Cohomología de grupos, día 2

Alexey Beshenov (cadadr@gmail.com)

31 de agosto de 2016

1. La resolución barra

Hemos construido ciertas resoluciones de $\mathbb{Z}$ por $\mathbb{Z}[G]$-módulos libres para $G \cong \mathbb{Z}$ y $\mathbb{Z}/m\mathbb{Z}$. Hay una construcción general que funciona para cualquier grupo G.

1.1. Construcción. Para $n \geq 0$ sea

$$G^{n+1} := \underbrace{G \times \cdots \times G}_{n+1}.$$

El anillo $\mathbb{Z}[G^{n+1}]$ es un G-módulo con acción de G por la izquierda

$$g \cdot (g_0, g_1, \ldots, g_n) := (g\,g_0, g\,g_1, \ldots, g\,g_n).$$

Consideremos la sucesión de morfismos de $\mathbb{Z}[G]$-módulos

$$P_\bullet\colon\ \cdots \to \mathbb{Z}[G^{n+2}] \xrightarrow{d_{n+1}} \mathbb{Z}[G^{n+1}] \xrightarrow{d_n} \mathbb{Z}[G^n] \to \cdots \to \mathbb{Z}[G^2] \to \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

donde $P_n := \mathbb{Z}[G^{n+1}]$ y los $d_n\colon P_n \to P_{n-1}$ están definidos como sumas alternadas

$$d_n := \sum_{0 \leq i \leq n} (-1)^i\, \partial_i,$$

de los operadores

$$\partial_i(g_0, \ldots, g_n) := (g_0, \ldots, g_{i-1}, \widehat{g_i}, g_{i+1}, \ldots, g_n).$$

1.2. Observación. *$(P_\bullet, d_\bullet)$ es una sucesión exacta:* $\operatorname{im} d_{n+1} = \ker d_n$.

Demostración. Primero, es un complejo ($d_n \circ d_{n+1} = 0$; es decir, $\operatorname{im} d_{n+1} \subseteq \ker d_n$) gracias a las identidades simpliciales $\partial_i \circ \partial_j = \partial_{j-1} \circ \partial_i$ para $i < j$. Luego, este complejo tiene (co)homología trivial porque es homotópico a cero. Para demostrarlo, tenemos que encontrar una familia de morfismos $h_n\colon P_n \to P_{n+1}$ que satisfagan las identidades

$$d_{n+1} \circ h_n + h_{n-1} \circ d_n = \mathrm{id}_{P_n}.$$

De hecho, podemos poner

$$h_n(g_0, g_1, \ldots, g_n) := (1, g_0, g_1, \ldots, g_n).$$

Luego,

$$\begin{aligned} d_{n+1} \circ h_n(g_0, \ldots, g_n) &= (g_0, \ldots, g_n) - \sum_{0 \leq i \leq n} (-1)^i (1, g_0, \ldots, g_{i-1}, \widehat{g_i}, g_{i+1}, \ldots, g_n) \\ &= (g_0, \ldots, g_n) - h_{n-1} \circ d_n(g_0, \ldots, g_n). \end{aligned}$$

∎

De hecho, este complejo viene de topología algebraica. Noten que la resolución periódica que hemos obtenido para los grupos finitos cíclicos es diferente; la última también proviene de topología, pero usa una idea diferente. Véase [K.S. Brown, Cohomology of Groups, §I.4–I.6].

1.3. Observación. *Los $\mathbb{Z}[G]$-módulos $P_n := \mathbb{Z}[G^{n+1}]$ son libres.*

Demostración. Sobre $\mathbb{Z}$, el módulo $\mathbb{Z}[G^{n+1}]$ está generado por los elementos

$$(*) \qquad (g_0, \ldots, g_n), \quad g_i \in G,$$

pero no es una base sobre $\mathbb{Z}[G]$. Sin embargo, notemos que todo elemento (*) puede ser escrito como

$$(g_0, g_0 g_1, g_0 g_1 g_2, \ldots, g_0 g_1 g_2 \cdots g_n) = g_0 \cdot (1, g_1, g_1 g_2, \ldots, g_1 g_2 \cdots g_n) =: g_0 \cdot [\![g_1 | g_2 | \cdots | g_n]\!]$$

y los elementos $[\![g_1 | g_2 | \cdots | g_n]\!]$ forman una base de $\mathbb{Z}[G^{n+1}]$ sobre $\mathbb{Z}[G]$ (en el caso especial $n = 0$, tenemos $\mathbb{Z}[G]$ con una base que consiste en un elemento $[\![\;]\!]$). ■

