está definido y $h(Coker(f(A))) = 1$ se sigue que $h(B)$ está definido y además

$$h(B) = h(f(A)) \cdot 1 = h(A).$$

□

4.6. Trivialidad cohomológica

Un G-módulo M se llama cohomológicamente trivial si para todo subgrupo $H \subseteq G$ se tiene que $\widehat{H}^q(H, M) = 0$ para todo $q \in \mathbb{Z}$. Por (4,1,4) los módulos relativamente proyectivos o relativamente inyectivos son cohomológicamente triviales. Los resultados de esta sección se deben a T. Nakayama con simplificaciones en las demostraciones de D. Rim.

4.6.1. Cohomología de p-grupos

Lemma 4.6.1. *Sea p un entero primo, G un p-grupo y M un G-módulo tal que $pM = 0$. Entonces, las condiciones siguientes son equivalentes:*

(1) $M = 0$*;*

(2) $H^0(G, M) = 0$*;*

(3) $H_0(G, M) = 0$.

Demostración. Claramente (1) implica (2) y (3).

(2) $\Rightarrow$ (1): Supongamos que $M \neq 0$ y sea $0 \neq x \in M$. Entonces, el submódulo $X \subseteq M$ generado por x es finito de orden una potencia de p (ya que $px = 0$ por hipótesis, y así X es finitamente generado y de torsión, y por lo tanto finito). Consideremos las G-órbitas de los elementos de X; estas órbitas tienen orden una potencia de p (ya que el orden de G es una potencia de p), y existe al menos un punto fijo, el 0; así la órbita del 0 (que consta solo del 0) tiene orden 1; así, si escribimos

$$X = \bigcup_{y \in X} orb(y)$$

entonces

$$p^t = |X| = \sum_{y\in X} |orb(y)| = \sum_{0\neq y\in X} |orb(y)| + |orb(0)| = \sum_{0\neq y\in X} |orb(y)| + 1,$$

y como cada $|orb(y)|$ es una potencia de p, para que la igualdad anterior sea cierta se necesita que existan al menos otros $p-1$ puntos fijos además del 0, y por lo tanto existen al menos p puntos fijos de tal forma que $H^0(G,M) = M^G \neq 0$. $(3) \Rightarrow (1)$: Sea $M' := Hom_{\mathcal{F}_p}(M, \mathcal{F}_p) = Hom_{\mathbb{Z}}(M, \mathcal{F}_p)$ el dual de M considerado como espacio vectorial sobre $\mathcal{F}_p$ (ya que $pM = 0$). Entonces,

$$H^0(G, M') = (M')^G = (Hom_{\mathbb{Z}}(M, \mathcal{F}_p))^G = Hom(M, \mathcal{F}_p)$$

es el dual de H_0 ya que $H_0(G,M) = \mathbb{Z} \otimes_G M$ y así

$$\begin{aligned} Hom_{\mathcal{F}_p}(H_0(G,M), \mathcal{F}_p) &= Hom_{\mathbb{Z}}(\mathbb{Z} \otimes_G M, \mathcal{F}_p) = Hom_{\mathbb{Z}G}(M, Hom_{\mathbb{Z}}, \mathcal{F}_p)) \\ &\simeq Hom_{\mathbb{Z}G}(M, \mathcal{F}_p), \end{aligned}$$

el cual es 0 por hipótesis. Se sigue que $H^0(G, M') = 0$, y como $(2) \Rightarrow (1)$ entonces $M' = 0$ y por lo tanto $M = 0$.

□

Lemma 4.6.2. *Sea p un entero primo, G un p-grupo y M un G-módulo tal que $pM = 0$. Supongamos además que $H_1(G,M) = 0$. Entonces, M es un módulo libre sobre $\mathcal{F}_p[G] = \mathbb{Z}G/p\mathbb{Z}G$.*

Demostración. Como $pM = 0$ entonces $p \cdot H_0(G,M) = p \cdot M/I_G M = 0$ y por lo tanto $H_0(G,M)$ es un espacio vectorial sobre $\mathcal{F}_p$. Sea e_λ una base de este espacio y levantamos cada e_λ a $a_\lambda \in M$. Mostraremos que a_λ genera a M. En efecto, sea M' el submódulo de M generado por los a_λ y consideremos el cociente $M'' := M/M'$. Asociada a la sucesión exacta $0 \to M' \to M \to M'' \to 0$ se tiene la sucesión

$$H_0(G, M') \xrightarrow{f} H_0(G, M) \to H_0(G, M'') \to 0$$

en la cual el morfismo f es un isomorfismo por construcción. Se sigue que $H_0(G, M'') = 0$ y así, por el lema anterior, $M'' = 0$, i.e., $M' = M$. Entonces, como los a_λ generan a M se tiene un G-epimorfismo $\phi : L \to M$, donde L es un $\mathcal{F}_p[G]$-módulo libre; por construcción, ϕ induce un isomorfismo

