Cohomología de grupos, día 3

Alexey Beshenov (cadadr@gmail.com)

1 de septiembre de 2016

1. Extensiones de grupos

1.1. Definición. Una **extensión** de grupo G por A es una sucesión exacta corta

$$0 \to A \to E \to G \to 1$$

Se dice que dos extensiones son **equivalentes** si hay un morfismo $E \to E'$ que forma parte de un diagrama conmutativo de filas exactas

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, equal] & 1 \\
0 \arrow[r] & A \arrow[r] & E' \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

Como siempre, A denota un grupo abeliano (por esto a la izquierda escribimos "$0 \to$"; la operación en A va a ser denotada por $+$) y G denota un grupo no necesariamente abeliano —la razón es que la teoría de extensiones de núcleo no abeliano es demasiado sofisticada para nuestros apuntes.

Notemos que $E \to E'$ en el diagrama de arriba es necesariamente un isomorfismo por el lema del cinco (que se cumple también para grupos no necesariamente abelianos —trate de demostrarlo). En particular, tenemos una verdadera relación de equivalencia.

1.2. Observación. *Si tenemos una extensión*

$$0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$$

entonces G actúa sobre A, y la acción puede ser descrita como

$$i(g \cdot a) = \widetilde{g}\, i(a)\, \widetilde{g}^{-1}, \quad \text{donde } \widetilde{g} \in E \text{ es tal que } p(\widetilde{g}) = g.$$

2. Extensiones escindidas y $H^1(G, A)$

2.1. Definición. Se dice que una extensión

$$0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$$

se escinde si existe un homomorfismo de grupos $s\colon G \to E$ tal que $p \circ s = \mathrm{id}_G$.

Notemos que si la extensión se escinde, entonces como un conjunto, E se identifica con el producto cartesiano $A \times G$, y la biyección entre conjuntos $A \times G \xrightarrow{\cong} E$ es dada por $(a, g) \mapsto i(a)\, s(g)$. La multiplicación de tales pares no es necesariamente la multiplicación $(a, g) \cdot (b, h) = (ab, gh)$, ya que es "torcida" por la acción de G sobre A. A saber, tenemos

$$i(a)\, s(g)\, i(b)\, s(h) = i(a)\, \underbrace{s(g)\, i(b)\, s(g)^{-1}}\, s(g)\, s(h) = i(a)\, i(g \cdot b)\, s(g)\, s(h) = i(a + g \cdot b)\, s(gh).$$

Entonces, en términos de pares $(a, g) \in A \times G$, la multiplicación es

$$(a, g) \cdot (b, h) = (a + g \cdot b, gh).$$

Esta construcción recibe un nombre especial:

2.2. Definición. Sea A un grupo con acción de otro grupo G. Entonces el **producto semidirecto** $A \rtimes G$ es el conjunto $A \times G$ con operación $(a, g) \cdot (b, h) := (a + g \cdot b, gh)$.

Se puede verificar fácilmente que esta operación es asociativa y define una estructura de grupo sobre el conjunto $A \times G$. Estas consideraciones nos dan la siguiente

2.3. Observación. *Una extensión se escinde si y solamente si es equivalente a*

$$0 \to A \xrightarrow{a \mapsto (a,1)} A \rtimes G \xrightarrow{(a,g) \mapsto g} G \to 1$$

2.4. Ejemplo. Si la acción de G sobre A es trivial, entonces $A \rtimes G$ coincide con el producto directo de grupos $A \times G$. ▲

2.5. Ejemplo. El grupo $\mathbb{Z}/2\mathbb{Z}$ actúa sobre $\mathbb{Z}/n\mathbb{Z}$ por $[x] \mapsto [-x]$. El producto semidirecto correspondiente $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ es el **grupo diédrico** D_n (que a veces también se denota por D_{2n}). ▲