Entonces, tenemos una resolución de $\mathbb{Z}$ por $\mathbb{Z}[G]$-módulos libres. Por la notación

$$[\![g_1 | g_2 | \cdots | g_n]\!] := (1, g_1, g_1 g_2, \ldots, g_1 g_2 \cdots g_n)$$

donde los elementos están separados por barras; por ello esta recibe el nombre de **resolución barra**. Calculemos los diferenciales en la base de los símbolos $[\![g_1 | g_2 | \cdots | g_n]\!]$:

$$\partial_i [\![g_1 | g_2 | \cdots | g_n]\!] = \begin{cases} g_1 \cdot [\![g_2 | \cdots | g_n]\!], & i = 0, \\ [\![g_1 | g_2 | \cdots | g_i g_{i+1} | \cdots | g_n]\!], & 0 < i < n, \\ [\![g_1 | g_2 | \cdots | g_{n-1}]\!], & i = n. \end{cases}$$

Entonces,

$$\begin{aligned} d_1 [\![g]\!] &= g \cdot [\![\;]\!] - [\![\;]\!], \\ d_2 [\![g | h]\!] &= g \cdot [\![h]\!] - [\![gh]\!] + [\![g]\!], \\ &\vdots \\ d_n [\![g_1 | g_2 | \cdots | g_n]\!] &= \sum_{0 \le i \le n} (-1)^i \partial_i [\![g_1 | g_2 | \cdots | g_n]\!] \\ &= g_1 \cdot [\![g_2 | \cdots | g_n]\!] + \sum_{1 \le i \le n-1} (-1)^i \, [\![g_1 | g_2 | \cdots | g_i g_{i+1} | \cdots | g_n]\!] + (-1)^n \, [\![g_1 | g_2 | \cdots | g_{n-1}]\!]. \end{aligned}$$

A veces en la literatura se encuentran fórmulas un poco diferentes que corresponden a la **resolución normalizada**. Nuestro complejo $P_\bullet$ contiene un subcomplejo $D_\bullet$ de “símplices degenerados” $(g_0, \ldots, g_n)$ tales que $g_i = g_{i+1}$ para algún i. En la notación barra, tales elementos corresponden a $[\![g_1 | g_2 | \cdots | g_n]\!]$ con $g_i = 1$ para algún i. Tomando el cociente $P_\bullet / D_\bullet$, se obtiene el **complejo normalizado**, que es también una resolución libre de $\mathbb{Z}$, donde los $\mathbb{Z}[G]$-módulos libres están generados por los símbolos $[\![g_1 | \cdots | g_n]\!]$ con $g_i \in G \setminus \{1\}$. Los diferenciales son los mismos, solo que cuando tenemos $\partial_i [\![g_1 | g_2 | \cdots | g_n]\!] = [\![g_1 | \cdots | g_i g_{i+1} | \cdots | g_n]\!]$, el producto $g_i g_{i+1}$ puede ser igual a 1, así que en el complejo normalizado, para $0 < i < n$,

$$\partial_i [\![g_1 | g_2 | \cdots | g_n]\!] = \begin{cases} [\![g_1 | \cdots | g_i g_{i+1} | \cdots | g_n]\!], & g_i g_{i+1} \ne 1, \\ 0, & g_i g_{i+1} = 1. \end{cases}$$

2. Las fórmulas para calcular (co)homología

Gracias a la resolución barra $P_\bullet \twoheadrightarrow \mathbb{Z}$, podemos calcular los grupos de homología y cohomología como

$$\begin{aligned} H_n(G,A) &\cong H_n(P_\bullet \otimes_{\mathbb{Z}[G]} A),\\ H^n(G,A) &\cong H^n(\operatorname{Hom}_{\mathbb{Z}[G]}(P_\bullet, A)). \end{aligned}$$

Podemos hacer explícitos estos complejos y las fórmulas para sus diferenciales.