$$\Phi : L/I_G L = H_0(G, L) \xrightarrow{\simeq} M/I_G M = H_0(G, M).$$

Sea $R := Ker(\phi)$ y consideremos la sucesión exacta $0 \to R \to L \xrightarrow{\phi} M \to 0$ y la sucesión asociada

$$0 = H_1(G, M) \to H_0(G, R) \to H_0(G, L) \xrightarrow{\Phi} H_0(G, M) \to 0,$$

donde por hipótesis $H_1(G, M) = 0$; y como Φ es un isomorfismo, se sigue que $H_0(G, R) = 0$ y por lo tanto $R = 0$ por el lema anterior, i.e., ϕ es un isomorfismo. □

Teorema 4.6.3. *Sea p un entero primo, G un p-grupo y M un G-módulo tal que $pM = 0$. Entonces, las condiciones siguientes son equivalente:*

(1) M es un $\mathcal{F}_p[G]$-módulo libre;

(2) M es un G-módulo inducido;

(3) M es cohomológicamente trivial;

(4) $\widehat{H}^q(G, M) = 0$ para algún entero q.

Teorema 4.6.4. *Sea G un p-grupo y M un G-módulo sin p-torsión. Entonces las condiciones siguientes son equivalentes:*

(1) M es cohomológicamente trivial.

(2) $\widehat{H}^q(G, N) = \widehat{H}^{q+1}(G, M) = 0$ para algún entero q.

(3) M/pM es un $\mathcal{F}_p[G]$-módulo libre.

Demostración.

$(1) \Rightarrow (2)$: Se sigue de la definición de cohomológicamente trivial.

$(2) \Rightarrow (3)$: Como M no tiene p-torsión, entonces existe una sucesión exacta:

$$0 \to M \xrightarrow{P} M \to M/pM \to 0$$

que induce la sucesión exacta

$$\widehat{H}^q(G, M) \xrightarrow{P} \widehat{H}^q(G, M) \to \widehat{H}^q(G, MpM) \to \widehat{H}^{q+1}(G, M) \xrightarrow{P} \quad (4.5)$$

$$\xrightarrow{P} \widehat{H}^{q+1}(G, M),$$

y como $\widehat{H}^q(G, M) = \widehat{H}^{q+1}(G, M) = 0$, entonces esta sucesión muestra que $\widehat{H}^q(G, M/pM) = 0$ y por lo tanto, por el teorema anterior, se sigue que M/pM es libre sobre $\mathcal{F}_p[G]$.

$(3) \Rightarrow (1)$: Como M/pM es un $\mathcal{F}_p[G]$-módulo libre y por lo tanto todos los $\widehat{H}^m(G, M/pM) = 0$, la sucesión larga anterior muestra que

$$\widehat{H}^n(G, M) \xrightarrow{P} \widehat{H}^n(G, M)$$

es un isomorfismo para todo n. Pero como G tiene orden una potencia de p, entonces esta potencia de p anula al grupo $\widehat{H}^n(G, M)$, pero como M no tiene p-torsión entonces esto sólo es posible si $\widehat{H}^n(G, M) = 0$ para todo n. El mismo razonamiento se aplica a cualquier subgrupo H de G ya que M/pM es $\mathcal{F}_p[G]$-libre. Se sigue que M es cohomológicamente trivial.

□

Corolario 4.6.5. *Sean G un p-grupo y M un G-módulo el cual es libre como grupo abeliano y que satisface las condiciones equivalentes del teorema anterior. Entonces, para todo G-módulo N libre de p-torsión, el G-módulo $X := Hom_{\mathbb{Z}}(M, N)$ es cohomológicamente trivial.*

4.6.2. Cohomología de grupos finitos

Teorema 4.6.6. *Sean G un grupo finito, M un G-módulo que es $\mathbb{Z}$-libre y G_p un p-subgrupo de Sylow de G. Las condiciones siguientes son equivalentes:*

(1) Para todo primo p el G_p-módulo M satisface las condiciones equivalentes del teorema (4,6,4).

(2) M es un G-módulo proyectivo.

Demostración.

$(2) \Rightarrow (1)$: Se da por las condiciones del teorema (4,6,4).

