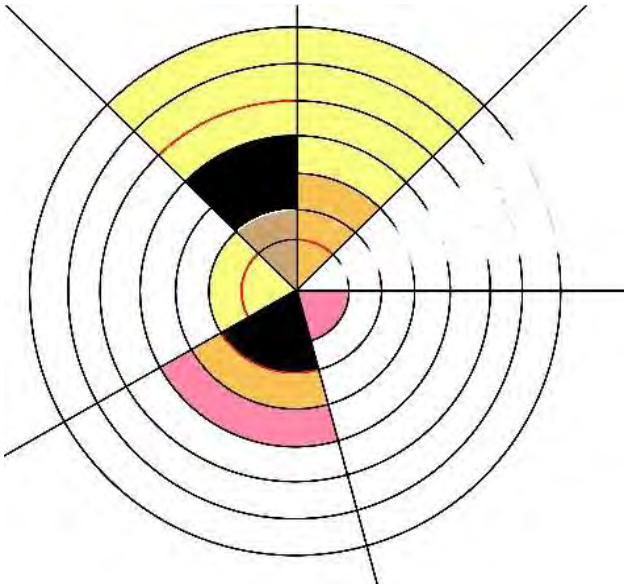
Universidad Nacional Autónoma de México

Posgrado en Ciencias Matemáticas

Facultad de Ciencias

Número de extensiones y el orden del multiplicador de Schur de los grupos Metacíclicos



TESIS

que para obtener el grado académico de

Maestro en Ciencias Matemáticas

presenta

Quitzeh Morales Meléndez

Director de Tesis: **Dr. Rolando Jiménez Benítez**

México, D.F. **Agosto, 2006**

Agradecimientos

Primeramente, quiero agradecer a mi asesor, Rolando Jiménez Benítez, por darme un problema que pude resolver y con el que me he divertido tanto. Con topólogos intentando hacer álgebra, la intuición geométrica produce imágenes peculiares.

Claro que quiero agracecer también a aquellos que escucharon pacientemente mis problemas y trataron de ayudarme, y lo hicieron, aunque tal vez no se hayan dado cuenta. Una palabra clave de Jacob Mostovoy. Una mente que vuela como pocas, la de Alberto Verjovski: a todo concepto matemático, asígnale una noción geométrica.

Acerca de los medios didácticos, Jose Luis Cisneros ha ido generando un lenguaje que, espero, en el futuro hará de la matemática una ciencia mucho más fluida hacia otras actividades humanas.

Al único que realmente ha leido a detalle la tesis, Rafael Villaroel.

A todos los que han atendido a mis elucubraciones. Casi todos[1] en el imate de Cuernavaca: Haydee, Bety, Aubin, Jawad, Adolfo; ojalá no se me haya olvidado alguien, si es así, no se ofenda.

A Natalia,
a quien más que dedicar la exposición debo agradecerla,
la tesis es sólo álgebra
y a ninguno de los dos nos gusta demasiado;
a ella menos que a mí
Quitzeh

[1] todos menos una, pero ella tiene sus líneas aparte

Índice general

Introducción

El estudio de las extensiones de grupos está íntimamente ligado al problema de clasificación de los grupos finitos. Este problema comenzó a estudiarse desde finales del siglo diecinueve y se sabía era extremadamente difícil, de ahí la importancia de desarrollar herramientas generales para estudiar estos grupos.

La existencia de una teoría de cohomología para grupos fue sugerida en 1936 por el trabajo de Hurewics acerca de espacios "aesféricos" [1] Sin embargo, incluso cuando del trabajo de Hurewics es inmediata una construcción algebraica del primer grupo de homología, para que esta herramienta resultase atractiva para algebristas, era necesario relacionarla con herramientas conocidas para ellos. Tal es el caso del multiplicador introducido por Schur en relación con representaciones proyectivas de grupos a inicios del siglo pasado, y encontrado en el trabajo de Hopf en 1942 como el segundo grupo de homología .

Posteriormente, la construcción de los espacios de Eilengerg–Mac Lane dio origen al concepto de homología y cohomología de grupos como herramienta para entender estructuras algebraicas.

El concepto de extensión fue introducido por Schreier en 1926, de ahí y del estudio de Baer de 1934 Eilenberg–Mac Lane y Eckmann pudieron reconocer los primeros tres grupos de cohomología, separados de los ejemplos topológicos.

Al intentar calcular la cohomología de una extensión de grupos Lyndon llegó la estudio de un tipo de sucesión espectral, un importante concepto en matemáticas que tomó forma hasta 1953, gracias a Serre y Hochschild. [2]

---

[1] Sólo el primer grupo de homotopía es no trivial.

[2] Esta reseña histórica es un extracto de [?] y se restringe a los temas tocados en esta tesis.

Cabe mencionar que la (co)homología de extensiones de grupos ha hallado recientemente aplicaciones en cristalografía, ya que, en dimensiones bajas, esta expresa invariantes de las simetrías de los (cuasi)cristales [?].

Este trabajo tiene como finalidad, en el caso de una extensión de un grupo cíclico por otro, es decir, de un grupo metacíclico, relacionar el multiplicador de Schur, un invariante del grupo, con el número de extensiónes salvo equivalencia. Ambos se calculan mediante técnicas de cohomología de grupos, aunque los cálculos en sí son accesibles a un nivel muy básico.

El siguiente trabajo está puede ser leido por matemáticos con una formación básica en el área de álgebra; es decir, los cursos de teoría de grupos, de anillos y campos y de números, que se imparten a nivel licenciatura, conviene estar familiarizado con las nociones de producto tensorial de módulos y módulos de homomorfismos, aunque no resulta estrictamente necesario.

Resumen

A todo grupo G se le puede poner en correspondencia un anillo con unitario, llamado el *anillo de grupo* y al cual denotamos $\mathbb{Z}G$, construido de la siguiente manera.

$$\mathbb{Z}G = \{\sum_{g\in G} a(g)g \,|a(g) \in \mathbb{Z},\ a(g) = 0\ \forall g \in G \text{ salvo un número finito.}\}.$$

Es decir, $\mathbb{Z}G$ es el grupo libre abeliano generado por los elementos de G. Ahora, la multiplicación de G se extiende de manera natural [3] a una multiplicación en $\mathbb{Z}G$ que hace de él un anillo cuyo unitario es el elemento neutro $1 \in G$.

Por ejemplo, el grupo trivial $G = 1$ claramente tiene $\mathbb{Z}$ como anillo de grupo y la multiplicación resulta la multiplicación usual de enteros.

Asimismo, todo homomorfismo de grupos $f : G \to G'$ se extiende a un homomorfismo de anillos $\mathbb{Z}G \to \mathbb{Z}G'$. De esta manera, el único homomorfismo $G \to 1$ nos da un homomorfismo canónico $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$, llamado de *aumentación*, que se caracteríza por

$$\varepsilon(\sum_{g\in G} a(g)g) = \sum_{g\in G} a(g).$$

[3] Por linealidad, considerando al grupo abeliano como $\mathbb{Z}$-módulo.

Sea R un anillo cualquiera. Una *sucesión* de R-módulos (si $R = \mathbb{Z}G$, escribimos G-módulo), es una expresión C de la forma

$$\cdots \to C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \to \cdots$$

($n \in \mathbb{Z}$) en que las flechas representan homomorfismos y los C_n son R-módulos. Una sucesión es llamada *complejo de cadenas* (o complejo, por brevedad) cuando la composición de cualesquiera homomorfismos consecutivos es cero ($\partial^2 = 0$), en este caso tiene sentido definir la *homología* del complejo $H_n = Z_n/B_n$, donde $Z_n = \ker \partial_n$, $B_n = \operatorname{Im} \partial_{n+1}$. El complejo se dice *acíclico* (o la sucesión es *exacta*) cuando $H_n = 0$ para cada $n \in \mathbb{Z}$; es decir, la imágen de cada homomorfismo es igual al núcleo del siguiente.

Una *resolución* de un R-módulo M es una sucesión exacta

$$\cdots \to F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} M \to 0.$$

Si cada F_i es libre, la resolución F se dice *libre*.

Ahora notemos que podemos considerar a $\mathbb{Z}$ como G-módulo poniendo $g \cdot 1 = 1$ para todo $g \in G$ (aquí 1 denota el generador de $\mathbb{Z}$). Haciendo así, una resolución de $\mathbb{Z}$ sobre $\mathbb{Z}G$ es una resolución de $\mathbb{Z}$ visto como G-módulo.

Sea F una resolución libre de $\mathbb{Z}$ sobre $\mathbb{Z}G$. Sea M un G-módulo, entonces $F \otimes_G M$ denota el complejo

$$\cdots \to F_{n+1} \otimes_G M \xrightarrow{\partial_{n+1}\otimes 1} F_n \otimes_G M \xrightarrow{\partial_n \otimes 1} F_{n-1} \otimes_G M \to \cdots$$

($f \otimes 1(x \otimes m) = f(x) \otimes m$) y $\operatorname{Hom}_G(F, M)$ denota el complejo

$$\cdots \to \operatorname{Hom}_G(F_{n-1}, M) \xrightarrow{\delta_{n-1}} \operatorname{Hom}_G(F_n, M) \xrightarrow{\delta_n} \operatorname{Hom}_G(F_{n+1}, M) \to \cdots$$

($\delta_n u(x) = (-1)^{n+1} u(\partial_{n+1} x)$). Definimos *homología y cohomología del grupo* G *con coeficientes en el* G*-módulo* M como la homología de estos complejos, respectivamente.

Una sucesión exacta *corta* es una de la forma

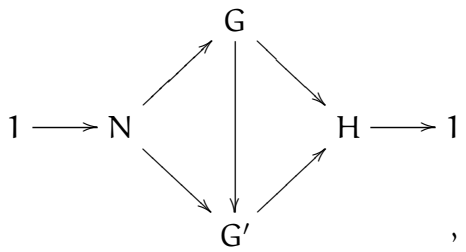
$$1 \to N \to G \to H \to 1,$$

donde 1 en este caso denota el neutro del los grupos (sería cero si los grupos fueran abelianos y se escribiesen en notación aditiva, como es el caso de los módulos). En el caso de grupos, una sucesión exacta corta es también llamada una *extensión* de N por H. [?]

Otra extensión

$$1 \to N \to G' \to H \to 1,$$

es equivalente si hay un homomorfismo $G \to G'$ que hace conmutar el diagrama



,

este es necesariamente un isomorfismo. [4]

Nosotros estamos interesados en extensiones de la forma

$$0 \to \mathbb{Z}/m \to G \to \mathbb{Z}/n \to 0,$$

donde $\mathbb{Z}/m$ es el grupo de enteros módulo m [5]. En este caso el grupo G es llamado *metacíclico*. De acuerdo a [?], debido a que el término $\mathbb{Z}/m$ de la sucesión es abeliano, este puede ser considerado como un $\mathbb{Z}/n$-módulo y, entonces, el orden de $H^2(\mathbb{Z}/n, \mathbb{Z}/m)$ es el número de clases equivalencia de este tipo de extensiones, fijando m, n y la acción de $\mathbb{Z}/n$ sobre $\mathbb{Z}/m$ [6].

