SOBRE LOS GRUPOS DE AUTOMORFISMOS

por

Garrett Birkhoff

Es bien conocido que *los automorfismos de cada álgebra abstracta forman un grupo*. Nuestro objeto es demostrar tres recíprocas de esta proposición.

Recordamos el teorema de Cayley, que dice que cada grupo G es isomorfo al grupo de sus traslaciones *a la derecha*

$$(1) \qquad T_a: \; x \longrightarrow x T_a = xa.$$

Recordamos también que las traslaciones a la derecha de G son las transformaciones permutables (¹) con las traslaciones a la izquierda $x \longrightarrow bx$ de G. Es decir, que son los *automorfismos* del álgebra abstracta G, cuyos *elementos* son los elementos de G, y cuyas operaciones son las operaciones unitarias

$$(2) \qquad U_b: \; x \longrightarrow bx.$$

Porque decir que ϑ es homomórfico con respecto a U_b, es decir que $\vartheta(x U_b) = \vartheta(x) U_b$, que es decir que ϑ y U_b son permutables. Obtenemos de esta manera casi trivial, el teorema siguiente:

Teorema 1. - *Cada grupo abstracto G con x elementos es isomorfo con el grupo de todos los automorfismos de un álgebra abstracta G de α elementos y α operaciones unitarias.*

Entonces construiremos de G un sistema parcialmente ordenado X con $\alpha^2 + \alpha$ elementos, y con un grupo de automorfismos isomorfo a G. Los elementos de X son los $g \varepsilon G$ y los pares (g, g_τ) con $g \varepsilon G$, $g_\tau \varepsilon G$. Para *ordenar* X, supondremos que los elementos de G son «bien ordenados»:

(¹) Cr. por ejemplo Miller, Blichfeldt y Dickson, ''*Theory and Applications of Finite Groups*''. Para los conceptos de álgebra abstracta, sistema parcialmente ordenado, y ''red'' cr. el ''*Lattice Theory*'' del autor, pp. 2, 5, 16.

$$G = \{ e = g_1, g_2, g_3, \ldots, g_\omega, g_{\omega+1}, \ldots \}$$

y escribiremos, para cada $g \varepsilon G$,

$$(3) \qquad g > (g, g_1) > (g, g_2) > \ldots > (g, g_\omega) > (g, g_{\omega+1}) > \ldots$$

Así subdividimos X en α cadenas maximales sin elementos comunes. Escribiremos también

$$(4) \qquad g > (g_\tau g, g_\tau) > (g_\tau g, g_{\tau+1}) > (g_\tau g, g_{\tau+2}) > \ldots$$

de manera que $(g, g_1) \not> (h, g_2)$ si $g \neq h$. Es fácil ver que X es un sistema parcialmente ordenado con respecto a (3) y (4).

Es fácil ver también que las transformaciones

$$(5) \qquad \alpha_a\colon \; g \longrightarrow ga, \;\; (g, g_\tau) \longrightarrow (ga, g_\tau)$$

y sus inversas $\alpha_a{-1}$ conservan (3) y (4). De donde se sigue que el grupo A de los α_a, que es isomorfo con G, es un subgrupo del grupo de todos los automorfismos de G. Recíprocamente, sea α algún automorfismo de X, y sea $a = \alpha(e)$. Es fácil demostrar que α permuta las cadenas maximales (3). En efecto, permuta los elementos g maximales; ya que (g, g_1) es el único elemento $x < g$ y no menor que ningún otro elemento, $\alpha(g, g_1) = (\alpha(g), g_1)$; en general, puesto que $(g, g_{\tau+1}$ es el elemento $x < (g, g_\tau)$ más grande, se demuestra por inducción transfinita que $\alpha(g, g_\tau) = (\alpha(g), g_\tau)$. Falta por demostrar que $\alpha(g) = ga$. Pero (e, g_τ^{-1}) es por (4) el elemento más grande de la cadena (e, g_σ) contenido en (e, g_τ); sigue que $(\alpha(e)\, g_\tau^{-1}) = (a, g_\tau^{-1})$ es el elemento más grande de la cadena (a, g_σ) contenido en $(\alpha(e, g_\tau)$, y por (4) queda $a = g_\tau^{-1}\, \alpha(g)$ o $\alpha(g_\tau) = g_\tau a$. Así se completa la demostración, y podemos afirmar el teorema siguiente:

Teorema 2. - *Cada grupo abstracto G con α elementos es isomorfo con el grupo de todos los automorfismos de un sistema parcialmente ordenado X de $\alpha^2 + \alpha$ elementos.*

Esta construcción tiene la ventaja de que X no posee más que una relación y ninguna operación. Sin embargo X no es «álgebra abstracta» en el sentido usual [1], y la demostración usa el Axioma de Selección. Vamos a ver cómo podemos eliminar la primera desventaja.

Teorema 3. - *Cada grupo abstracto G con α elementos es isomorfo con el grupo de todos los automorfismos de una red distributiva («distributive lattice») B^X con a lo más $2^{\alpha^2+\alpha}$ elementos.*

Demostración. Sea B^X el conjunto de todas las funciones unívocas con dominio X y valores 0 o 1, tales que $x \leqq x'$ en X implica $f(x) \leqq f(x')$ (es decir, funciones no decrecientes). Es fácil ver que si definimos

$$(6) \qquad f \leqq g \text{ significa } f(x) \leqq g(x) \text{ para toda } x,$$

este B^X llega a ser una red distributiva [2]. Ya que la definición de B^X es abstracta, es evidente que cada automorfismo α: $x \rightarrow x\alpha$ de X induce un automorfismo $f(x) \rightarrow f(x\alpha)$ sobre B^X. A causa del Teorema 2, el Teorema 3 estará demostrado si podemos demostrar que B^X no tiene ningún otro automorfismo.

Consideremos la clase $X^* \leqq B^X$ de todas las funciones

$$(7) \qquad f_a(x) = \begin{cases} 1 & \text{si } x \geqq a \\ 0 & \text{si no } x \geqq a. \end{cases}$$

Son las únicas funciones tales que la unión g de todas las $f < f_a$ de B^X satisface $g < f_a$ (en efecto, $g(x) = 1$ si $x > a$, $g(x) = 0$ si $x \not> a$). Se sigue de aquí que cada automorfismo α de B^X permuta los elementos de X isomórficamente — es decir, ya que X^* es dualmente isomórfico con X, como un automorfismo $\bar{\alpha}$ de B^X inducido por un automorfismo de X. Además. cada $f \varepsilon B^X$ puede ser representado únicamente como una unión

$$(8) \qquad f = \vee f_a \text{ para las } a \text{ tales que } f(a) = 1,$$

de elementos de X^*. De aquí se sigue que α permuta los $f \varepsilon B^X$ de la misma manera que $\bar{\alpha}$, lo que completa la demostración.

Sería interesante demostrar los Teoremas 2 - 3 sin usar el Axioma de Selección, y también de reducir las constantes α, $\alpha^2 + \bar{\alpha}$, y $2^{\alpha^2+\alpha}$ en los Teoremas 1, 2, 3 respectivamente

HARVARD UNIVERSITY

(2) Cr. "*An extended Arithmetic*", por G. Birkhoff, Duke Jour. Math. 3 (1937), 311-16.