$(1) \Rightarrow (2)$: Pongamos a M como el cociente de un G-módulo libre L y consideremos la sucesión excta resultante:

$$0 \to N \to L \to M \to 0.$$

Como M es $\mathbb{Z}$-libre, el funtor $Hom_{\mathbb{Z}}(M, \ )$ es exacto y por lo tanto la sucesión exacta anterior da lugar a una sucesión exacta.

$$0 \to Hom_{\mathbb{Z}}(M, N) \to Hom_{\mathbb{Z}}(M, L) \to Hom_{\mathbb{Z}}(M, M) \to 0.$$

Como $N \subseteq L$ y L es libre, entonces N es libre de torsión y así por el corolario anterior $Hom_{\mathbb{Z}}(M, N)$ es cohomológicamente trivial como G_p-módulo, para

cada p, y por lo tanto $H^1(G, Hom_{\mathbb{Z}}(M,N)) = 0$ por el corolario (4,2,5). Observemos ahora que

$$H^0(G, Hom_{\mathbb{Z}}(M,N)) = (Hom_{\mathbb{Z}}(M,N))^G = Hom_G(M,N),$$

y lo mismo par los otros grupos de la sucesión anterior, entonces dicha sucesión nos dice que

$$Hom_G(M,L) \to Hom_G(M,M) \to 0$$

es suprayectivo y por lo tanto el morfismo identidad de M se extiende a un G-morfismo $M \to L$ y por lo tanto la sucesión $0 \to N \to L \to M \to 0$ se escinde, i.e., M es factor directo del módulo libre L, i.e., M es proyectivo. □

Teorema 4.6.7. *Sean G un grupo finito y M un G-módulo. Las condiciones siguientes son equivalentes:*

(1) Para todo primo p, $\widehat{H}^q(G_p, M) = 0$ para dos valores consecutivos de q (que pueden depender del primo p).

(2) M es cohomológicamente trivial.

(3) Existe una sucesión exacta $0 \to P_1 \to P_0 \to M \to 0$ en el cual los P_i son G-proyectivos. (Es decir, la dimensión proyectiva de M es ≤ 1).

Demostración.

$(3) \Rightarrow (2)$: Como los proyectivos son cohomológicamente triviales, la sucesión larga de cohomología asociada a la sucesión corta dada muestra que M es cohomológicamente trivial.

$(2) \Rightarrow (1)$:Es trivial.

$(1) \Rightarrow (3)$:Escojamos una sucesión exacta de G-módulos

$$0 \to P \to P_0 \to M \to 0$$

con P_0 libre como $\mathbb{Z}G$-módulo libre (en particular P_0 también es libre como $\mathbb{Z}$-módulo y consecuentemente P es $\mathbb{Z}$-libre también); se sigue que

$$\widehat{H}^q(G_p, P) \simeq \widehat{H}^{q-1}(G_p, M)$$

para todo q y todo primo p, y por lo tanto $\widehat{H}^q(G_p, P) = 0$ para dos valores consecutivos de q por (1). Se sigue que P satisface la hipótesis (1) del teorema

(4,6,6) anterior, en particular la hipótesis (2) del teorema (4,6,4), y por lo tanto es proyectivo.

□

La siguiente demostración se basa en Onishi [1], utilizando los teoremas demostrados anteriormente.

Proposición 4.6.1. *Sea G un grupo finito y A un G-módulo. Si para algún entero k y para algún entero impar positivo d, $H^k(H,A)$ y $H^{k+d}(H,A)$ son triviales para todos los subgrupos H de G, entonces $H^r(H,A)$ es trivial para toda $r \in \mathbb{Z}$ y para todos los subgrupos $H \subseteq G$.*

Demostración. Por inducción sobre el orden $n = |G|$. El teorema es trivial para $n = 1$. Supongamos $n > 1$ y asumamos que el teorema se cumple para todos los grupos de orden $< n$. En particular, podemos asumir que $H^r(H,A) = 0$ para cada dimensión r y para cada subgrupo propio H de G. Si n no es potencia de un número primo, entonces todos los subgrupos de Sylow de G son subgrupos propios y utilizando el teorema anterior queda demostrada la trivialidad.
Supongamos que n es una potencia de un número primo, por lo tanto G es soluble. Sea H un subgrupo propio normal de G tal que el grupo cociente G/H es cíclico. Como $H^r(H,A) = 0$ para cada r, tenemos la sucesión exacta fundamental de Hochschild-Serre:

$$0 \to H^r(G/H, A^H) \to H^r(G,A) \to H^r(H,A)$$

para cada $r > 0$. Como el último término es trivial, entonecs $H^r(G/H, A^H) \cong H^r(G,A)$ para cada $r > 0$. Por cambio de dimensión, pudimos haber asumido que $k > 0$. Entonces tenemos que $H^k(G/A, A^H) = H^{k+d}(G/H, A^H) = 0$. Como G/H es cíclico y d es impar, tenemos que $H^r(G/H, A^H) = 0$ para cada r, y por el isomorfismo entonces tenemos que $H^r(G,A) = 0$ para cada $r > 0$. De la misma manera se llega a que $H^r(G,A) = 0$ para cada $r \leq 0$. □

4.7. El teorema de Tate

El teorema de Tate es el ingrediente principal para demostrar el teorema principal de la teoría de campos de clases. Las demostraciones son de Tate y Nakayama continuando las ideas anteriores.