Ya que la sección $s\colon G \to E$ tiene que cumplir $p \circ s = \mathrm{id}_G$, esta corresponde a una aplicación $f\colon G \to A$ tal que $s(g) = (f(g), g)$. No cualquier aplicación $f\colon G \to A$ da lugar a una sección ya que s tiene que ser un homomorfismo de grupos. Veamos cuál es la condición correspondiente sobre f: si $s\colon g \mapsto (f(g), g)$, entonces la identidad $s(gh) = s(g)\, s(h)$ corresponde a

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

Esto quiere decir que las secciones corresponden a los **morfismos cruzados** (también conocidos como **1-cociclos**) $f\colon G \to A$ tales que

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

(es decir, f es un homomorfismo cruzado por la acción de G). Notemos que los morfismos cruzados forman un grupo abeliano respecto a la adición punto por punto $(f + f')(g) := f(g) + f'(g)$.

2.6. Definición. Para una sucesión escindida $0 \to A \to E \to G \to 1$, se dice que dos secciones $s, s'\colon G \to E$ son **conjugadas** si $s'(g) = i(a)\, s(g)\, i(a)^{-1}$ para algún $a \in A$.

Notemos que en términos de los morfismos cruzados, la identidad $s'(g) = i(a)\, s(g)\, i(a)^{-1}$ puede ser escrita como

$$(f'(g), g) = (a, 1) \cdot (f(g), g) \cdot (a^{-1}, 1) = (a + f(g) - g \cdot a, g).$$

Es decir, dos secciones s y s' son conjugadas si y solamente si los morfismos cruzados f y f' están relacionados como $f(g) - f'(g) = g \cdot a - a$.

Nuestras consideraciones dicen que las secciones módulo conjugación corresponden a los homomorfismos cruzados módulo homomorfismos cruzados de la forma $g \mapsto g \cdot a - a$ para algún $a \in A$. Recordemos el complejo estándar que calcula la cohomología $H^\bullet(G, A)$:

$$0 \to C^0(G,A) \xrightarrow{d^0} C^1(G,A) \xrightarrow{d^1} C^2(G,A) \to \cdots$$

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

Se ve que los homomorfismos cruzados $f\colon G \to A$ con precisamente los que están en $\ker d^1$ y los homomorfismos cruzados de la forma $g \mapsto g \cdot a - a$ son los que están en $\operatorname{im} d^0$. Así que el primer grupo de cohomología $H^1(G,A) \cong \ker d^1 / \operatorname{im} d^0$ clasifica precisamente las posibles secciones de extensiones escindidas módulo conjugación.

2.7. Teorema. *Para una extensión escindida*

$$0 \to A \to A \rtimes G \to G \to 1$$

las secciones $s\colon G \to E$ módulo conjugación corresponden a los elementos de $H^1(G,A)$.

2.8. Ejemplo. Hay dos acciones de $\mathbb{Z}/2\mathbb{Z}$ sobre $\mathbb{Z}/3\mathbb{Z}$: la acción trivial y la acción por $[1] \mapsto [2]$ y $[2] \mapsto [1]$.

- La acción trivial surge en la extensión escindida

  $$0 \to \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

  y hay una sola posible sección $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

- La acción no trivial surge en otra extensión escindida

  $$0 \to \mathbb{Z}/3\mathbb{Z} \to S_3 \to \mathbb{Z}/2\mathbb{Z} \to 0$$

  S_3 contiene un subgrupo normal único isomorfo a $\mathbb{Z}/3\mathbb{Z}$: es el subgrupo que consiste en $(\ )$, $(1,2,3)$, $(1,3,2)$. Luego, hay tres posibles secciones $\mathbb{Z}/2\mathbb{Z} \to S_3$:

  $$s_1\colon 1 \mapsto (1,2), \quad s_2\colon 1 \mapsto (1,3), \quad s_3\colon 1 \mapsto (2,3),$$

  pero todas estas secciones son conjugadas ya que

  $$(1,3) = (1,2,3) \circ (1,2) \circ (1,2,3)^{-1} \quad \text{y} \quad (2,3) = (1,3,2) \circ (1,2) \circ (1,3,2)^{-1}.$$