2.1. Observación.

1) *Sea $C_\bullet(G,A)$ el complejo donde*

$$C_n(G,A) := \{\textit{sumas finitas } \sum_i a_i \otimes [\![g_{i1}|g_{i2}|\cdots|g_{in}]\!] \mid a_i \in A,\ g_{i1},\ldots,g_{in} \in G\}$$

(hemos escrito los coeficientes a_i a la izquierda, considerando A como un $\mathbb{Z}[G]$-módulo por la derecha) y los diferenciales son

$$d_n(a\otimes[\![g_1|g_2|\cdots|g_n]\!]) = (a\cdot g_1)\otimes[\![g_2|\cdots|g_n]\!] - a\otimes[\![g_1\,g_2|g_3|\cdots|g_n]\!] + \cdots + (-1)^n\, a\otimes[\![g_1|\cdots|g_{n-1}]\!].$$

Entonces

$$H_n(G,A) \cong H_n(C_\bullet(G,A)).$$

2) *Sea $C^\bullet(G,A)$ el complejo donde*

$$C^n(G,A) = \{\textit{aplicaciones } f\colon G^n \to A\}$$

y los diferenciales $d^{n-1}\colon C^{n-1}(G,A) \to C^n(G,A)$ son

$$(d^{n-1}f)(g_1,\ldots,g_n) = g_1\cdot f(g_2,\ldots,g_n) - f(g_1\,g_2,\ldots,g_n) + \cdots + (-1)^n\, f(g_1,\ldots,g_{n-1}).$$

Entonces

$$H^n(G,A) \cong H^n(C^\bullet(G,A)).$$

A veces los complejos de arriba se presentan como las *definiciones* de (co)homología de grupos, pero hay que saber que estas fórmulas simplemente provienen de algunas resoluciones específicas.

Usando complejos particulares, se puede dar una demostración breve del siguiente

2.2. Teorema. *Si G es un grupo finito que contiene m elementos, entonces para todo $n > 0$ los grupos $H^n(G,A)$ y $H_n(G,A)$ son aniquilados por m.*

Demostración. Va a ser suficiente considerar la multiplicación por m sobre nuestro complejo $P_\bullet$: este morfismo entre complejos induce la multiplicación por m sobre $H^n(G,A)$ y $H_n(G,A)$. Si el morfismo entre complejos es homotópico a cero, entonces los morfismos inducidos en H^n y H_n son nulos.

Entonces, sea $f_\bullet\colon P_\bullet \to P_\bullet$ el morfismo definido por la multiplicación por m en grados > 0 y multiplicación por $(m-N)$ en grado 0, donde N como siempre denota el elemento de norma $\sum_{g\in G} g$. Definamos una familia de morfismos $h_n\colon P_n \to P_{n+1}$ por

$$h_n[\![g_1|\cdots|g_n]\!] := (-1)^{n+1} \sum_{g\in G} [\![g_1|\cdots|g_n|g]\!].$$

Tenemos que verificar las identidades

$$d_{n+1}\circ h_n + h_{n-1}\circ d_n = f_n.$$

Para $n > 0$ tenemos

$$\begin{aligned} d_{n+1} \circ h_n [\![g_1 | \cdots | g_n]\!] = (-1)^{n+1} \sum_{g \in G} \Big(& g_1 \cdot [\![g_2 | \cdots | g_n | g]\!] + \\ & \sum_{1 \le i \le n-1} (-1)^i \, [\![g_1 | \cdots | g_i g_{i+1} | \cdots | g_n | g]\!] + \\ & (-1)^n \, [\![g_1 | \cdots | g_{n-1} | g_n g]\!] + (-1)^{n+1} [\![g_1 | \cdots | g_n]\!] \Big), \\ h_{n-1} \circ d_n [\![g_1 | \cdots | g_n]\!] = -(-1)^{n+1} \sum_{g \in G} \Big(& g_1 \cdot [\![g_2 | \cdots | g_n | g]\!] + \\ & \sum_{1 \le i \le n-1} (-1)^i \, [\![g_1 | g_2 | \cdots | g_i g_{i+1} | \cdots | g_n | g]\!] + (-1)^n \, [\![g_1 | g_2 | \cdots | g_{n-1} | g]\!] \Big). \end{aligned}$$