Teorema 4.7.1. *Sean G un grupo finito, B, C dos G-módulos y $f : B \to C$ un G-morfismo. Para cada primo p sea G_p un p-subgrupo de Sylow de G y supongamos*

que existe un entero n_p tal que el morfismo

$$f_q^* \ : \ \widehat{H}^q(G_p, B) \to \widehat{H}^q(G_p, C)$$

es suprayectivo para $q = n_p$, biyectivo para $q = n+1$, e inyectivo para $q = n_p+2$. Entonces, para cualquier subgrupo $H \subseteq G$ y cualquier entero q, el morfismo

$$f_q^* \ : \ \widehat{H}^q(H, B) \to \widehat{H}^q(H, C)$$

es un isomorfismo.

Demostración. Sea $Q := Hom_{\mathbb{Z}}(\mathbb{Z}G, B)$ el coinducido tal que $i : B \hookrightarrow Q$, $i(x)(\sigma) := \sigma \cdot x$. Entonces $(f, i) : B \to C \otimes Q$ es inyectivo y por lo tanto se tiene una sucesión exacta corta:

$$0 \to B \to C \otimes Q \to R \to 0, \tag{4.1}$$

donde R es el cociente correspondiente. Ahora, como Q es cohomológicamente trivial, la cohomología de $C \otimes Q$ es la misma que la de C. Entonces, la sucesión larga de cohomología asociada a la sucesión corta anterior.

$$\widehat{H}^q(G_p, B) \to \widehat{H}^q(G_p, C) \to \widehat{H}^q(G_p, R) \to \widehat{H}^{q+1}(G_p, B) \to \widehat{H}^{q+1}(G_p, C)$$

y las hipótesis del teorema implican que $\widehat{H}^q(G_p, R) = 0$ para $q = n_p$ y $q = n_p + 1$. Se sigue del teorema anterior que R es cohomológicamente trivial y así el teorema se sigue de la sucesión larga de cohomología asociada a (1). □

Teorema 4.7.2. *Sean G un grupo finito, A, B, C tres G-módulos y $\phi : A \otimes B \to C$ un G-morfismo. Sea q un entero fijo y $a \in \widehat{H}^q(G, A)$ dado. Supongamos que para cada primo p existe un entero n_p tal que el morfismo*

$$\widehat{H}^n(G_p, B) \to \widehat{H}^{n+q}(G_p, C)$$

inducido por el producto (relativo a ϕ) con $Res_{G/G_p}(a)$ es suprayectivo para $n = n_p$, biyectivo para $n = n_p + 1$ e inyectivo para $q = n_p + 2$. Entonces, para todos los subgrupos $H \subseteq G$ y todos los enteros n, el producto (relativo a ϕ) con $Res_{G/H}(a)$ induce un morfismo

$$\widehat{H}^n(H, B) \to \widehat{H}^{n+q}(H, C).$$

(Recordemos que el producto de x con y relativo a ϕ está dado por $\phi^*(x \cdot y)$).

Teorema 4.7.3. *Sean G un grupo finito, A un G-módulo, $a \in H^2(G, A)$. Para cada primo p sea G_p un p-subgrupo de Sylow de G y supongamos que:*

(1) $H^1(G_p, A) = 0$.

(2) $H^2(G_p, A)$ *está generado por* $Res_{G/G_p}(a)$ *y tiene orden igual al de* G_p.

Entonces, para todos los subgrupos $H \subseteq G$ *y todos los enteros* n*, el producto con* $Res_{G/H}(a)$ *induce un isomorfismo*

$$\widehat{H}^n(H, \mathbb{Z}) \to \widehat{H}^{n+2}(H, A).$$

Demostración. Pongamos $B = \mathbb{Z}, C = A, q = 2y n_p = -1$ en el teorema anterior.

(i): Para $n = -1$, la suprayectividad de

$$\widehat{H}^{-1}(G_p, \mathbb{Z}) \to \widehat{H}^1(G_p, A) \tag{4.2}$$

se sigue de la hipótesis (1) del teorema.

(ii): Para $n = 0$, el grupo $\widehat{H}^0(G_p, \mathbb{Z})$ es cíclico de orden igual al orden de G_p ya que $\widehat{H}^0(G_p, \mathbb{Z}) \simeq \mathbb{Z}^{G_p}/N_{G_p}\mathbb{Z} \simeq \mathbb{Z}/|G_p|\mathbb{Z}$ (porque G_p actúa trivialmente en $\mathbb{Z}$), y por lo tanto la biyectividad de

$$\widehat{H}^0(G_p, \mathbb{Z}) \to \widehat{H}^2(G_p, A)$$

se sigue de la hipótesis (2).

(iii): Para $n = 1$, la inyectividad de

$$\widehat{H}^1(G_p, \mathbb{Z}) \to \widehat{H}^3(G_p, A)$$

se sigue del hecho de que $\widehat{H}^1(G_p, \mathbb{Z}) = Hom(G_p, \mathbb{Z}) = 0$.