Todo esto concuerda con el hecho de que $H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z})$ sea trivial para ambas acciones de $\mathbb{Z}/2\mathbb{Z}$ sobre $\mathbb{Z}/3\mathbb{Z}$ (véase nuestro cálculo general de $H^n(\mathbb{Z}/m\mathbb{Z}, A)$). ▲

3. Extensiones y $H^2(G,A)$

Ahora sea

$$0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$$

una extensión no necesariamente escindida. Ya no tenemos secciones, pero todavía existe una *aplicación entre conjuntos* $s\colon G \to E$ tal que $p \circ s = \mathrm{id}_G$. El qué tan alejada está esta aplicación de ser un homomorfismo de grupos es medida por cierta aplicación $f\colon G \times G \to A$:

$$s(g)\, s(h) = i(f(g,h))\, s(gh).$$

Sería natural exigir

$$s(1) = 1, \text{ en particular } f(g,1) = f(1,h) = 0.$$

Tenemos una biyección $A \times G \xrightarrow{\cong} E$ definida por $(a,g) \mapsto i(a)\, s(g)$. Luego,

$$\begin{aligned} i(a)\, s(g)\, i(b)\, s(h) &= i(a)\, \underbrace{s(g)\, i(b)\, s(g)^{-1}}\, s(g)\, s(h) \\ &= i(a)\, i(g\cdot b)\, s(g)\, s(h) \\ &= i(a+g\cdot b)\, i(f(g,h))\, s(gh) \\ &= i(a+g\cdot b+f(g,h))\, s(gh). \end{aligned}$$

Luego el grupo E consiste en pares (a,g) junto con una multiplicación definida por

$$(a,g)\cdot(b,h) = (a+g\cdot b+f(g,h), gh).$$

Si comenzamos con una aplicación $f\colon G \times G \to A$, la operación de arriba sobre $A \times G$ no define una estructura de grupo porque no es asociativa. Se calcula que

$$\begin{aligned} ((a,g)\cdot(b,h))\cdot(c,k) &= (a+g\cdot b+f(g,h),\, gh)\cdot(c,k) = (a+g\cdot b+f(g,h)+gh\cdot c+f(gh,k),\, ghk), \\ (a,g)\cdot((b,h)\cdot(c,k)) &= (a,g)\cdot(b+h\cdot c+f(h,k), hk) = (a+g\cdot b+gh\cdot c+g\cdot f(h,k)+f(g,hk), ghk), \end{aligned}$$

así que para que la multiplicación sea asociativa, f tiene que satisfacer la identidad

$$g\cdot f(h,k) - f(gh,k) + f(g,hk) - f(g,h) = 0. \tag{1}$$

Tal función f recibe el nombre de **2-cociclo**. Ahora una verificación rutinaria demuestra que una aplicación $f\colon G \to G \to A$ tal que $f(g,1) = f(1,h) = 0$ y que cumple la condición de 2-cociclo (1) junto con una acción de G sobre A produce un grupo E a partir de la multiplicación $(a,g)\cdot(b,h) = (a+g\cdot b+f(g,h), gh)$.

Hemos producido un 2-cociclo normalizado $f\colon G \times G \to A$ a partir de una sección normalizada $s\colon G \to E$. Tenemos que ver cómo están relacionados los cociclos f y f' que corresponden a dos secciones normalizadas s, s' de la misma extensión. Así que consideremos una aplicación f' tal que $s'(g)\, s'(h) = i(f'(g,h))\, s'(gh)$. Sea $u\colon G \to A$ la aplicación que expresa la diferencia entre s y s':