El objetivo de este trabajo es calcular $H^2(\mathbb{Z}/n, \mathbb{Z}/m)$ tomando la acción como parámetro y relacionar su orden con el de $H_2(G, \mathbb{Z}) = H_2G$ utilizando los resultados hallados en [?] acerca de grupos metacícli cos.

[4] Examinando el subdiagrama de la izquierda vemos que debe ser uno a uno y, con el de la derecha, que debe ser sobre.

[5] Equivalentemente, el grupo cíclico de orden m

[6] Es decir, fijando la estructura de $\mathbb{Z}/n$-módulo sobre $\mathbb{Z}/m$.

CAPíTULO 1

Preliminares

1. Complejos de cadenas

A continuación parafraseo y traduzco fragmentos del capítulo cero de [?], complementando con las pruebas de los resultados que se enuncian.

Sea R un anillo arbitrario. Un R-módulo graduado es una sucesión $C = (C_n)_{n\in\mathbb{Z}}$ de R-módulos. Si $x \in C_n$, decimos que x tiene grado n y escribimos $\deg x = n$. Un morfismo $f : C \to C'$ de grado p del R-módulo graduado C al R-módulo graduado C' es una sucesión $f = (f_n : C_n \to C_{n+p})_{n\in\mathbb{Z}}$ de homomorfismos de módulos, entonces $\deg f(x) = \deg f + \deg x$. Los morfismos de módulos graduados se componen de la manera obvia.

Un complejo de cadenas sobre R es un par (C, d) donde C es un R-módulo graduado y d es un endomorfismo de C (i.e. $d : C \to C$), de grado -1 tal que $d^2 = 0$. El morfismo d es llamado diferencial u operador frontera del complejo C. Dado un complejo de cadenas C (obviando la diferencial), definimos los ciclos $Z(C) = \ker d = (\ker d_n)_{n\in\mathbb{Z}}$, las fronteras $B(C) = \operatorname{Im} d = (\operatorname{Im} d_{n+1})_{n\in\mathbb{Z}}$ y la homología $H(C) = Z(C)/B(C)$, ya que $d^2 = 0$ implica $B(C) \subset Z(C)$. Todos estos son módulos graduados. Normalmente, los complejos de cadenas se denotan así:

$$\cdots \to C_{n+1} \overset{d_{n+1}}{\to} C_n \overset{d_n}{\to} C_{n-1} \to \cdots,$$

cuando no cause confusión, se omiten las diferenciales y, en caso de que el complejo sea no negativo ($C_n = 0,\ n < 0$), denotamos

$$\cdots \to C_{n+1} \to C_n \to C_{n-1} \to \cdots \to C_0 \to 0.$$

Notemos que cualquier R-módulo M puede considerarse como complejo de cadenas, con M en la posición cero y ceros en las demás posiciones, la diferencial es necesariamente cero.

Similarmente, un complejo de cocadenas es un par (C, d) pero, en este caso, d tiene grado 1 y se escribe

$$0 \to C^0 \to \cdots \to C^{n-1} \to C^n \to C^{n+1} \to \cdots$$

cuando el complejo es no negativo. Para las nociones correspondientes, hablaremos de cociclos, cofronteras y cohomología. Reindexando por $C_n = C^{-n}$ podemos considerar como complejo de cadenas a cualquier complejo de cocadenas, por ello complejos de cadenas y cocadenas son esencialmente el mismo concepto. Es en las aplicaciones donde estos conceptos se dividen.

Un morfismo de cadenas $f : C \to C'$ es un morfismo de grado 0 para el cual $fd = d'f$ (d y d' son las diferenciales respectivas).

Una homotopía de un morfismo de cadenas f a otro g, es un morfismo $h : C \to C'$ de grado 1, tal que $d'h + hd = f - g$. Es claro que un morfismo de cadenas es homotópico a sí mismo vía la homotopía cero [1] y que $-h$ es una homotopía de g a f; además si k es una homotopía de g a un tercer morfismo u, entonces $f - u = f - g + g - u = d'(h+k)+(h+k)d$. Por esta razón, decimos que f y g son homotópicas y escribimos $f \simeq g$.

PROPOSICIÓN 1. *Un morfismo de cadenas* $f : C \to C'$ *induce un morfismo* $H(f) : H(C) \to H(C')$ *y* $H(f) = H(g)$*, si* $f \simeq g$.

DEMOSTRACIÓN. Sean $e, c \in C$ y supongamos que $dc = 0$, entonces $d'(fc) = f(dc) = 0$ por lo que $f(\ker d) \subset \ker d'$; por otro lado, si $dc = e$, entonces $fe = f(dc) = d'(fe)$, de donde $f(\operatorname{Im} d) \subset \operatorname{Im} d'$. Significa que hay un morfismo inducido $H(f) : H(C) \to H(C')$.

Ahora, sea h una homotopía de f a g y consideremos $c \in \ker d$. Entonces $(f - g)c = (d'h + hd)c = d'(hc)$, de donde los morfismos inducidos coinciden. □.

Un morfismo de cadenas $f : C \to C'$ se dice equivalencia débil si $H(f)$ resulta ser un isomorfismo; f es equivalencia homotópica si hay otro morfismo $f' : C' \to C$, tal que $f'f \simeq id_C$ y $ff' \simeq id_{C'}$. Es claro que, en tal caso, se induce un isomorfismo en homología. Un complejo de cadenas se dice acíclico cuando $H(C) = 0$ y se dice contraible cuando

[1] Aunque hay que tomar el cero en el lugar correcto para que la homotopía tenga el grado requerido.

$\mathrm{id}_C \simeq 0$, una homotopía de la identidad a cero se llama contracción. Queda claro de nuevo que un complejo contraible es acíclico.

2. Producto Tensorial

En esta sección introduciremos la noción de producto tensorial de complejos de cadenas, iniciando con la noción usual de producto tensorial. En adelante, concentraremos nuestra atención en anillos con unitario, por lo que R denotará siempre uno de este tipo.

Dados M y N grupos abelianos, definimos su *producto tensorial* como

$$M \otimes N = F(M \times N)/A,$$

donde $F(M \times N)$ denota el grupo abeliano libre generado por los elementos del producto cartesiano $M \times N$, y A es el subgrupo de $F(M \times N)$ generado por los elementos de la forma

$$(m, n) + (m', n) - (m + m', n), \qquad m, m' \in M,\ n \in N;$$
$$(m, n) + (m, n') - (m, n + n'), \qquad m \in M,\ n, n' \in N.$$

La imagen de (m, n) bajo la proyección natural se denota usualmente por $m \otimes n$, este es claramente un conjunto de generadores para $M \otimes N$.

El producto tensorial tiene la siguiente propiedad universal: dada cualquier aplicación bilineal [2] $f : M \times N \to L$, existe una única aplicación lineal $h : M \otimes N \to L$ tal que $f(m, n) = h(m \otimes n)$. Para probar esta propiedad, uno define h por la última identidad y luega revisa las condiciones para que esta definición sea buena, de este modo uno encuentra la definición de A.

Sea R un anillo. Ahora supongamos que M y N son R-módulos derecho e izquierdo, respectivamente. Definimos

$$M \otimes_R N = (M \otimes N)/B,$$

con B generado por los elementos de la forma

$$mr \otimes n - m \otimes rn, \qquad m \in M,\ n \in N.$$

Nuevamente, la imagen de los elementos del tipo $m \otimes n$ bajo la proyección natural constituyen un conjunto de generadores y se denotan, por costumbre, de la misma manera. La estructura de R-módulo sobre $M \otimes_R N$ está dada por $r(m \otimes n) = mr \otimes n = m \otimes rn$ (se requiere

[2] Viendo a M y N como $\mathbb{Z}$-módulos.

que M sea módulo derecho para que esta estructura sea asociativa: $ab(m \otimes n) = m(ab) \otimes n = (ma)b \otimes n = ma \otimes bn = a(m \otimes bn) = a(b(m \otimes n))$. La propiedad universal sigue siendo válida sólo cuando L es es un grupo abeliano. En este caso, la R-bilinealidad está expresada por la condición $f(mr, n) = f(m, rn)$. La propiedad universal puede probarse de manera análoga al caso de grupos abelianos.

Una propiedad básica del producto tensorial es el isomorfismo $R \otimes_R M \approx M$, definido a través de la aplicación bilineal $R \times M \to M$; $(r, m) \mapsto rm$ (que induce $r \otimes m \mapsto rm$); la inversa de este es $m \mapsto 1 \otimes m$ (es claro que ambos son homomorfismos, además $r \otimes m \mapsto rm \mapsto 1 \otimes rm = r \otimes m$ y $m \mapsto 1 \otimes m \mapsto m$). Nótese que este isomorfismo es de R-módulos si definimos $r(s \otimes m) = rs \otimes m$

Otra propiedad, obvia pero importante, es el comportamiento bajo sumas directas: de $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$ y $m \otimes 0 = 0$, se sigue el isomorfismo $M \otimes_R (N_1 \oplus N_2) \approx M \otimes_R N_1 \oplus M \otimes_R N_2$.

Consideremos homomorfismos $f : M \to M'$, $g : N \to N'$, de R-módulos derechos e izquierdos, respectivamete. Entonces podemos definir $f \times g : M \times_R N \to M' \otimes_R N'$; $(m, n) \mapsto f(m) \otimes g(n)$ que es evidentemente bilineal; luego, de la propiedad universal obtenemos $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ lineal, tal que $m \otimes n \mapsto f(m) \otimes g(n)$.

En particular, podemos considerar $f \otimes 1 : M \otimes_R N \to M' \otimes_R N$, donde 1 denota la identidad de N. La asociación $f \mapsto f \otimes 1$ tiene la siguientes propiedades *funtoriales*. Si $g : M \to M'$, $f : M' \to M''$, entonces

$$f \otimes 1 \circ g \otimes 1 = (f \circ g) \otimes 1,$$

ya que $f \otimes 1 \circ g \otimes 1(m \otimes n) = f \otimes 1(g(m) \otimes n) = (f(g(m)) \otimes n) = f \circ g \otimes 1(m \otimes n)$, además

$$1 \otimes 1 = 1,$$

que puede ser verificada por el lector directamente. Se tienen propiedade análogas para $1 \otimes g$. Nótese que, si $f \circ g = 0$, entonces $f \circ g \otimes 1 = 0$ ya que $0 \otimes n = 0 \otimes 0n = 0$ $(n \in N)$.