Notemos que

$$(d_{n+1} \circ h_n + h_{n-1} \circ d_n) [\![g_1 | \cdots | g_n]\!] = (-1)^{2 \cdot (n+1)} \sum_{g \in G} [\![g_1 | \cdots | g_n]\!] = m \cdot [\![g_1 | \cdots | g_n]\!],$$

ya que los otros términos en las sumas se cancelan (¡estamos sumando sobre todos los elementos de G!). Para $n = 0$ tenemos que verificar la identidad $d_1 \circ h_0 = f_0$. De hecho,

$$d_1 \circ h_0 [\![\;]\!] = d_1 (- \sum_{g \in G} [\![g]\!]) = \sum_{g \in G} ([\![\;]\!] - g \cdot [\![\;]\!]) = (m - N) \cdot [\![\;]\!].$$

■

2.3. Ejemplo (H_1 y abelianización). Consideremos el grupo de homología $H_1(G, \mathbb{Z})$, donde $\mathbb{Z}$ es el $\mathbb{Z}[G]$-módulo trivial. Por nuestras fórmulas,

$$H_1(G, \mathbb{Z}) \cong \frac{\ker(C_1(G, \mathbb{Z}) \xrightarrow{d_1} C_0(G, \mathbb{Z}))}{\operatorname{im}(C_2(G, \mathbb{Z}) \xrightarrow{d_2} C_1(G, \mathbb{Z}))}$$

Los $C_n(G, \mathbb{Z})$ son grupos abelianos libres generados por los símbolos $[\![g_1 | g_2 | \cdots | g_n]\!]$ donde $g_i \in G$. Los primeros diferenciales son

$$\begin{aligned} d_1 [\![g]\!] &= [\![\;]\!] - [\![\;]\!] = 0, \\ d_2 [\![g | h]\!] &= [\![h]\!] - [\![gh]\!] + [\![g]\!], \end{aligned}$$

y en consecuencia $H_1(G, \mathbb{Z})$ es isomorfo al grupo abeliano libre generado por todos los símbolos $[\![g]\!]$ para $g \in G$, módulo las relaciones $[\![h]\!] + [\![g]\!] - [\![gh]\!]$. Esta es precisamente la abelianización de G:

$$H_1(G, \mathbb{Z}) \cong G / [G, G].$$

▲

La fórmula $H_1(G, \mathbb{Z}) \cong G/[G, G]$ es una manifestación del hecho de que para un espacio topológico X, su primer grupo de homología singular $H_1(X; \mathbb{Z})$ es la abelianización del grupo fundamental $\pi_1(X)$ (esto es un caso especial del **teorema de Hurewicz**). De hecho, para todo grupo G existe un espacio topológico BG, llamado su **espacio clasificador** (o el **espacio de Eilenberg–MacLane** $K(G,1)$) tal que BG es conexo y

$$\pi_n(X) \cong \begin{cases} G, & n = 1, \\ 0, & n > 1. \end{cases}$$

Luego, la homología $H_n(G,\mathbb{Z})$ coincide con la homología singular $H_n(BG;\mathbb{Z})$. En realidad, la resolución libre de $\mathbb{Z}$ por $\mathbb{Z}[G]$-módulos que hemos encontrado arriba es simplemente el complejo singular (aumentado por $\epsilon\colon C_0 \to \mathbb{Z}$)

$$\cdots \to C_2(EG) \to C_1(EG) \to C_0(EG) \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

para el espacio recubridor universal de BG, conocido como EG. Por construcción, BG y EG son complejos celulares y el grupo G actúa libremente sobre las células de EG. Para los detalles véase por ejemplo §1.B del libro de Hatcher.