Con esto se verifican todas las hipótesis del teorema anterior, y el resultado se sigue. □

Capítulo 5

Cohomología de Galois

5.1. Cohomología de Galois

Teorema 5.1.1. *Si G es el grupo de Galois de una extensión finita de Galois K/k, entonces*

$$\widehat{H}(G,K)=0 \qquad \textit{para toda } q\in\mathbb{Z}.$$

Demostración. Por el teorema de la base normal existe un $w \in K$ tal que si $G=\{\sigma_1,\ldots,\sigma_n\}$, entonces $\sigma_1(w),\ldots,\sigma_n(w)$ es una base de K sobre k, i.e.,

$$K \simeq \bigoplus_{j=1}^{n} \sigma_j(w)\cdot k$$

y así K es G-inducido, y como G es finito, entonces por (4,0,1) K es G-coinducido también y por lo tanto sus grupos de cohomología de Tate se anulan (4,1,4) □

Para el grupo multiplicativo K^* los grupos de cohomología $H^q(G,K^*)$ en general no son cero para $q\geq 2$, pero para $q=1$ tenemos el siguiente resultado:

Teorema 5.1.2. ***(Teorema 90 de Hilbert).*** *Si G es el grupo de Galois de una extensión finita de Galois K/k, entonces $H^1(G,K^*)=0$.*

Demostración. Mostraremos que todo 1-cociclo $f : G\to K^*$ es una 1-cofrontera. En efecto, si $c\in K$ formamos la suma

$$b:=\sum_{\sigma\in G} f(\sigma)\cdot\sigma(c)\in K,$$

y observemos que como G es finito, la suma es finita también; y como los automorfismos σ son linealmente independientes (Dedekind), entonces existe un $c \in K$ tal que la suma es diferente de cero.. Pero entonces, para toda $\tau \in G$:

$$\begin{aligned} 0 \neq \tau(b) &= \tau\left(\sum_{\sigma\in G} f(\sigma)\cdot\sigma(c)\right) \\ &= \sum_{\sigma\in G} \tau(f(\sigma))\cdot\tau\sigma(c) \\ &= \sum_{\sigma\in G} f(\tau)^{-1}f(\tau\sigma)\cdot\tau\sigma(c) \quad \text{ya que } f \text{ es morfismo cruzado} \\ &= f(\tau)^{-1}\cdot\sum_{\sigma\in G} f(\tau\sigma)(\tau\sigma)(c) \\ &= f(\tau)^{-1}\cdot b, \end{aligned}$$

ya que $\tau\sigma$ recorre G cuando σ lo hace, y por definición de b.
Se sigue que $0 \neq \tau(b) = f(\tau)^{-}1\cdot b$, i.e., para toda $\tau \in G$:

$$f(\tau) = \tau(b)^{-1}\cdot b = \tau(b^{-1})\cdot(b^{-1})^{-1},$$

lo que muestra que f es una 1-cofrontera con $x = b^{-1} \in G$. □

5.2. Grupos profinitos

Definición 5.2.1. *Un grupo profinito es un grupo topológico G que es Hausdorff, compacto y tiene una base de vecindades abiertas de la identidad $1 \in G$ consistente de subgrupos normales.*

Observación. Necesitaremos usar más adelante algunas propiedades de grupos topológicos en general: sean G un grupo topológico y H la intersección de todas las vecindades del elemento neutro 1 de G. Entonces:

(i) H es un subgrupo de G.

(ii) H es la cerradura $\overline{\{1\}}$ de $\{1\}$.

(iii) G/H es Hausdorff.

(iv) G es Hausdorff si y sólo si $H = 1$.

A continuación veremos que la definición anterior de grupos profinitos es equivalente a la definición vista en el capitulo 1:

Teorema 5.2.2. *(1) Si G es un grupo profinito y N recorre la familia de subgrupos normales abiertos de G, entonces*

$$G \simeq \varprojlim G/N,$$

(isomorfismo y homeomorfismo).

(2) Recíprocamente, si $(G_\alpha, \phi_\beta^\alpha)$ es un sistema inverso de grupos finitos, con la topología discreta, entonces

$$G = \varprojlim_N G_\alpha$$

es un grupo profinito.

Corolario 5.2.3. *Sea G un grupo profinito. Si H es un subgrupo cerrado de G, entonces*

$$H \simeq \varprojlim H/H \cap N_i,$$

donde los N_i recorren la familia de subgrupos normales abiertos de G.

Corolario 5.2.4. *Sea G un grupo profinito. Si H es un subgrupo cerrado de G, entonces*

$$G/H \simeq \varprojlim G/N_i H,$$

donde N_i recorren la familia de subgrupos normales abiertos de G.

Los dos corolarios anteriores nos dicen que, si G es un grupo profinito, entonces los subgrupos cerrados de G también son profinitos y los cocientes de G también son profinitos.