Finalmente, consideremos complejos de cadenas C, C' de R-módulos derechos e izquierdos, respectivamente; definimos su producto tensorial $C \otimes_R C'$ por

$$(C \otimes_R C')_n = \bigoplus_{p+q=n} C_p \otimes_R C'_q$$

la diferencial se define por la fórmula $D(c \otimes c') = dc \otimes c' + (-1)^p c \otimes d'c'$, $c \in C_p, c' \in C'_q$. Es claro que D tiene el grado correcto y como

$$\begin{aligned} D^2(c \otimes c') &= D(dc \otimes c' + (-1)^p c \otimes d'c') \\ &= d^2c \otimes c' + (-1)^{(p-1)} dc \otimes d'c' \\ &\quad + (-1)^p dc \otimes d'c' + (-1)^{2p} c \otimes d'^2 c' = 0, \end{aligned}$$

este es un complejo de cadenas.

En realidad, nosotros sólo haremos uso del producto tensorial del tipo $C \otimes_R M$, donde M es un R-módulo izquierdo. Veamos un par de propiedades de este. Sea $f : C \to C'$ un morfismo de cadenas. Hay una manera natural de definir $f \otimes 1\,(1 : M \to M)$, esto es, coordenada a coordenada; tal morfismo tiene el mismo grado que f y, como $D'(f \otimes 1) = d'f \otimes 1 + (-1)^{\deg f} f \otimes d_M 1 = d'f \otimes 1$ y $D(a \otimes m) = da \otimes m$ (de donde $(f \otimes 1)D = fd \otimes 1$) podemos afirmar que el *funtor* $- \otimes 1$ preserva morfismos de cadenas. Ahora consideremos la identidad $d'h + hd = f - g$, tensorizando en ambos lados con la identidad,

$$\begin{aligned} (d'h + hd) \otimes 1 &= (f - g) \otimes 1 \\ d'h \otimes 1 + hd \otimes 1 &= f \otimes 1 - g \otimes 1 \\ D'(h \otimes 1) + (h \otimes 1)D &= f \otimes 1 - g \otimes 1. \end{aligned}$$

Significa que tensorizar con la identidad de M preserva homotopías.

3. Complejo de morfismos graduados

Prodederemos como en la sección anterior, iniciando con las nociones usuales.

Sean M y N R-módulos, pensemos izquierdos. Denotemos por $\mathrm{Hom}_R(N, M)$ al conjunto de R-homomorfismos $N \to M$. La estructura de N induce una estructura natural de grupo abeliano sobre $\mathrm{Hom}_R(M, N)$ definida por $u + v(m) = u(m) + v(m)$ para $u, v \in \mathrm{Hom}_R(M, N)$, $m \in M$, que sigue siendo lineal: $r[(u+v)m] = r(u(m)+$

$\nu(m)) = u(rm) + \nu(rm)$. Si el anillo R no es conmutativo, no hay una manera canónica de dar estructura de R-módulo a $\mathrm{Hom}_R(M, N)$.

Dado un homomorfismo $f : M \to M'$, consideremos la aplicación

$$\mathrm{Hom}(f, N) : \mathrm{Hom}_R(M', N) \to \mathrm{Hom}_R(M, N), \qquad u \mapsto u \circ f,$$

es un ejercicio mental ver que este es un homomorfismo [3]. La primera propiedad funtorial, en este caso, es simplemente la asociatividad de la composición de funciones, con el detalle de la *contravariancia*, es decir

$$\mathrm{Hom}(f \circ g, N) = \mathrm{Hom}(g, N) \circ \mathrm{Hom}(f, N),$$

porque $\mathrm{Hom}(f \circ g, N)u = u \circ (f \circ g) = (u \circ f) \circ g = \mathrm{Hom}(g, N)(\mathrm{Hom}(f, N)u)$; y la segunda es $u \circ 1 = u$ (que nos da $\mathrm{Hom}(1, N) = 1$). Como en el caso del producto tensorial, si $f \circ g = 0$, también $\mathrm{Hom}(f \circ g, N) = 0$.

En ciertos casos, hay un isomorfismo $\mathrm{Hom}_R(R, M) = M/M_0$, donde es el submódulo [4] $M_0 = \{m \in M | rm = 0 \forall r \in R\}$. Esto es debido a que un elemento $m \in M$ define un homomorfismo φ_m tal que $r \mapsto rm$ ($\varphi(m) \in \mathrm{Hom}_R(R, M)$ porque $(r + s)m = rm + sm$); además $\varphi_{m+n}(r) = r(m + n) = rm + rn = \varphi_m(r) + \varphi_n(r)$, por lo que φ define un homomorfismo de grupos abelianos. Si $\varphi_m = 0$ entonces $Rm = 0$. Ahora, sea $u \in \mathrm{Hom}_R(R, M)$ y asumamos, existe $r \in R$ tal que $Rr = R$, en tal caso, $\varphi_{u(r)} = u$. Cuando $M_0 = 0$, análogamente a como sucedió con el producto tensorial, se tiene el isomorfismo $\mathrm{Hom}_R(R, M) \approx_R M$, definiendo $(rf)(s) = f(sr)$ que cumple $(rf)(ls) = f(lsr) = lf(sr) = l(rf)(s)$. Esto es cierto, por ejemplo, cuando R tiene unitario, puesto que $Rm = 0$ implica $0 = 1m = m$ y $R1 = R$.

También tenemos un isomorfismo $\mathrm{Hom}_R(M, N_1 \oplus N_2)$' $\approx \mathrm{Hom}_R(M, N_1) \oplus \mathrm{Hom}_R(M, N_2)$. Esto es porque cualquier homomorfismo $M \to N_1 \oplus N_2$ se parte, de manera única, en isomorfismos $M \to N_i$, componiendo con las proyecciones naturales.

---

[3] Imagina que la u es una suma.

[4] Si $m, n \in M_0$, $r \in R$ entonces $R(m + n) = Rm + Rn = 0 + 0$ y $R(rm) = (Rr)m = 0$ porque $Rr \subset R$.

Para complejos de cadenas C, C', definimos $\mathrm{Hom}_R(C, C')_n$ como el conjunto de morfismos de grado n de C a C', es decir, $\mathrm{Hom}_R(C, C')_n = \prod_{n\in\mathbb{Z}} \mathrm{Hom}_R(C_p, C'_{p+n})$; con operador frontera $D_n(: \mathrm{Hom}_R(C, C')_n \to \mathrm{Hom}_R(C, C')_{n-1})$ dado por $d'f - (-1)^n fd$. Este es un complejo de cadenas, ya que

$$\begin{aligned} D_{n-1} \circ D_n f &= D_{n-1}(d'f - (-1)^n fd) \\ &= d'^2 f - (-1)^{n-1} d'fd - (-1)^n d'fd \pm fd^2 = 0. \end{aligned}$$

Estamos particularmente interesados en módulos de homomorfismos del tipo $\mathrm{Hom}_R(C, M)$, con M un R-módulo izquierdo. Como M está concentrado en dimensión cero ($M = C'_0,\ C'_i = 0, i \neq 0$), $\mathrm{Hom}_R(C, M)^n = \mathrm{Hom}_R(C, M)_{-n} = \mathrm{Hom}_R(C_n, M)$, considerando a este como complejo de cocadenas. Es importante saber si se preservan las homotopías y los morfismos de cadenas.

Sea $f : C \to C'$ un morfismo de cadenas. La definición de $\mathrm{Hom}(f, M) : \mathrm{Hom}_R(C', M) \to \mathrm{Hom}_R(C, M)$es análoga a la anterior, esto es, $u \mapsto u \circ f$; tal morfismo tiene el mismo grado que f y, si f es morfismo de cadenas

$$\begin{aligned} D_n(\mathrm{Hom}(f, M)u) &= d_M(uf) - (-1)^n (uf)d = -(-1)^n (uf)d \\ &= -(-1)^n (ud')f = \mathrm{Hom}(f, M)(d_M u - (-1)^n ud') \\ &= \mathrm{Hom}(f, M)D'_n u, \end{aligned}$$

($\deg u = n$, y $d_M = 0$ porque M está concentrado en dimensión cero) por eso podemos afirmar que el *funtor* $\mathrm{Hom}_R(-, M)$ preserva morfismos de cadenas. Ahora consideremos la identidad $d'h + hd = f - g$ y apliquemos $\mathrm{Hom}_R(-, M)$ de ambos lados, a un elemento u de grado n

$$\begin{aligned} \mathrm{Hom}(d'h + hd, M)u &= \mathrm{Hom}(f - g, M)u \\ u(d'h + hd) &= u(f - g) \\ ud'h + uhd &= uf - ug \end{aligned}$$

porque u es homomorfismo

$$\begin{aligned}(D'_n u)[-(-1)^n h] + D_n(u[-(-1)^n h]) &= \mathrm{Hom}(f, M)u - \mathrm{Hom}(g, M)u \\ \mathrm{Hom}(-(-1)^n h, M)D'_n u + D_n \mathrm{Hom}(-(-1)^n h, M)u & \\ = \mathrm{Hom}(f, M)u - \mathrm{Hom}(g, M)u.&\end{aligned}$$

Significa $\mathrm{Hom}_R(-, M)$ preserva homotopías [5].

4. Resoluciones libres

Sea R un anillo con unitario y M un R-módulo. Una resolución de M es una sucesión exacta de R-módulos

$$\cdots \to F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} M \to 0.$$

Si cada F_i es libre[6], la resolución se dice libre.

Las resoluciones libres existen para cualquier módulo: sea F_0 el R-módulo libre con un generador por cada elemento de M, i.e.

$$F_0 = \{ \sum_{m \in M} a(m) e_m \,|\, a(g) \in R,\ a(m) = 0 \ \dot{\forall} m \in M\}$$

(el símbolo $\dot{\forall}$ significa "para todo, salvo un número finito"), aquí, e_m es un símbolo formal, una letra por decir algo. Luego, la asignación $e_m \mapsto m$ induce un homomorfismo $\varepsilon : F_0 \to M$ que es sobre por definición. Al módulo $\ker \varepsilon$, de las *relaciones* de M, podemos aplicarle el mismo procedimiento y así sucesivamente para obtener una resolución de M.

En términos de complejos de cadenas, una resolución puede verse como complejo acíclico con M en la posición -1, o bien $F = (F_i, \partial_i)_{i \geqslant 0}$ se considera como complejo acíclico y $\varepsilon : F \to M$ como morfismo de cadenas; la exactitud de la sucesión, significa que ε es una equivalencia débil ($H_0(F) \approx M$).

---

[5] Como las direcciones de los homomorfismos se invierten bajo $\mathrm{Hom}_R(-, M)$, la última identidad se ve un poco distinta (la prima se cambia de lugar). También hay que tener la precaución de cambiar el signo de h en cada grado, es decir, la homotopía es $h' = (-(-1)^n h_n)_{n \in \mathbb{Z}}$, en términos de h.