2.4. Ejemplo (Un poco más de topología algebraica). Para $\mathbb{Z}$ el espacio clasificador es la circunferencia $\mathbb{S}^1$ y en general para $\mathbb{Z}^m$ el espacio clasificador es el toro

$$\mathbb{T}^m := \underbrace{\mathbb{S}^1 \times \cdots \times \mathbb{S}^1}_{m}$$

y para el grupo libre F_m generado por m elementos su espacio clasificador es el ramo de circunferencias

$$\underbrace{\mathbb{S}^1 \vee \cdots \vee \mathbb{S}^1}_{m}.$$

Por ejemplo, los grupos de homología del toro $\mathbb{T}^m$ se calculan por la fórmula de Künneth para el producto de espacios $\mathbb{T}^m = \mathbb{T}^{m-1} \times \mathbb{S}^1$:

$$\begin{aligned} H_n(\mathbb{Z}^m,\mathbb{Z}) &\cong H_n(\mathbb{T}^m) \\ &\cong \bigoplus_i H_i(\mathbb{T}^{m-1}) \otimes H_{n-i}(\mathbb{S}^1) \\ &\cong H_n(\mathbb{T}^{m-1}) \otimes H_0(\mathbb{S}^1) \oplus H_{n-1}(\mathbb{T}^{m-1}) \otimes H_1(\mathbb{S}^1) \\ &\cong H_n(\mathbb{T}^{m-1}) \oplus H_{n-1}(\mathbb{T}^{m-1}) \end{aligned}$$

(la circunferencia tiene homología igual a $\mathbb{Z}$ en grados 0 y 1 y nula en otros grados). Se ve que los rangos de los grupos de homología satisfacen la relación del triángulo de Pascal

$$\operatorname{rk} H_n(\mathbb{T}^m) = \operatorname{rk} H_n(\mathbb{T}^{m-1}) + \operatorname{rk} H_{n-1}(\mathbb{T}^{m-1}),$$

así que

$$H_n(\mathbb{Z}^m,\mathbb{Z}) \cong H_n(\mathbb{T}^m) \cong \mathbb{Z}^{\binom{n}{m}}.$$

En el caso de los grupos libres, tenemos

$$H_n(F_m,\mathbb{Z}) \cong H_n(\underbrace{\mathbb{S}^1 \vee \cdots \vee \mathbb{S}^1}_{m}) \cong \begin{cases} \mathbb{Z}, & n = 0, \\ \mathbb{Z}^{\oplus m}, & n = 1, \\ 0, & n > 1. \end{cases}$$

▲

2.5. Ejemplo (H^1 y homomorfismos cruzados). Para un G-módulo A, un **homomorfismo cruzado** (también conocido como **1-cociclo**) $f\colon G \to A$ es una aplicación entre conjuntos que satisface

$$f(gh) = g \cdot f(h) + f(g)$$

para todo $g, h \in G$. Notemos que los homomorfismos cruzados forman un grupo abeliano junto con la adición punto por punto

$$(f_1 + f_2)(g) := f_1(g) + f_2(g).$$

En particular, para todo elemento fijo $a \in A$ la aplicación

$$f_a(g) := g \cdot a - a$$

es un homomorfismo cruzado:

$$f_a(gh) = (gh) \cdot a - a = (gh) \cdot a - g \cdot a + g \cdot a - a = g \cdot f_a(h) + f_a(g).$$

Por nuestras fórmulas,

$$H^1(G, A) \cong \frac{\ker(C^1(G,A) \xrightarrow{d^1} C^2(G,A))}{\operatorname{im}(C^0(G,A) \xrightarrow{d^0} C^1(G,A))}.$$

Los grupos $C^n(G, A)$ están formados por las aplicaciones $f\colon G^n \to A$. Para $n = 0$, tenemos la identificación natural $C^0(G, A) \cong A$. Los primeros diferenciales son

$$\begin{aligned}
(d^0 a)(g) &= g \cdot a - a,\\
(d^1 f)(g,h) &= g \cdot f(h) - f(gh) + f(g),\\
(d^2 f)(g,h,k) &= g \cdot f(h,k) - f(gh,k) + f(g,hk) - f(g,h).
\end{aligned}$$