Teorema 5.2.5. *Sean G un grupo profinito, N un subgrupo normal cerrado de G y $\rho : G \to G/N$ el epimorfismo canónico. Entonces, existe una función continua $s : G/N \to G$ (que, en general, no es un homomorfismo) tal que $\rho \circ s = id$, i.e., $\rho(s(x)) = x$ para todo $x \in G/N$. A la función s se le llama una sección de ρ.*

5.3. Cohomología de grupos profinitos

Definición 5.3.1. *M es un G-módulo discreto si M es un G-módulo (tomando en cuenta que G tiene una topología) tal que la acción de G en M es continua (con la topología discreta).*

Lemma 5.3.2. *Sea G un grupo profinito y M un G-módulo. Las afirmaciones siguientes son equivalentes:*

(1) M es un G-módulo discreto, i.e., la acción

$$G \times M \to M \qquad (\sigma, x) \mapsto \sigma x,$$

es continua. (Aquí M se considera con la topología discreta).

(2) $M = \bigcup_U M^U$, donde U recorre la familia de subgrupos abiertos de G.

Demostración. La continuidad de $G \times M \to M$ es equivalente a la propiedad de que para cada par $(\sigma, x) \in G \times M$ existe un abierto U de G tal que la vecindad abierta $\sigma U \times \{x\}$ de (σ, x) va a dar al conjunto abierto $\{\sigma x\}$ de M; pero esto significa precisamente que $x \in M^U$. □

Observemos que si G es un grupo profinito y $\mathcal{N} = \{U_i \ : \ i \in I\}$ es la familia de todos los subgrupos normales abiertos de G, la familia $\mathcal{N}$ está ordenada mediante: $i \leq j$ si $U_i \supset U_j$, de tal forma que $(I, \leq)$ es un conjunto dirigido y además tenemos las proyecciones canónicas

$$f_{ij} \ : \ G/U_j \to G/U_i$$

siempre que $i \leq j$. Se tiene entonces el sistema inverso $\{G/U_i, f_{ij}\}$ de grupos finitos. Entonces por el teorema (5,2,2)

$$G \simeq \varprojlim G/U_i,$$

y si M es un G-módulo discreto, entonces

$$M = \bigcup_{U_i} M^{U_i} \simeq \varprojlim M^{U^i},$$

donde el último isomorfismo es el natural.

Fijemos ahora un entero $q \geq 0$. Entonces, para cada $i \leq j$ las proyecciones canónicas $f_{ij} \ : \ G/U_j \to G_{U_i}$ inducen los morfismos de inflación:

$$Inf_i^j \ : \ H^q(G/U_i, M^{U_i}) \to H^q(G/U_j, M^{U_j}),$$

de tal forma que se tiene un sistema directo de grupos abelianos:

$$\{H^q(G/U_i, M^{U_i}) \ ; \ Inf_i^j \ ; \ i, j \in I\}.$$

Definición 5.3.3. *Con la notación anterior, el grupo*

$$H^q(G, M) := \varinjlim H^q(G/U_i, M^{U_i})$$

se llama el q-ésimo grupo de cohomología de G en M.

Teorema 5.3.4. *Sean G un grupo profinito, H un subgrupo cerrado normal en G y M un G-módulo discreto tal que $H^1(H, M) = 0$. Entonces, se tiene la sucesión exacta inflación-restricción:*

$$0 \to H^2(G/H, M^H) \xrightarrow{Inf} H^2(G, M) \xrightarrow{Res} H^2(H, M).$$

Demostración. Obsérvese que por (5,2,3),

$$H \simeq \varprojlim H/H \cap N_i \simeq \varprojlim HN_i/N_i,$$

y por lo tanto la hipótesis $H^1(H, M) = 0$ es equivalente a la condición

$$H^1(HN_i(N_i, M^{N_i}) = 0$$

para todos los subgrupos normales abiertos N_i de G. Ahora, como

$$(G/N_i)/(HN_i/N_i) \simeq G/HN_i$$

y $H^1(HN_i/N_i, M^{N_i}) = 0$ para toda i, entonces se tienen las sucesiones inflación-restricción usuales

$$0 \to H^2(G/N_iH, M^{N_iH}) \xrightarrow{Inf} H^2(G/N_i, M^{N_i}) \xrightarrow{Res} H^2(HN_i/N_i, M^{N_i}),$$

y para $i \leq j$ los morfismos Inf_i^j hacen conmutar el diagrama correspondiente, para $i \leq j$:

$$\begin{array}{ccccc}
0 \longrightarrow H^2(G/N_iH, M^{N_iH}) & \xrightarrow{Inf} & H^2(G/N_i, M^{N_i}) & \xrightarrow{Res} & H^2(HN_i/N_i, M^{N_i}) \\
\downarrow{\scriptstyle Inf_i^j} & & \downarrow{\scriptstyle Inf_i^j} & & \downarrow{\scriptstyle Inf_i^j} \\
0 \longrightarrow H^2(G/N_jH, M^{N_jH}) & \xrightarrow[Inf]{} & H^2(G/N_j, M^{N_j}) & \xrightarrow[Res]{} & H^2(HN_j/N_j, M^{N_i}),
\end{array}$$