[6] Recordemos que un R-módulo se dice libre si es isomorfo a una suma directa de copias de R.

5. El anillo de grupo

A todo grupo G se le puede poner en correspondencia un anillo con unitario, llamado el *anillo de grupo* y al cual denotamos $\mathbb{Z}G$, construido de la siguiente manera.

$$\mathbb{Z}G = \{\sum_{g\in G} a(g)g \,|a(g) \in \mathbb{Z},\ a(g) = 0\ \dot\forall g \in G\}.$$

Es decir, $\mathbb{Z}G$ es el grupo libre abeliano generado por los elementos de G. Ahora, la multiplicación de G se extiende de manera natural [7] a una multiplicación en $\mathbb{Z}G$ que hace de él un anillo cuyo unitario es el elemento neutro $1 \in G$.

Por ejemplo, el grupo trivial $G = 1$ claramente tiene $\mathbb{Z}$ como anillo de grupo y la multiplicación resulta la multiplicación usual de enteros.

El grupo G puede ser incluido de la manera obvia dentro de su anillo de grupo, de esta manera, G es un subgrupo del grupo $(\mathbb{Z}G)^*$ de unidades de $\mathbb{Z}G$.

El anillo de grupo tiene la siguiente *propiedad universal*. Dado un anillo R, cualquier homomorfismo de grupos $f : G \to R^*$, tiene una única extensión a un homomorfismo de anillos $\widetilde{f} : \mathbb{Z}G \to R$, definida por

$$\widetilde{f}(g + h) = f(g) + f(h) \quad \text{y} \quad \widetilde{f}(ag) = af(g)\ (a \in \mathbb{Z})$$

(en particular, $\widetilde{f}(g) = f(g)$, por lo que esta es una extensión; además, de la misma identidad y de que f es homomorfismo, $\widetilde{f}(gh) = \widetilde{f}(g)\widetilde{f}(h)$ lo que se extiende al producto del anillo de grupo usando repetidamente la definición).

A manera de ejemplo, observemos que el único homomorfismo $G \to 1$ nos da un homomorfismo canónico $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$, llamado de *aumentación*, que se caracteriza por

$$\varepsilon(\sum_{g\in G} a(g)g) = \sum_{g\in G} a(g).$$

[7] Por linealidad, considerando al grupo abeliano como $\mathbb{Z}$-módulo.

6. Módulos sobre el anillo de grupo

Por simplicidad, llamamos G-módulos a los módulos sobre el anillo del grupo G. Recordemos que un R-módulo puede pensarse como un grupo abeliano A, junto con un homomorfismo de R al anillo de endomorfismos [8] de A; de acuerdo con la propiedad universal, tal homomorfismo corresponde a un homomorfismo de grupos $G \to \mathrm{End}(A)^* = \mathrm{Aut}(A)$, el grupo de automorfismos de A. Es decir, un G-módulo es simplemente un grupo abeliano junto con una acción de G.

Por ejemplo, cualquier grupo abeliano A es un G-módulo bajo la acción trivial, en este caso, $ra = \varepsilon(r)a,\ a \in A, r \in \mathbb{Z}G$ con ε la aumentación [9]. En particular, $\mathbb{Z}$ es siempre un G-módulo.

7. La homología y cohomología del grupo

Cuando M, N son ambos G-módulos izquierdos[?], consideramos a M como G-módulo derecho bajo $mg = g^{-1}m$. El producto tensorial obtenido de esta forma se denota por $M \otimes_G N$.

Consideremos una resolución libre F de $\mathbb{Z}$ sobre $\mathbb{Z}G$, i.e. una resolución de $\mathbb{Z}$ visto como G-módulo con acción trivial, y sea M un G-módulo izquierdo, definimos la *homología de* G *con coeficientes en* M por

$$H_*(G, M) = H_*(F \otimes_G M)$$

y la *cohomología de* G *con coeficientes en* M por

$$H^*(G, M) = H^*(\mathrm{Hom}_G(F, M)),$$

de acuerdo a las secciones anteriores, estos conceptos están bien definidos[10] y son invariantes bajo homotopías[11].

8. La resolución estándar y la notación barra

Es posible construir una resolución de $\mathbb{Z}$ sobre $\mathbb{Z}G$ a partir de los elementos de G.

---

[8] Denotado por $\mathrm{End}(A) = \mathrm{Hom}_{\mathbb{Z}}(A, A)$, tiene estructura de anillo inducida por la composición de funciones.

[9] $ra = \sum_{g \in G} n(g)g \cdot a = \sum_{g \in G} n(g)ga = \sum_{g \in G} n(g)a = \varepsilon(r)a$

[10] $F \otimes_G M$ y $\mathrm{Hom}_G(F, M)$ son complejos de cadenas

[11] Los funtores $- \otimes_G M$ y $\mathrm{Hom}_G(-, M)$ preservan homotopías

Sea F_n el grupo libre abeliano generado por las $(n+1)$-adas de la forma $(g_i)_{i=0}^n$, G actúa sobre F_n mediante $g \cdot (g_i)_{i=0}^n = (gg_i)_{i=0}^n$. Esta acción es libre: de $gg_i = g_i$ se sigue $g = 1$; significa que las orbitas bajo esta acción son copias de G y, por eso, cada órbita genera una copia de $\mathbb{Z}G$; además, debido a que tales órbitas son disjuntas, concluimos que F_n es suma directa de copias de $\mathbb{Z}G$, es decir, F_n es libre.

La diferencial $\partial : F_n \to F_{n-1}$ se define por

$$\partial(g_i)_{i=0}^n = \sum_{i=0}^{n}(-1)^i(g_0, \ldots, \hat{g}_i, \ldots, g_n) = \sum\nolimits_{i=0}^{n}(-1)^i(\hat{g}_i),$$

donde el gorro indica que el elemento que lo porta ha sido omitido y $\varepsilon : F_0 = \mathbb{Z}G \to \mathbb{Z}$ es la aumentación. Este es un operador frontera, ya que

$$\begin{aligned}
\partial^2(g_i)_{i=0}^n &= \sum_{i=0}^{n}(-1)^i\partial(\hat{g}_i) \\
&= \sum_{i=0}^{n}(-1)^i\left[\sum_{j<i}(-1)^j(\hat{g}_j, \hat{g}_i) + \sum_{j<i}(-1)^{j-1}(\hat{g}_i, \hat{g}_j)\right] \\
&= \sum_{j,i}[(-1)^i(-1)^j(\hat{g}_i, \hat{g}_j) + (-1)^i(-1)^{j-1}(\hat{g}_i, \hat{g}_j)] = 0
\end{aligned}$$

Para ver que este complejo es acíclico, de acuerdo a la primera sección, basta ver que es contraible, incluso como complejo de $\mathbb{Z}$-módulos[12]. Para ello definimos $h : F_n \to F_{n+1}$ tal que $h(g_i)_{i=0}^n = (1, g_0, \ldots, g_n) = (1, g_i)_{i=0}^n$ y $h(1) = 1$ si $n = -1$ y calculamos

$$\begin{aligned}
(\partial h + h\partial)(g_i)_{i=0}^n &= \partial h(g_i)_{i=0}^n + h\partial(g_i)_{i=0}^n \\
&= \partial(1, g_i)_{i=0}^n + h\sum_{i=0}^{n}(-1)^i(\hat{g}_i) \\
&= (g_i)_{i=0}^n + \sum_{i=0}^{n}(-1)^{i+1}(1, \hat{g}_i) + \sum_{i=0}^{n}(-1)^i(\hat{g}_i) \\
&= (1, g_i)_{i=0}^n,
\end{aligned}$$

en un caso, y $(\partial h + h\varepsilon)(g) = \partial(1, g) + (1) = (g) - (1) + (1)$ en el otro. Significa que h es una homotopía de contracción.

[12] La identidad $\operatorname{Im}\partial_n = \ker\partial_{n+1}$ no depende de la estructura de G-módulo.

Por lo tanto, $F_* = F_*(G)$ es una resolución, comúnmente llamada *resolución estándar*.

Ahora, notemos que, como

$$\begin{aligned}(g_0, \ldots, g_n) &= g_0(1, g_0^{-1}g_1, \ldots, g_0^{-1}g_n) \\ &= g_0(1, g_0^{-1}g_1, g_0^{-1}g_1g_1^{-1}g_2, \ldots, g_0^{-1}g_1g_1^{-1}\cdots g_{n-1}^{-1}g_n)\end{aligned}$$

renombrando $g'_i = g_{i-1}^{-1}g_i$, $i = 1, 2, \ldots, n$, obtenemos una $\mathbb{Z}G$-base de F_n de la forma

$$(1, g_1, g_1g_2, \ldots, g_1\cdots g_n) = [g_1|\cdots|g_n]$$

conocida como la notación barra[13]; para esta base, tenemos

$$\begin{aligned}(\hat{g}_0) &= g_1[g_2|\cdots|g_n] \\ (\hat{g}_i) &= [g_1|\cdots|g_{i-1}g_i|\cdots|g_n], \quad i = 1, 2, \ldots, n-1 \\ (\hat{g}_n) &= [g_1|\cdots|g_{n-1}]\end{aligned}$$

Podemos también *normalizar* esta resolución. Consideremos el módulo (graduado) $\bar{F}_* = F_*/D_*$ donde D_* es generado por los $(g_i)_{i=0}^n$ tales que $g_i = g_{i+1}$ para alguna i. Si $(g_j) \in D_n$

$$\partial(g_j) = \sum_{j\neq i,i+1}^{n} (-1)^j(\hat{g}_j) \in D_{n-1}$$

(los elementos que corresponden a i e $i+1$ se cancelan), de donde hay una diferencial inducida sobre $\bar{F}_*$ que lo hace un complejo de cadenas; además es claro que $hD_* \subset D_*$, por lo que se induce una homotopía de contracción que muestra que $\bar{F}_*$ es acíclico y, por tanto, una resolución.