Y se ve que

$$H^1(G, A) \cong \frac{\text{homomorfismos cruzados}}{\text{homomorfismos de la forma } g \mapsto g \cdot a - a}.$$

En particular, si A es un G-módulo trivial, los homomorfismos cruzados son simplemente homomorfismos de grupos y

$$H^1(G, A) \cong \operatorname{Hom}_{\mathbf{Grp}}(G, A).$$

(De hecho, para cualquier espacio topológico X, el teorema de coeficientes universales nos dice que $H^1(X; A) \cong \operatorname{Hom}_{\mathbb{Z}}(H_1(X; \mathbb{Z}), A) = \operatorname{Hom}_{\mathbf{Grp}}(\pi_1(X), A)$.) ▲

2.6. Ejemplo (El teorema 90 de Hilbert). El primer resultado sobre cohomología de grupos fue descubierto por Hilbert (1897) y es conocido como el **teorema 90**: *si L/K es una extensión finita de Galois, entonces $H^1(\operatorname{Gal}(L/K), L^\times) = \{1\}$.*

Para ver que el grupo $H^1(\operatorname{Gal}(L/K), L^\times)$ es trivial, tenemos que ver que los homomorfismos cruzados $f\colon \operatorname{Gal}(L/K) \to L^\times$, es decir, las aplicaciones que satisfacen

$$f(\sigma\sigma') = \sigma(f(\sigma')) \cdot f(\sigma)$$

para todo $\sigma, \sigma' \in \operatorname{Gal}(L/K)$, son todas de la forma

$$f(\sigma) = \frac{\sigma(a)}{a}$$

para algún $a \in L^\times$. Noten que nuestra notación es multiplicativa.

Un resultado básico que necesitamos es que los automorfismos de L son linealmente independientes: si $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}(L/K)$ son automorfismos distintos y $c_1, \ldots, c_n \in L$ son algunos coeficientes tales que

$$c_1\, \sigma_1(x) + \cdots + c_n\, \sigma_n(x) = 0$$

para todo $x \in L$, entonces $c_1 = \cdots = c_n = 0$. En particular, la combinación lineal

$$\sum_{\sigma \in \mathrm{Gal}(L/K)} f(\sigma) \cdot \sigma \colon L \to L$$

no es cero, ya que $f(\sigma) \neq 0$ para todo $\sigma \in \mathrm{Gal}(L/K)$; es decir, existe algún $b \in L^\times$ tal que

$$\sum_{\sigma \in \mathrm{Gal}(L/K)} f(\sigma) \cdot \sigma(b) \neq 0.$$

Sea a el elemento *inverso* a la suma de arriba. Para todo $\sigma \in \mathrm{Gal}(L/K)$ tenemos

$$\begin{aligned}
\sigma(a)^{-1} = \sigma(a^{-1}) &= \sum_{\sigma' \in \mathrm{Gal}(L/K)} \sigma(f(\sigma')) \cdot \sigma\,\sigma'(b) \\
&= \sum_{\sigma' \in \mathrm{Gal}(L/K)} \frac{f(\sigma\,\sigma')}{f(\sigma)} \cdot \sigma\,\sigma'(b) \\
&= \frac{1}{f(\sigma)} \sum_{\sigma' \in \mathrm{Gal}(L/K)} f(\sigma\,\sigma') \cdot \sigma\,\sigma'(b) \\
&= \frac{1}{f(\sigma)} \sum_{\sigma'' \in \mathrm{Gal}(L/K)} f(\sigma'') \cdot \sigma''(b) = \frac{a^{-1}}{f(\sigma)}.
\end{aligned}$$

Así $f(\sigma) = \frac{\sigma(a)}{a}$. ▲

2.7. Ejemplo. La forma clásica del teorema 90 es un poco diferente, ya que en el siglo XIX no existía la terminología cohomológica. Hilbert demostró lo siguiente: *si L/K es una extensión finita cíclica, entonces todo elemento $b \in L$ de norma $N_{L/K}(b) := \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(b) = 1$ es de la forma $\sigma(a)/a$ para algún $a \in L$ y σ un generador de* $\mathrm{Gal}(L/K)$.