y por lo tanto podemos pasar al límite directo en cada columna obteniendo la sucesión exactaa siguiente (la cual es exacta porque el funtor $\varinjlim$ es exacto):

$$0 \to \varinjlim H^2(G/N_iH, M^{N_iH}) \xrightarrow{Inf} \varinjlim H^2(G/N_i, M^{N_i}) \xrightarrow{Res} \varinjlim H^2(HN_i/N_i, M^{N_i}).$$

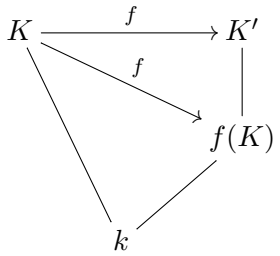
Finalmente observamos que:

$$\begin{aligned}
\varinjlim H^2(G/N_iH, M^{N_iH}) &\simeq H^2(G/H, M^H) && \text{por (5,2,4)}, \\
\varinjlim H^2(G/N_i, M^{N_i}) &\simeq H^2(G, M) && \text{por (5,2,2)}, \\
\varinjlim H^2(HN_i/N_i, M^{N_i}) &\simeq H^2(H, M) && \text{por (5,2,3)},
\end{aligned}$$

□

5.4. El grupo de Brauer

Sea k un campo y consideremos dos extensiones de Galois K/k y K'/k con grupos de Galois $G = Gal(K/k)$ y $G' = Gal(K'/k)$ respectivamente. Si $f : K \to K'$ es un k-monomorfismo, entonces la imagen $f(K) \subseteq K'$ es un campo intermedio de K'/k que es k-isoomorfo a K. En el diagrama siguiente:



las extensiones $f(K)/k$ y $K'/f(K)$ son de Galois, y si $H = Gal(K'/f(K))$ entonces, como las extensiones K/k y $f(K)/k$ son k-isomorfas, se tiene que

$$G = Gal(K/k) \simeq Gal(f(K)/k).$$

Definimos entonces

$$\tilde{f} : G' := Gal(K'/k) \to Gal(K/k) = G$$

mediante:

$$\sigma \mapsto \tilde{f}(\sigma) := \sigma|_{f(K)},$$

Se tiene entonces que el morfismo $\tilde{f} : G' \to G$ es compatible con el morfismo $f : K^* \to K'^*$, de tal forma que induce homomorfismos:

$$f_q : H^q(Gal(K/k), K^*) \to H^q(Gal(K'/k), K'^*),$$

y se tiene el siguiente resultado:

Proposición 5.4.1. *Los morfismos*

$$f_q : H^q(Gal(K/k), K^*) \to H^q(Gal(K'/k), K'^*)$$

son independientes de la elección del k-monomorfismo $f : K \to K'$.

Demostración. Dos k-monomorfismos $f, f' : K \to K'$ difieren sólo por una conjugación, i.e., existe $\tau \in Gal(K/k)$ tal que $f' = \tau f \tau^{-1}$. El resultado se sigue de (3,2,1). □

Corolario 5.4.1. *Sea k un campo y sean $k^s, k'(s)$ dos cerraduras separables de k. Entonces, existe un isomorfismo canónico*

$$H^q(Gal(k^s/k), k^{s*}) \to H^q(Gal(k'^s/k), k'^{s*}).$$

Así, en este caso, no importa cuál cerradura separable se use. Tiene sentido usar la notación siguiente:

$$H^q(k) := H^q(Gal(k^s/k), k^{s*}).$$

Definición 5.4.2. *Si k es un campo, el grupo de Brauer de k es el grupo*

$$Br(k) := H^2(Gal(k^s/k), k^{s*}) = \varinjlim H^2(Gal(K/k), K^*),$$

donde K/k recorre la familia de subextensiones finitas de Galois K/k de k^s/k.