Expresemos los complejos que se obtienen, en términos de la resolución barra, al calcular la homología del grupo. Los elementos de $F_*(G) \otimes_G M = C_*(G, M)$ son sumas finitas de elementos de la forma $m \otimes [g_1|\cdots|g_n]$ y el operador frontera $\partial : C_n(G, M) \to C_{n-1}(G, M)$

[13]Esto también sirve para probar que, como G-módulo, F_n depende sólo de n parámetros.

está dado por

$$\partial(m \otimes [g_1|\cdots|g_n]) = mg_1 \otimes [g_2|\cdots|g_n] + \sum_{i=1}^{n-1}(-1)^i m \otimes [g_1|\cdots|g_{i-1}g_i|\cdots|g_n] + (-1)^n m \otimes [g_1|\cdots|g_{n-1}].$$

De manera similar, un elemento de $\mathrm{Hom}_R(F_*(G), M) = C^*(G, M)$ puede pensarse como una función arbitraria de n variables $f : G^n \to M$ (puesto que G^n es el conjunto de generadores). El operador cofrontera
$\delta : C^{n-1}(G, M) \to C^n(G, M)$ se ve como

$$(\delta f)(g_i)_{i=1}^n = g_1 f(g_i)_{i=2}^n + \sum_{i=1}^{n-1}(-1)^i f(g_1, \ldots, g_{i-1}g_i, \cdots, g_n) + (-1)^n f(g_i)_{i=1}^{n-1}.$$

Estas expresiones aparecerán de manera natural en el capítulo siguiente.

CAPíTULO 2

Extensiones con núcleo abeliano

Una sucesión exacta *corta* es una de la forma

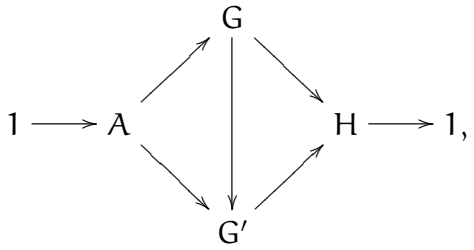
$$1 \to A \to G \to H \to 1,$$

donde 1 en este caso denota el neutro del los grupos (sería cero si los grupos fueran abelianos y se escribiesen en notación aditiva, como es el caso de los módulos). En el caso de grupos, una sucesión exacta corta es también llamada una *extensión* de A por H. [?]

Otra extensión

$$1 \to A \to G' \to H \to 1,$$

es equivalente si hay un homomorfismo $G \to G'$ que hace conmutar el diagrama



este es necesariamente un isomorfismo. [1]

El *problema de extensión* consiste en hallar todos los grupos G, salvo equivalencia, en función del subgrupo N y del cociente $G/A = H$. Este problema, como veremos, aunque no en el caso general[2], involucra la cohomología de grupo en dimensiones bajas.

Asumamos que A es un grupo abeliano (escrito en notación aditiva). Una característica de la extensión

$$0 \to A \xrightarrow{i} G \xrightarrow{\pi} H \to 1$$

[1] Examinando el subdiagrama de la izquierda vemos que debe ser uno a uno y, con el de la derecha, que debe ser sobre.

[2] En caso general se requiere del concepto de módulo cruzado [?], [?].

es que esta origina una acción de H sobre A o, sea, que A tiene estructura de H-módulo. Esto es debido a que A, visto como subgrupo de G bajo la inclusión i, posee la acción de G por conjugación pero, siendo abeliano, la acción de A en sí mismo es trivial. Significa que hay una acción induccida de $G/A = H$ sobre A. Entonces, la acción de h en a bajo i es conjugación por un representante $\widetilde{h}$ de h en G:

$$i(ha) = \widetilde{h}i(a)\widetilde{h}^{-1},$$

con $\pi(\widetilde{h}) = h$. Para nuestros propósitos, es más cómodo escribir tal identidad como una *regla de conmutación*:

$$\widetilde{h}i(a) = i(ha)\widetilde{h}.$$

Sabiendo lo anterior, se considera el problema de clasificar las extensiones que originan una acción dada.

1. Extensiones escindidas

Veamos que hay extensiones para cualesquier par de grupos A y H. Sea A un H-módulo y

$$0 \to A \xrightarrow{i} G \xrightarrow{\pi} H \to 1$$

una extensión que da origen a tal estructura. Decimos que esta extensión se escinde si tiene una escisión, i.e. hay un homomorfismo $s : H \to G$ tal que $\pi s = id_H$. Nótese que tal escisión debe ser inyectiva.

Dada una escisión, hay una biyección $A \times H \approx G$ definida por $(a, h) \mapsto i(a)s(h)$[3]. De esta manera, hay una única estructura de grupo sobre $A \times H$ que hace de tal biyección un isomorfismo. Calculemos tal estructura.

$$i(a)s(h)i(b)s(k) = i(a)i(hb)s(h)s(k)$$

por la regla de conmutación y, como i y s son homomorfismos,

$$= i(a + hb)s(hk).$$

[3] Aplicando π a la identidad $i(a)s(h) = i(a')s(h')$ obtenemos $h = h'$ ($A = \ker \pi$) y, de ahí, $i(a) = i(a')$ pero i es inyectiva por definición. La suprayectividad es consecuencia de que todo elemento de G pertenece a una clase lateral $gi(A)$ y que s, siendo inyectiva, da un conjunto de representantes de estas. Nótese que no hacemos uso de que s sea homomorfismo.

Por eso, la esctructura de grupo sobre $A \times H$ está dada por

$$(a, h) \cdot (b, k) = (a + hb, hk).$$

Esta ley de grupo[4], definida para cualquier acción de H sobre A, se conoce como *producto semidirecto* y se denota usualmente por $A \rtimes H$; la escisión canónica es $h \mapsto (0, h)$. Podemos resumir esto en la siguiente

PROPOSICIÓN 1. *La extensión con núcleo abeliano*

$$0 \to A \xrightarrow{i} G \xrightarrow{\pi} H \to 1$$

se escinde si, y sólo si, es equivalente a la extensión

$$0 \to A \xrightarrow{i'} A \rtimes H \xrightarrow{\pi'} H \to 1$$

donde i' y π' son las inclusión y proyección canónicas heredadas del producto cartesiano.

Es decir, hay sólo una extensión escindida para cada acción.

Describamos ahora las posibles escisiones.

PROPOSICIÓN 2. *Para cualquiér H-módulo A. Las clases de A-conjugación de escisiones de la extensión*

$$0 \to A \to A \rtimes H \to H \to 1$$

están en correspondencia uno a uno con los elementos de $H^1(G, A)$.

DEMOSTRACIÓN. Sea $s : H \to A \rtimes H$ una sección, i.e. una función tal, que $\pi s = \mathrm{id}$, entonces $s(h) = (fh, h)$ donde f es una función $H \to A$; además

$$s(h)s(k) = (fh + hfk, hk),$$

para que la sección s sea homomorfismo, f debe satisfacer $f(hk) = fh + hfk$, equivalentemente,

$$0 = hfk - f(hk) + fh = (\delta f)(h, k).$$

---

[4] $(a, h) \cdot (b, k) = (a + hb, hk) = (0, 1)$ implica $hb = -a$ que equivale a $b = -a$ y $k = h^{-1}$; además $(-a, h^{-1})(a, h) = (a + h^{-1}(-a), h^{-1}h) = (0, 1)$. Revisemos la asociatividad.

$$\begin{aligned}[(a, h)(b, k)](c, l) = (a + hb, hk)(c, l) &= ((a + hb) + (hk)c, (hk)l) \\ &= (a + h(b + kc), h(kl)) = (a, h)[(b, k)(c, l)]\end{aligned}$$

.

O bien, f debe ser un 1-cociclo de $C^1(H, A)$.

Vamos a decir que dos escisiones s_1 y s_2 son A-conjugadas[5] si hay un elemento $a \in A$ para el cual $s_1(h) = i(a)s_2i(a)^{-1}$ para todo $h \in H$. En $A \rtimes H$,

$$(a, 1)(b, h)(a, 1)^{-1} = (a + b - ha, h);$$

así, la relación de conjugación, se ve como $f_1h = a + f_2h - ha$, i.e.

$$(f_2 - f_1)h = ha - a = hf(1) - f(1) = (\delta f)h$$

donde $f : C^0(H, A) = \mathrm{Hom}_H(\mathbb{Z}H, A) = A \to A; 1 \mapsto a$. □

2. Número de extensiones

Una vez habiendo calentado (con la sección anterior), quedamos listos para ver cuantas extensiones hay para una acción fija. La estrategia es similar: buscar funciones $H^n \to A$ y hacer uso de la resolución barra.

TEOREMA 3. *Sea A un H-módulo y denotemos por $\mathcal{E}(H, A)$ las clases de equivalencia de extensiones de A por H que originan la acción de H sobre A. Entonces hay una biyección*

$$\mathcal{E}(H, A) \approx H^2(H, A).$$

DEMOSTRACIÓN. Nuevamente consideremos la extensión

$$0 \to A \xrightarrow{i} G \xrightarrow{\pi} H \to 1$$

y escojamos una sección $s : H \to G$ ($\pi s = \mathrm{id}_H$). Por simplicidad en la exposición, puesto que será requerido más adelante, vamos a sumir que s está *normalizada*, i.e.

$$s(1) = 1.$$

Si s resulta homomorfismo, entonces la extensión escinde y ya conocemos su estructura. De otro modo, como $s(hk)$ y $s(h)s(k)$ son enviados a hk bajo π, deben estar en la misma clase lateral; es decir,

$$s(h)s(k) = i(f(h, k))s(hk)$$

donde $f : H \times H \to A$ es alguna función *normalizada*: de $s(h) = s(1)s(h) = s(h)s(1) = i(f(1, h))s(1 \cdot h) = i(f(h, 1)s(h \cdot 1)$ se sigue

$$f(1, h) = 0 = f(h, 1)$$

[5]Debiese quedar claro a quien ha tomado un curso de teoría de grupos que a continuación se define una relación de equivalencia.

para todo $h \in H$. Usualmente a f se le llama *conjunto de factores* asociados a la extensión y a s. Ahora deberemos probar que la extensión puede recobrarse a partir de la acción y del conjunto de factores. Como $s(H)$ es un conjunto de representantes de las clases laterales, nuevamente tenemos la biyección $(a, h) \mapsto i(a)s(h)$. Calculemos la multiplicación inducida en $A \times H = G_f$ en este caso:

$$\begin{aligned} i(a)s(h)i(b)s(k) &= i(a)i(hb)s(h)s(k) \\ &= i(a + hb)i(f(h,k))s(hk) \\ &= i(a + hb + f(h,k))s(hk); \end{aligned}$$

de donde,

$$(a, h) \cdot (b, k) = (a + hb + f(h,k), hk).$$

Encontremos condiciones para que esto defina una estructura de grupo.

$$\begin{aligned} [(a,h)(b,k)](c,l) &= (a + hb + f(h,k), hk)(c,l) \\ &= (a + hb + f(h,k) + (hk)c + f(hk,l), (hk)l), \end{aligned}$$

por otro lado,

$$\begin{aligned} (a,h)[(b,k)(c,l)] &= (a,h)(b + kc + f(k,l), kl) \\ &= (a + hb + h(kc) + hf(k,l) + f(h,kl), h(kl)). \end{aligned}$$

De modo que, para que el producto sea asociativo, el conjunto de factores $f : H \times H \to A$ debe satisfacer la relación

$$f(h,k) + f(hk,l) = hf(k,l) + f(h,kl)$$

equivalentemente,

$$0 = hf(k,l) - f(hk,l) + f(h,kl) - f(h,k) = (\delta f)(h,k,l)$$

para cualesquiera $h, k, l \in H$. En otras palabras, f es un 2-cociclo obtenido de la resolución barra normalizada.