De hecho, si $\mathrm{Gal}(L/K)$ es un grupo cíclico de orden m generado por un elemento σ, entonces $N_{L/K}(b) = 1$ significa que

$$b \cdot \sigma(b) \cdot \sigma^2(b) \cdots \sigma^{m-1}(b) = 1.$$

En consecuencia, $f\colon \mathrm{Gal}(L/K) \to L^\times$ definido por

$$f(\sigma^i) := b \cdot \sigma(b) \cdot \sigma^2(b) \cdots \sigma^{i-1}(b)$$

es un homomorfismo cruzado (1-cociclo). Por el teorema 90 en la forma $H^1(\mathrm{Gal}(L/K), L^\times) = \{1\}$, concluimos que f es de la forma $\sigma^i \mapsto \sigma^i(a)/a$ para algún $a \in L^\times$. En particular, $f(\sigma) = b = \sigma(a)/a$. ▲

El grupo $H^2(\mathrm{Gal}(L/K), L^\times)$ es el **grupo de Brauer relativo** $\mathrm{Br}(L/K)$ y en general no es trivial (hemos visto que $H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times) \cong \mathbb{Z}/2\mathbb{Z}$). Sin embargo, en algunos casos interesantes podemos demostrar que $|H^2(G,A)| = |H^1(G,A)|$:

2.8. Observación. *Si G es un grupo cíclico finito y A es un G-módulo finito, entonces $|H^2(G,A)| = |H^1(G,A)|$.*

Demostración. Recordemos nuestros cálculos de cohomología:

$$H^n(G,A) = \begin{cases} A^G = \ker(A \xrightarrow{t-1} A), & n = 0, \\ \{a \in A \mid N \cdot a = 0\}/(t-1)A, & n > 0 \text{ impar}, \\ A^G/NA, & n > 0 \text{ par}. \end{cases}$$

Aquí t es un generador de G y $N = \sum_{g \in G} g$ es el elemento de norma. Tenemos una sucesión exacta

$$0 \to A^G \to A \xrightarrow{(t-1)} A \to A/(t-1)A \to 0$$

Y entonces

$$\text{(*)} \qquad \frac{|A|}{|A^G|} = |(t-1)A|, \quad \frac{|A|}{|(t-1)A|} = |A/(t-1)A|$$

—esto tiene sentido pues A es finito por nuestra hipótesis. Luego, tenemos una sucesión exacta

$$1 \to H^1(G,A) \to A/(t-1)A \xrightarrow{\overline{N}} A^G \to H^2(G,A) \to 0$$

de la cual deducimos que

$$|H^2(G,A)| = \frac{|A^G|}{|\operatorname{im} \overline{N}|}, \quad \frac{|A/(t-1)A|}{|H^1(G,A)|} = |\operatorname{im} \overline{N}|.$$

Pero $|A^G| = |A/(t-1)A|$ por las ecuaciones (*), y por lo tanto $|H^2(G,A)| = |H^1(G,A)|$. ■

2.9. Ejemplo. Si $K = \mathbb{F}_q$ es un cuerpo finito, y L/K es una extensión finita, el grupo de Galois $\operatorname{Gal}(L/K)$ es cíclico y por la observación de arriba

$$\operatorname{Br}(L/K) := H^2(\operatorname{Gal}(L/K), L^\times) = H^1(\operatorname{Gal}(L/K), L^\times).$$

Pero el último grupo es trivial por el teorema 90. De hecho,

$$\operatorname{Br}(K) := \varinjlim_{\substack{L/K \\ \text{ext. finita de Galois}}} H^2(\operatorname{Gal}(L/K), L^\times) = H^2(K^{\text{sep}}/K, (K^{\text{sep}})^\times)$$

recibe el nombre de **grupo de Brauer absoluto** de K, y hemos calculado que $\operatorname{Br}(\mathbb{F}_q) = 0$. Esta no es sino una manifestación del **pequeño teorema de Wedderburn**: *todo anillo de división finito es automáticamente un cuerpo.* ▲

Para mayor información sobre H^1, H^2 y el grupo de Brauer, recomiendo el libro P. Gille, T. Szamuely, "Central Simple Algebras and Galois Cohomology".