$$s'(g) = i(u(g))\, s(g).$$

La normalización $s'(1) = s(1) = 1$ implica que $u(1) = 1$. Tenemos

$$
\begin{aligned}
i(f'(g,h))\, s'(g\,h) = s'(g)\, s'(h) &= i(u(g))\, s(g)\, i(u(h))\, s(h) \\
&= i(u(g))\, \underbrace{s(g)\, i(u(h))\, s(g)^{-1}}\, s(g)\, s(h) \\
&= i(u(g))\, i(g\cdot u(h))\, s(g)\, s(h) \\
&= i(u(g) + g\cdot u(h))\, i(f(g,h))\, s(g\,h) \\
&= i(u(g) + g\cdot u(h) + f(g,h))\, s(g\,h) \\
&= i(u(g) + g\cdot u(h) + f(g,h))\, i(u(gh))^{-1}\, i(u(gh))\, s(g\,h) \\
&= i(u(g) + g\cdot u(h) + f(g,h) - u(gh))\, s'(g\,h).
\end{aligned}
$$

Así que

$$f'(g,h) - f(g,h) = g\cdot u(h) - u(gh) + u(g).$$

Entonces, diferentes 2-cociclos normalizados corresponden a la misma extensión cuando la diferencia entre ellos es de la forma

$$(g,h) \mapsto g\cdot u(h) - u(gh) + u(g). \tag{2}$$

Tales funciones se llaman **2-cofronteras** normalizadas. Nos queda notar que los 2-cociclos normalizados son precisamente $\ker d^2$ en el complejo normalizado $C^\bullet(G,A)$ y las 2-cofronteras normalizadas son precisamente $\operatorname{im} d^1$ en el complejo normalizado. El complejo normalizado, tal y como el complejo habitual, calcula $H^\bullet(G,A)$.

3.1. Teorema. *Las clases de equivalencia de extensiones $0 \to A \to E \to G \to 1$ que dan lugar a una acción fija de G sobre A corresponden a los elementos de $H^2(G,A)$.*

3.2. Ejemplo. El grupo de cohomología $H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z})$ es trivial para ambas acciones de $\mathbb{Z}/2\mathbb{Z}$ sobre $\mathbb{Z}/3\mathbb{Z}$. La acción trivial nos da la extensión $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, mientras que la acción no trivial nos da la extensión S_3. ▲

3.3. Ejemplo (Álgebras con productos cruzados; Emmy Noether). Sea L/K una extensión de Galois. Todo elemento de $H^2(\operatorname{Gal}(L/K), L^\times)$ es representado por un 2-cociclo normalizado $f\colon \operatorname{Gal}(L/K)\times\operatorname{Gal}(L/K) \to L^\times$. A saber, es una colección de elementos $\{\alpha_{\sigma,\tau} \in L^\times\}_{\sigma,\tau\in\operatorname{Gal}(L/K)}$ que satisfacen la condición

$$\sigma(k_{\tau,\rho})\cdot k_{\sigma\tau,\rho}^{-1}\cdot k_{\sigma,\tau\rho}\cdot k_{\sigma,\tau}^{-1} = 1 \tag{3}$$

(es la misma fórmula que (1), solo en la notación multiplicativa) con normalización

$$k_{\sigma,1} = k_{1,\sigma} = 1.$$

Sea A el espacio vectorial sobre L con base de elementos e_σ para $\sigma \in \operatorname{Gal}(L/K)$. Definamos una multiplicación sobre A por

$$\left(\sum_{\sigma\in\operatorname{Gal}(L/K)} a_\sigma\, e_\sigma\right)\cdot\left(\sum_{\tau\in\operatorname{Gal}(L/K)} a_\tau\, e_\tau\right) := \sum_{\sigma,\tau\in\operatorname{Gal}(L/K)} k_{\sigma,\tau}\, a_\sigma\, \sigma(b_\tau)\, e_{\sigma\tau}.$$

Una verificación tediosa demuestra que gracias a (3), la multiplicación es asociativa. La identidad respecto a esta multiplicación es e_1. Notemos que A es también un espacio vectorial sobre K, y tenemos

$$\alpha(x\,y) = (\alpha\,x)\,y = x\,(\alpha\,y) \quad \text{para cualesquiera } x,y\in A, \alpha\in K.$$

El álgebra sobre K que hemos construido se llama un **álgebra con producto cruzado** y se denota por $A = (L/K, \{k_{\sigma,\tau}\})$. Notemos que para el cociclo trivial con $k_{\sigma,\tau} = 1$ para todo $\sigma, \tau \in \mathrm{Gal}(L/K)$, el álgebra con producto cruzado $(L/K, \{k_{\sigma,\tau}\})$ es simplemente el álgebra $M_n(K)$ de matrices de $n \times n$ sobre $\mathbb{K}$.