El elemento $(0, 1)$ resulta el neutro del grupo:

$$(0,1) \cdot (b,k) = (1b + f(1,k), 1k) = (b,k)$$

y

$$(a,h) \cdot (0,1) = (a + h0 + f(h,1), h1) = (a,h)$$

$$(a + hb + f(h, k), hk) = (0, 1)$$

nos da $k = h^{-1}$, de donde debe suceder $a + hb + f(h, h^{-1}) = 0$,i.e.

$$b = -h^{-1}(a + f(h, h^{-1}))$$

que debe funcionar por la izquierda:

$$\begin{aligned}(-h^{-1}a - h^{-1}f(h, h^{-1}), h^{-1})(a, h) = \\ (-h^{-1}a - h^{-1}f(h, h^{-1}) + h^{-1}a + f(h^{-1}, h)), 1) \\ = (-h^{-1}f(h, h^{-1}) + f(h^{-1}, h)), 1),\end{aligned}$$

por eso, deberá ser cierta la identidad

$$h^{-1}f(h, h^{-1}) = f(h^{-1}, h).$$

Como f es cociclo,

$$\begin{aligned}0 &= h^{-1}f(h, h^{-1}) - f(h^{-1}h, h^{-1}) + f(h^{-1}, hh^{-1}) - f(h^{-1}, h) \\ &= h^{-1}f(h, h^{-1}) - f(h^{-1}, h)\end{aligned}$$

De modo que la multiplicación de G_f está bien definida.

Denotando $\varphi(i(a)s(h)) = (a, h)$ tenemos

$$\varphi i(a) = \varphi(i(a)s(1)) = (a, 1),$$

la inclusión canónica y,

$$\pi\varphi^{-1}(a, h) = h,$$

la proyección canónica que son claramente homomorfismos. Entonces, la extensión inicial es equivalente a la extensión

$$0 \to A \xrightarrow{i'} G_f \xrightarrow{\pi'} H \to 1$$

definida solamente en términos de f y una acción dada de H sobre A.

Ahora cambiemos la elección de la sección s por una s' (también normalizada); como $h = \pi s(h) = \pi s'(h)$ sabemos que $s'(h) = i(c(h))s(h)$, donde $c : H \to A$ es arbitraria salvo por la condición $c(1) = 0$, i.e. es un elemento arbitrario de $C^1_N(H, A)$. Calculemos el

conjunto de factores asociado.

$$\begin{aligned} s'(h)s'(k) &= i(c(h))s(h)i(c(k))s(k) = i(a)i(hc(k))s(h)s(k) \\ &= i(c(h) + hc(k))i(f(h,k))s(hk) \\ &= i(c(h) + hc(k) + f(h,k) - c(hk))i(c(hk))s(hk) \\ &= i(c(h) + hc(k) + f(h,k) - c(hk))s'(hk), \end{aligned}$$

así

$$f'(h,k) = f(h,k) + hc(k) - c(hk) + c(h) = f(h,k) + (\delta c)(h,k). \quad \square$$

CAPíTULO 3

Congruencias

1. Un poco de aritmética

Antes de comenzar con los cálculos, recordemos un poco la estructura del grupo $\mathbb{Z}/m$. Por definición,

$$\mathbb{Z}/m = \mathbb{Z}/m\mathbb{Z}$$

o bien, dos números a y b son equivalentes módulo m ($a \equiv b (\mathrm{mod}\, m)$) si m divide a $a - b$ ($m|a - b$). Además de la estructura aditiva, debido a que $\mathbb{Z}$ es un anillo bajo la multiplicación usual y $m\mathbb{Z}$ un ideal, $\mathbb{Z}/m$ tiene también estructura de anillo (conmutativo con unitario) inducida por la multiplicación usual de enteros.

El grupo de elementos invertibles en $\mathbb{Z}/m$ (o unidades) puede ser descrito como

$$(\mathbb{Z}/m)^* = \{a \in \mathbb{Z}/m | (a, m) = 1\}$$

((a, m) denota el máximo común divisor de a y m), ya que, $(a, m) = 1$ equivale a $ab + mc = 1$ para algún b, de donde $ab \equiv 1 (\mathrm{mod}\, m)$ [1]. El orden de este grupo se denota por $\varphi(m) = |(\mathbb{Z}/m)^*|$ y se llama la función $\varphi\, (: \mathbb{N} \to \mathbb{N})$ de Euler (evaluada en m).[2]

Todo endomorfismo[3] de $\mathbb{Z}/m$ está determinado por la imagen del generador $1 \in \mathbb{Z}/m \mapsto a \in \mathbb{Z}/m$ y el morfismo coincide con la multiplicación por este elemento ($\psi_a(b) = b\psi(1) = ba = ab$). Esto da una identificación

$$\mathrm{End}\, (\mathbb{Z}/m) \approx \mathbb{Z}/m, \qquad (\psi_a \mapsto a);$$

---

[1] En lo sucesivo, si no provoca confusión, denotaremos $ab = 1$

[2] En realidad, Euler definió $\varphi(m)$ como la cantidad de primos relativos a m que sean positivos y menores a este.

[3] Homomorfismo $\mathbb{Z}/m \to \mathbb{Z}/m$.

en particular, el grupo de automorfismos [4] $\mathrm{Aut}\,(\mathbb{Z}/m) \approx (\mathbb{Z}/m)^*$ (porque $1 = \psi_a\psi_b(1) = ab$). Significa que toda estructura de $\mathbb{Z}/n$-módulo sobre $\mathbb{Z}/m$ viene de un homomorfismo $\mathbb{Z}/n \to (\mathbb{Z}/m)^*$. Similarmente, uno de estos homomorfismos está determinado por la imagen del generador de $1 \in \mathbb{Z}/n \mapsto t \in \mathbb{Z}/m$, bajo la restricción $t^n = (t^{(\varphi(m),n)})^l = 1$, $(l = \frac{n}{(\varphi(m),n)})$, es decir $t^n = t^{(\varphi(m),n)} = 1$, debido a que el orden de t debe ser un divisor de $\varphi(m)$.

2. Estructura del grupo de invertibles

En esta sección exploraremos la estructura del grupo de automorfismos del anillo $\mathbb{Z}/n$, basándonos en el ejemplo 1.4 de [?].

$$\mathrm{Aut}\,(\mathbb{Z}/nm) = \mathrm{Aut}\,(\mathbb{Z}/n \times \mathbb{Z}/m) = \mathrm{Aut}\,(\mathbb{Z}/n) \times \mathrm{Aut}\,(\mathbb{Z}/m)$$

cuando (n,m)=1, ya que $\mathbb{Z}/nm = \mathbb{Z}/n \times \mathbb{Z}/m$. Por eso, para describir la estructura de estos grupos, basta considerar el caso $n = p^r$ donde p es un número primo. En este caso, el grupo $(\mathbb{Z}/m)^*$ tiene $p^{r-1}(p-1)$ elementos.

Caso $n = 2^r$. Cuando $r = 1$, $\varphi(2) = 1$. Cuando $r = 2$, el grupo de invertibles tiene dos elementos y por eso es isomorfo a $\mathbb{Z}/2$.

Para $r \geqslant 3$, probaremos que $\mathrm{Aut}\,(\mathbb{Z}/2^r) = \mathbb{Z}/2 \times \mathbb{Z}/(2^{r-2})$. El elemento de orden dos es -1, probemos que 5 tiene orden 2^{r-2}. Primero, $5 \equiv 1(\mathrm{mod}\,2^2), \not\equiv 1(\mathrm{mod}\,2^3)$ y, como

$$(1 + 4 \cdot 2^s)^2 = 1 + 4 \cdot 2^{s+1}(1 + 2^{s+1}) \equiv 1(\mathrm{mod}\,2^{s+2}),\ \not\equiv 1(\mathrm{mod}\,2^{s+3}),$$

tenemos que $(1+4)^{2^{r-2}} \equiv 1(\mathrm{mod}\,2^r),\ \not\equiv 1(\mathrm{mod}\,2^{r+1})$, i.e. el orden de cinco es 2^{r-2}.

Ahora sólo falta ver que -1 y $5^{2^{r-3}}$ no son congruentes (ambos tienen orden 2). Asumamos que $2^r | 5^{2^{r-3}} + 1$, en particular, $2^{r-1} | (5^{2^{r-3}} - 1) + 2$, pero $2^{r-1} | (5^{2^{r-3}} - 1)$ (de la prueba anterior); significa que $2^{r-1} | 2$, i.e. $r = 1$ ó 2.

Caso $n = p^r$ con p primo impar. Probemos que $\mathrm{Aut}\,(\mathbb{Z}/p^r) = \mathbb{Z}/(p-1) \times \mathbb{Z}/p^{r-1}$, de hecho $1+p$ tiene orden p^{r-1} porque

$$(1 + pk)^p = 1 + p^2k + \binom{pk}{2}p^2 + \cdots + (pk)^p = 1 + p^2k(1 + a)$$

[4] Homomorfismos con inverso bilateral: $\psi_a\psi_b = \psi_b\psi_a = \mathrm{Id}_{\mathbb{Z}/m}$.

con a divisible por p. Por lo tanto, si $1 + pk \equiv 1 (\mathrm{mod}\, p^{s-1})$, $\not\equiv 1 (\mathrm{mod}\, p^s)$, entonces $(1+pk)^p \equiv 1 (\mathrm{mod}\, p^s)$, $\not\equiv 1 (\mathrm{mod}\, p^{s+1})$, comenzando con $k = 1$ obtenemos que

$$(1+p)^{p^{r-1}} \equiv 1 (\mathrm{mod}\, p^r),\ \not\equiv 1 (\mathrm{mod}\, p^{r+1}),$$

i.e. $1+p$ tienen orden p^{r-1}. Significa que $1+p$ genera el p-subgrupo de Sylow de $\mathrm{Aut}\,(\mathbb{Z}/p^r)$.

Ahora notemos que la proyección canónica $\mathbb{Z}/p^r \to \mathbb{Z}/p$ $(= \mathbb{Z}/p^r/p\mathbb{Z}/p^r)$, induce un homomorfismo $\mathrm{Aut}\,(\mathbb{Z}/p^r) \to \mathrm{Aut}\,(\mathbb{Z}/p)$ que es sobre (toma $1, 2, \ldots, p-1 \in \mathbb{Z}/p^r$); pero, de teoría de Galois, sabemos que su grupo de invertibles, $(\mathbb{Z}/p)^*$, es cíclico isomorfo a $\mathbb{Z}/p-1$, ya que consta de raices de la unidad [5]. Por lo tanto, la única opción es que $\mathrm{Aut}\,(\mathbb{Z}/p^r) = \mathbb{Z}/(p-1) \times \mathbb{Z}/p^{r-1}$. Por último, como todos los elementos de la forma $1 + pk$ forman el segundo factor, podemos asegurar que el generador del primer factor no es congruente con 1 módulo p.