Observemos ahora que si se tiene una torre de extensiones $L \supseteq K \supseteq k$, con L/K y K/k de Galois, entonces, por teoría de Galois se tiene que

$$Gal(K/k) \simeq Gal(L/k)/Gal(L/K) =: G/H.$$

Ahora, si $M = L^*$ (como módulo de Galois), entonces

$$M^H = M^{Gal(L/K)} = (L^*)^{Gal(L/K)} = K^*.$$

Y como $H^1(H, K) = H^1(Gal(L/K), K^*) = 0$ entonces se tiene la sucesión inflación-restricción asociada:

Teorema 5.4.3. *Si se tiene una torre de extensiones $L \supseteq K \supseteq k$, con L/K y K/k de Galois, entonces se tiene la sucesión exacta:*

$$0 \to H^2(Gal(K/k), K^*) \xrightarrow{Inf} H^2(Gal(L/k), L^*) \xrightarrow{Res} H^2(Gal(L/K), L^*).$$

Demostración. Observamos sólo que: $G = Gal((L/k),\ H = Gal(L/K)$ y $G/H \simeq Gal(K/k)$. □

Corolario 5.4.4. *Si K/k es de Galois, entonces se tiene una sucesión exacta:*

$$0 \to H^2(Gal(K/k), K^*) \xrightarrow{Inf} Br(k) \xrightarrow{Res} Br(K).$$

Demostración. Sea k^s cualquier cerradura separable de k que contiene a K; entonces también es una cerradura separable de K. □

Corolario 5.4.5. *Si k es un campo y $\{K_i, k\}$ es la familia de todas las extensiones finitas de Galois de k contenidas en una cerradura separable de k^s de k, entonces*

$$Br(k) = H^2(k) = \bigcup_i H^2(Gal(K_i/k, K_i^*).$$

Demostración. El corolario anterior nos dice que el limite directo

$$Br(k) := H^2(Gal(k^s/k), k^{s*}) \simeq \varinjlim H^2(Gal(K/k), K^*)$$

es una unión. □

Teorema 5.4.6. *Sea k un campo. Las condiciones siguientes son equivalentes:*

(1) El grupo de Brauer de cualquier extensión finita separable K de k es cero.

(2) Si K/k es finita separable y L/K es finita de Galois, entonces el $Gal(L/K)$-módulo L^* es cohomológicamente trivial.

(3) Si K/k es finita separable y L/K es finita de Galois, entonces el morfismo de norma

$$N_{L/K} \ : \ L^* \to K^*$$

es suprayectivo.

Demostración.

$(2) \Rightarrow (3)$: Como

$$1 = \widehat{H}^0(Gal(L/K), L^*) = (L^*)^{Gal(L/K)}/N_{L/K}L^* = K^*/N_{L/K}L^*,$$

entonces $K^* = N_{L/K}L^*$.

$(2) \Rightarrow (1)$: Por hipótesis cada $H^2(Gal(L/K), L^*) = 0$; así,

$$Br(K) = \varinjlim H^2(Gal(L/K), L^*) = 0.$$

$(1) \Rightarrow (2)$: Sea $H \subseteq G = Gal(L/K)$ cualquier subgrupo; entonces $H = Gal(L/K')$ para un campo intermedio $K \subseteq K' \subseteq L$. Ahora, como por hipótesis $Br(K) = 0$ entonces en particular $H^2(H, L^*) = 0$; y como $H^1(H, L^*) = 0$ por el teorema 90 de Hilbert, entonces se cumplen las hipótesis del teorema (4,6,7) para $q = 1, 2$. Se sigue que L^* es cohomológicamente trivial.

$(3) \Rightarrow (2)$: La hipótesis es $\widehat{H}^0(G, L^*) = 0$ y el teorema 90 de Hilbert dice que $\widehat{H}^1(G, L^*) = 0$. Por el teorema (4,6,7) se sigue que L^* es cohomológicamente trivial.

□

Ejemplo. El grupo de Brauer del campo de los reales $\mathbb{R}$ es:

$$Br(\mathbb{F}) = H^2(Gal(\mathbb{C}/\mathbb{R}, \mathbb{C}^*),$$

donde el grupo de Galois $G = Gal(\mathbb{C}/\mathbb{R})$ es cíclico de orden 2 generado por la conjugación. Así, por (4,4,1):

$$Br(\mathbb{R}) = H^2(Gal(\mathbb{C}/\mathbb{R}, \mathbb{C}^*) = (\mathbb{C}^*)^G/N\mathbb{C}^* = \mathbb{R}^*/\mathbb{R}^*_{>0} = \mathbb{Z}/2\mathbb{Z}.$$

Ejemplo. El grupo cociente $\mathbb{Q}/\mathbb{Z}$ es un grupo de Brauer. Más aún, es el grupo de Brauer de un campo K completo bajo una valuación discreta y con campo residual finito.

Bibliografía

[1] Onishi, H. (1967). On cohomological triviality. *Proceedings of the American Mathematical Society*, 18(6):1117–1118.

[2] Rotman, J. J. (2008). *An introduction to homological algebra*. Springer Science & Business Media.

[3] Szamuely, T. (2009). *Galois groups and fundamental groups*, volume 117. Cambridge University Press.

[4] Weibel, C. A. (1995). *An introduction to homological algebra*. Number 38. Cambridge university press.

[5] Zaldivar, F. (2001). *Cohomología de Galois de campos locales*, volume 17. Sociedad Matemática Mexicana.

[6] Zaldívar, F. (2006). *Teoría de Galois*, volume 3. Anthropos Editorial.