Resulta que el grupo de cohomología $H^2(\mathrm{Gal}(L/K), L^\times)$ clasifica precisamente tales álgebras:

$$\mathrm{Br}(L/K) \cong H^2(\mathrm{Gal}(L/K), L^\times) \cong \{\text{álgebras con producto cruzado } (L/K, \{k_{\sigma\tau}\})\}/\text{isomorfismo}.$$

Para mayores detalles, véase el capítulo II del libro *N. Jacobson, "Finite-dimensional division algebras over fields"*.

Para dar un ejemplo no trivial de esta construcción, recordemos que nuestro cálculo que $H^2(\mathbb{C}/\mathbb{R}, \mathbb{C}^\times) \cong \mathbb{Z}/2\mathbb{Z}$. Sea σ la conjugación compleja $\mathbb{C}^\times \to \mathbb{C}^\times$. En este caso, un 2-cociclo normalizado está definido por un número $k_{\sigma,\sigma} \in \mathbb{C}^\times$, pues el resto está definido por las condiciones de normalización

$$k_{1,1} = k_{\sigma,1} = k_{1,\sigma} = 1.$$

Las condiciones (3) son casi todas vacías, excepto el caso de los índices σ, σ, σ cuando tenemos la identidad $\sigma(k_{\sigma\sigma}) \cdot k_{\sigma\sigma}^{-1} = 1$; es decir, $k_{\sigma\sigma} \in \mathbb{R}^\times$.

Un momento de reflexión sobre la fórmula (2) para las 2-cofronteras nos dice que estas son de la forma

$$k_{\sigma,\sigma} = \bar{z}\, z = |z|^2 \quad \text{para algún } z \in \mathbb{C}^\times.$$

Entonces, dos cociclos normalizados representan el mismo elemento de $H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times)$ si y solamente si la diferencia entre $k_{\sigma\sigma}$ y $k'_{\sigma\sigma}$ es un factor positivo $x \in \mathbb{R}_{>0}$. Así que, módulo las 2-cofronteras, hay dos posibilidades distintas: $k_{\sigma\sigma} = 1$ (el cociclo trivial) y $k_{\sigma\sigma} = -1$ (el cociclo no trivial).

El cociclo trivial nos da el álgebra de matrices $M_2(\mathbb{R})$. A partir del cociclo con $k_{\sigma\sigma} = -1$ se construye un álgebra sobre $\mathbb{C}$ con una base de dos elementos $\mathbf{1}, \mathbf{j}$ y multiplicación

$$\mathbf{1} \cdot \mathbf{1} = \mathbf{1}, \; \mathbf{1} \cdot \mathbf{j} = \mathbf{j} \cdot \mathbf{1} = \mathbf{j}, \; \mathbf{j} \cdot \mathbf{j} = -\mathbf{1}.$$

Sobre $\mathbb{R}$, esta es un álgebra asociativa de dimensión 4, y es exactamente el **álgebra de cuaterniones** $\mathbb{H}$. Recordemos que normalmente $\mathbb{H}$ se define como el álgebra sobre $\mathbb{R}$ con una base $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ y multiplicación

	1	**i**	**j**	**k**
1	**1**	**i**	**j**	**k**
i	**i**	−**1**	+**k**	−**j**
j	**j**	−**k**	−**1**	+**i**
k	**k**	+**j**	−**i**	−**1**

Para ver que es un álgebra sobre $\mathbb{C}$ con una base $\mathbf{1}, \mathbf{j}$, basta notar que

$$a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} = (a + b\,\mathbf{i}) + (c + d\,\mathbf{i}) \cdot \mathbf{j}.$$

▲