Podemos resumir lo anterior como el resultado siguiente.

TEOREMA 1. *Sea* $m = 2^{r_0} p_1^{r_1} \cdots p_k^{r_k}$ *un entero arbitrario y consideremos el anillo* $\mathbb{Z}/m$ *de enteros módulo* m. *Entonces,*

$$(\mathbb{Z}/m)^* \approx \mathbb{Z}/2 \times \mathbb{Z}/2^{r_0-2} \times \mathbb{Z}/p_1^{r_1-1} \cdots p_k^{r_k-1} \times \prod_{i=1}^{k} \mathbb{Z}/(p_i - 1).$$

En particular, $\varphi(m) = 2^{r_0-1} \cdot p_1^{r_1-1}(p_1-1) \cdots p_k^{r_k-1}(p_k-1)$, un numero cuya descomposición en primos puede considerarse caótica, sin embargo, veremos que en este trabajo sólo nos interesan los primos enumerados aquí.

[5] $(\mathbb{Z}/p)^*$ es el grupo de Galois de la extensión $\mathbb{Q}(\zeta)/\mathbb{Q}$, con $\zeta = e^{2\pi i/p}$; se recomienda ver los textos estándares de tería de anillos y campos.

CAPíTULO 4

Caso metacíclico

1. La resolución

Queremos calcular los grupos $H_*(\mathbb{Z}/n, \mathbb{Z}/m)$ y $H^*(\mathbb{Z}/n, \mathbb{Z}/m)$. Para tal fin, construiremos una resolución libre de $\mathbb{Z}$ sobre el anillo de grupo de $\mathbb{Z}/n$, el cual puede ser visto como $\mathbb{Z}[T|T^n = 1] = \mathbb{Z}[T]$.

Notemos que, dentro de $\mathbb{Z}[T]$, la relación $T^n = 1$ puede reescribirse como

$$0 = T^n = 1 = (T-1)(1 + T + \cdots + T^{n-1}) = (T-1)N;$$

ahora notemos que los elementos $T - 1$ y N pueden ser vistos como morfismos $\mathbb{Z}[T] \to \mathbb{Z}[T]$ mediante multiplicación. De este modo, tiene sentido considerar el complejo de cadenas

$$\cdots \xrightarrow{N} \mathbb{Z}[T] \xrightarrow{T-1} \mathbb{Z}[T] \xrightarrow{N} \mathbb{Z}[T] \xrightarrow{T-1} \mathbb{Z}[T] \to \mathbb{Z} \to 0.$$

Solamente falta ver que tal complejo es acíclico[1]. Primero calculemos el núcleo de $(T-1)$. Sea $a = \sum_{i=0}^{n-1} a(i)T^i \in \ker(T-1)$ entonces

$$\begin{aligned} 0 = (T-1)a &= \sum_{i=0}^{n-1} a(i)T^{i+1} - \sum_{i=0}^{n-1} a(i)T^i \\ &= \sum_{i=1}^{n} a(i-1)T^i - \sum_{i=0}^{n-1} a(i)T^i \\ &= a(n-1) + \sum_{i=1}^{n-1} [a(i-1) - a(i-1)]T^i - a(0), \end{aligned}$$

lo que equivale a $a(0) = a(1) = \cdots = a(n-1) = a'$; de donde $a = Na'$ y, se sigue, $\ker(T-1) = \operatorname{Im} N$.

[1] En realidad, esta resolución es de origen topológico, véase [?] para la construcción usual.

Falta calcular el núcleo de N. Supongamos $Na = 0$, en particular, el término de grado cero debe ser nulo, este se obtiene de los productos de la forma $T^i(T^{n-i})$, por ello, tal término es igual a $\sum_{i=0}^{n-1} a(i)$. Pero, de ahí,

$$a = \sum_{i=0}^{n-1} a(i)(T^i - 1)$$

y como $T^i - 1 = (T-1)(T^{i-1} + \cdots + T + 1)$, tenemos $a = (T-1)a'$ y, por tanto, $\ker N = \mathrm{Im}\,(T-1)$.

2. Cálculo del número de extensiones

Aplicando los funtores correspondientes, vemos que hay que calcular la homología de

$$\cdots \xrightarrow{N} \mathbb{Z}/m \xrightarrow{t-1} \mathbb{Z}/m \xrightarrow{N} \mathbb{Z}/m \xrightarrow{t-1} \mathbb{Z}/m \to \mathbb{Z} \to 0$$

y la cohomología de

$$\mathbb{Z}/m \xrightarrow{t-1} \mathbb{Z}/m \xrightarrow{N} \mathbb{Z}/m \xrightarrow{t-1} \mathbb{Z}/m \xrightarrow{N} \cdots$$

donde $t^n \equiv 1 (\mathrm{mod}\, m)$ Entonces, $H_0(\mathbb{Z}/n, \mathbb{Z}/m) = \mathbb{Z}/m/\mathrm{Im}\,(t-1)$, $H^0(\mathbb{Z}/n, \mathbb{Z}/m) = \ker\,(t-1)$ y

$$H_i(\mathbb{Z}/n, \mathbb{Z}/m) = H^{i+1}(\mathbb{Z}/n, \mathbb{Z}/m) = \ker\,(t-1)/\mathrm{Im}\ N$$

para $i \geqslant 0$ impar,

$$H_i(\mathbb{Z}/n, \mathbb{Z}/m) = H^{i-1}(\mathbb{Z}/n, \mathbb{Z}/m) = \ker\ N/\mathrm{Im}\,(t-1)$$

para pares mayores que cero.

Primero consideremos el caso en que la acción sea trivial $(t = 1)$ [2]. En tal caso, $\ker\,(t-1) = \mathbb{Z}/m$, $\mathrm{Im}\,(t-1) = 0$, $N = n$ y, por tanto

$$\ker\ N = \frac{m}{(m,n)}\mathbb{Z}/m,$$

$$\mathrm{Im}\ N = (m,n)\mathbb{Z}/m$$

y entonces

$$H_1(\mathbb{Z}/n, \mathbb{Z}/m) = \mathbb{Z}/(m,n),$$

$$H_2(\mathbb{Z}/n, \mathbb{Z}/m) = \frac{m}{(m,n)}\mathbb{Z}/m = \mathbb{Z}/(m,n).$$

[2] Sólo porque en este caso la respuesta general es fácil de obtener.

Solamente hay acciones no triviales de $\mathbb{Z}/n$ sobre $\mathbb{Z}/m$ cuando n y el orden $\varphi(m)$ del grupo $(\mathbb{Z}/m)^* = \mathrm{Aut}\,(\mathbb{Z}/m)$ tienen un divisor común.

Antes de considerar una acción de tipo general, observemos que $\mathbb{Z}/mn = \mathbb{Z}/m \times \mathbb{Z}/n$, si $(m, n) = 1$. Para simplificar nuestros cálculos, aprovechando las propiedades de H^* y H_* con respecto del módulo de coeficientes, resolveremos el caso cuando $m = p^r$ con p primo. En lo sucesivo usaremos los resultados del capítulo anterior.

Caso $p = 2$. Asumamos que $m = 2^r,\ r > 2,\ n = 2^s a,\ s \geqslant 1,\ a$ impar. En este caso, para que $t^n = 1$ es necesario que $t^{2^s} = 1$, por lo que podemos asumir $t = -1$, $t = 5^{2^{r-2-(s-k)}}$, ó $t = -5^{2^{r-2-(s-k)}}$, $0 < s - k \leqslant r - 2$.

Si $t = -1$, $t - 1 = -2$ y así,

$$\ker (t-1) = 2^{r-1}\mathbb{Z}/2^r, \qquad \mathrm{Im}\,(t-1) = 2\mathbb{Z}/2^r;$$

como n es par, $N = 0$ y

$$\ker N = \mathbb{Z}/2^r, \qquad \mathrm{Im}\ N = 0$$

de donde

$$H_1(\mathbb{Z}/n, \mathbb{Z}/2^r) = 2^{r-1}\mathbb{Z}/2^r = \mathbb{Z}/2,$$

$$H_2(\mathbb{Z}/n, \mathbb{Z}/2^r) = \mathbb{Z}/2^r/2\mathbb{Z}/2^r = \mathbb{Z}/2.$$

En general, si el orden de t es c, $n = cd$, el mapeo norma se ve como

$$N = d(1 + t + \cdots + t^{k-1}).$$

Si $t = 5^{2^{r-2-(s-k)}}$, $0 < s - k \leqslant r - 2$, entonces $t \equiv 1 (\mathrm{mod}\, 2^{r-(s-k)})$, $\not\equiv 1 (\mathrm{mod}\, 2^{r-(s-k)+1})$, i.e. $t - 1 = a2^{r-(s-k)}$ con a unidad de $\mathbb{Z}/2^r$. Por eso

$$\ker (t-1) = 2^{s-k}\mathbb{Z}/2^r, \qquad \mathrm{Im}\,(t-1) = 2^{r-(s-k)}\mathbb{Z}/2^r;$$

el orden de t es 2^{s-k}, de donde

$$N = 2^k b(1 + t + \cdots + t^{2^{s-k}-1}),$$

con b unidad, esto es numéricamente igual a

$$2^k b \frac{t^{2^{s-k}} - 1}{t - 1},$$

pero 2^r es la potencia de 2 más grande que divide al numerador y $t-1 = a2^{r-(s-k)}$), por eso

$$N = 2^s b',$$

con b' unidad de $\mathbb{Z}/2^r$. De modo que

$$\ker N = \begin{cases} 2^{r-s}\mathbb{Z}/2^r, & s < r; \\ \mathbb{Z}/2^r & s \geqslant r. \end{cases}, \qquad \operatorname{Im} N = \begin{cases} 2^s\mathbb{Z}/2^r, & s < r; \\ 0 & s \geqslant r. \end{cases}$$

Por lo tanto,

$$H_1(\mathbb{Z}/n, \mathbb{Z}/2^r) = 2^{s-k}\mathbb{Z}/2^r/2^s\mathbb{Z}/2^r = \begin{cases} \mathbb{Z}/2^k, & s < r; \\ \mathbb{Z}/2^{r-(s-k)} & s \geqslant r; \end{cases}$$

$$H_2(\mathbb{Z}/n, \mathbb{Z}/2^r) = 2^{r-s}\mathbb{Z}/2^r/2^{r-(s-k)}\mathbb{Z}/2^r = \begin{cases} \mathbb{Z}/2^k, & s < r; \\ \mathbb{Z}/2^{r-(s-k)} & s \geqslant r. \end{cases}$$

El orden de estos grupos se puede calcular por la fórmula

$$\frac{(t-1, 2^r)(N, 2^r)}{2^r}.$$

Y si $t = -5^{2^{r-2-(s-k)}}$, $0 < s-k \leqslant r-2$, su orden es también $2^{(s-k)}$, sin embargo, como $t \equiv -1 (\mathrm{mod}\, 2^{r-(s-k)})$, $r-(s-k) \geqslant 2$ se tiene que $t-1 = c2$ (c unidad); entonces

$$\ker(t-1) = 2^{r-1}\mathbb{Z}/2^r, \qquad \operatorname{Im}(t-1) = 2\mathbb{Z}/2^r$$

y

$$N = 2^{r+k-1}c' \qquad (c' \text{ unidad}),$$

$$\ker N = \begin{cases} \mathbb{Z}/2^r, & k \geqslant 1; \\ 2\mathbb{Z}/2^r & k = 0; \end{cases}, \qquad \operatorname{Im} N = \begin{cases} 0, & k \geqslant 1; \\ 2^{r-1}\mathbb{Z}/2^r & k = 0. \end{cases}$$

De modo que,

$$H_1(\mathbb{Z}/n, \mathbb{Z}/2^r) = \begin{cases} \mathbb{Z}/2, & k \geqslant 1; \\ 0 & k = 0; \end{cases}$$

$$H_2(\mathbb{Z}/n, \mathbb{Z}/2^r) = \begin{cases} \mathbb{Z}/2, & k \geqslant 1; \\ 0 & k = 0. \end{cases}$$

Caso de un primo impar. Asumamos que el orden de t no divide a p^{r-1} entonces, como se vió, $t-1$ no es divisible por p y por ello es invertible en $\mathbb{Z}/p^r$. Pero sabemos que p^r divide a

$$t^n - 1 = N(t-1),$$

por lo que divide a N. Por lo tanto [3]

$$\ker(t-1) = 0, \qquad \operatorname{Im}(t-1) = \mathbb{Z}/p^r;$$

$$\ker N = \mathbb{Z}/p^r, \qquad \operatorname{Im} N = 0$$

y

$$H_1(\mathbb{Z}/n, \mathbb{Z}/p^r) = H_2(\mathbb{Z}/n, \mathbb{Z}/p^r) = 0.$$

Sea $n = p^s a$, $(a,p) = 1$. Entonces, $t = (1+p)^{p^{r-1-(s-k)}}$, $0 < s-k \leqslant r-1$ y el orden de t es $s-k$. En este caso $p^{r-(s-k)}$ es la potencia de p más grande que divide a $t-1$ y

$$\ker(t-1) = p^{s-k}\mathbb{Z}/p^r, \qquad \operatorname{Im}(t-1) = p^{r-(s-k)}\mathbb{Z}/p^r;$$

ademas

$$N = p^k a \frac{t^{s-k}-1}{t-1} = p^s a'$$

(con a, a' unidades),

$$\ker N = \begin{cases} p^{r-s}\mathbb{Z}/p^r & s < r, \\ \mathbb{Z}/p^r & s \geqslant r; \end{cases}, \qquad \operatorname{Im} N = \begin{cases} p^s\mathbb{Z}/p^r & s < r, \\ 0 & s \geqslant r. \end{cases}$$

Finalmente,

$$H_1(\mathbb{Z}/n, \mathbb{Z}/p^r) = p^{s-k}\mathbb{Z}/p^r / p^s\mathbb{Z}/p^r = \begin{cases} \mathbb{Z}/p^k & s < r, \\ \mathbb{Z}/p^{r-(s-k)} & s \geqslant r; \end{cases}$$

$$H_2(\mathbb{Z}/n, \mathbb{Z}/p^r) = p^{r-s}\mathbb{Z}/p^r / p^{r-(s-k)}\mathbb{Z}/p^r = \begin{cases} \mathbb{Z}/p^k & s < r, \\ \mathbb{Z}/p^{r-(s-k)} & s \geqslant r. \end{cases}$$

En este caso, el orden de estos grupos también se puede calcular por la fórmula

$$\frac{(t-1, p^r)(N, p^r)}{p^r}.$$

En el caso general, debido a que, de acuerdo a nuestros cálculos

$$H^2(\mathbb{Z}/n, \mathbb{Z}/p^r) = H^2(\mathbb{Z}/p^s, \mathbb{Z}/p^r)$$

[3] De aquí es evidente que ninguno de nuestros cálculos depende de la parte caótica de $\varphi(m)$.

y

$$H^2(\mathbb{Z}/n, \mathbb{Z}/m) = \bigoplus_p H^2(\mathbb{Z}/p^s, \mathbb{Z}/p^r)$$

el orden de este grupo se puede calcular mediante la fórmula

$$\frac{(t-1, m)(N, m)}{m}.$$

De lo anterior se siguen dos resultados.

PROPOSICIÓN 1. *Si* $(m, n) = 1$, *entonces la extensión*

$$0 \to \mathbb{Z}/m \to G \to \mathbb{Z}/n \to 0$$

se escinde.

TEOREMA 2. *Sea* $\mathbb{Z}/n$ *el grupo cíclico de orden* n *y* $\mathbb{Z}/m$ *anillo de enteros módulo* m *considerado como* $\mathbb{Z}/n$*-módulo mediante la acción* t. *Entonces,*

$$H_i(\mathbb{Z}/n, \mathbb{Z}/m) \approx H^i(\mathbb{Z}/n, \mathbb{Z}/m) \approx \mathbb{Z}/\left(\frac{(t-1, m)(N, m)}{m}\right)$$

para $i > 0$, *donde*

$$N = 1 + t + \cdots + t^{n-1},$$

además, $n|N$, N/n *es potencia de dos y la potencia es positiva solamente cuando* t *es múltiplo de -1.*

En particular, si la acción es trivial ($t = 1$) *entonces*

$$H_i(\mathbb{Z}/n, \mathbb{Z}/m) \approx H^i(\mathbb{Z}/n, \mathbb{Z}/m) \approx \mathbb{Z}/(n, m)$$

COROLARIO 3. *El número clases de equivalencia de extensiones de la forma*

$$0 \to \mathbb{Z}/m \to G \to \mathbb{Z}/n \to 0$$

es $\frac{(t-1,m)(N,m)}{m}$.

De acuerdo a [?] el multiplicador de Schur $H_2G \approx \mathbb{Z}/l$ y, precisamente, [4]

$$l = \frac{(t-1, m)(N, h)}{m}, \quad \text{con } m|h(t-1),\ h|m.$$

[4] **Precaución:** La multiplicación por cero se interpreta en cualquier caso como multiplicación por m en estas fórmulas.

El número h es un parámetro de la presentación del grupo G y $h = m$ es equivalente a que la extensión sea trivial (G es producto semidirecto), lo cual nos lleva a lo siguiente.

COROLARIO 4. *Si la extensión*

$$0 \to \mathbb{Z}/m \to G \to \mathbb{Z}/n \to 0$$

se escinde, entonces

$$|H^2(\mathbb{Z}/n, \mathbb{Z}/m)| = |H_2G|$$

y esta es la cantidad de $\mathbb{Z}/m$-clases de conjugación de esciciones[5].

Recíprocamente, si $|H^2(\mathbb{Z}/n, \mathbb{Z}/m)| = |H_2G|$, obtenemos $(N, m) = (N, h)$, por eso para asegurar que la extensión es trivial, requerimos de alguna información adicional; por ejemplo $m|n$, ya que esto significa $(m, N) = m$.

COROLARIO 5. *Si $|H^2(\mathbb{Z}/n, \mathbb{Z}/m)| = |H_2G|$ y $m|n$. Entonces la extensión*

$$0 \to \mathbb{Z}/m \to G \to \mathbb{Z}/n \to 0$$

se escinde.

[5]Es decir, el orden de $H^1(\mathbb{Z}/n, \mathbb{Z}/m)$

Bibliografía

[1] Brown, Kenneth S. *Cohomology of groups.* Graduate Texts in Mathematics, 87. Springer-Verlag, New York-Berlin, 1982. x+306 pp. ISBN: 0-387-90688-6

[2] Adem, Alejandro; Milgram, R. James *Cohomology of finite groups.* Grundlehren der Mathematischen Wissenschaften, 309. Springer-Verlag, Berlin, 1994. viii+327 pp. ISBN: 3-540-57025-X

[3] Karpilovsky, Gregory. *The Schur multiplier.* London Mathematical Society Monographs. New Series, 2. The Clarendon Press, Oxford University Press, New York, 1987. x+302 pp. ISBN 0-19-853554-6

[4] Lenstra *Groups, Rings, and Fields.*
http://websites.math.leidenuniv.nl/algebra/topics.pdf

[5] Kasch, F. *Modules and rings.* Translated from the German and with a preface by D. A. R. Wallace. London Mathematical Society Monographs, 17. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1982. xii+372 pp. ISBN: 0-12-400350-8 16-01

[6] Mac Lane, Saunders *Homology* Die Grundlehren der mathematischen Wissenschaften, Bd. 114 Academic Press, Inc., Publishers, New York; Springer-Verlag, Berlin-Gttingen-Heidelberg 1963 x+422 pp.

[7] Hochschild, G.; Serre, J.-P. *Cohomology of group extensions.* Trans. Amer. Math. Soc. 74, (1953). 110–134.

[8] Lyndon, Roger C. *The cohomology theory of group extensions.* Duke Math. J. 15, (1948). 271–292.

[9] Eilenberg, Samuel; MacLane, Saunders *Cohomology theory in abstract groups II. Group extensions with a non-Abelian kernel.* Ann. of Math. (2) 48, (1947). 326–341.

[10] Hopf, Heinz *Fundamentalgruppe und zweite Bettische Gruppe.* (German) Comment. Math. Helv. 14, (1942). 257–309.

[11] W. Hurewicz, *Beitrage zur Topologie der Deformationen IV.* Aspharische Raume, Nederl. Akad. Wetensch. Proc. 39 (1936), 215–224.

[12] O. Schreier, *Uber die Erweiterung von Gruppen I*, Monatsh. Math. Phys. 34 (1926), 165-180.

[13] I. Schur, *Uber die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. 127 (1904), 20–50. Gesammelte Abhandlungen, I, 86–116.

[14] S. Mac Lane *Origins of the cohomology of groups.* Colloquium on Topology and Algebra, abril 1977, Zurich.

[15] Fisher, Benji N.; Rabson, David A. *Applications of group cohomology to the classification of quasicrystal symmetries.* J. Phys. A 36 (2003), no. 40, 10195–10214.