Miscelánea Matemática **40** (2004) 1–9 SMM

Un panorama del álgebra universal

Simone Hazan
simhazan@prodigy.net.mx

Resumen

En este artículo panorámico, presentamos conceptos de base del álgebra universal tales como definiciones fundamentales y teoremas de homomorfismos. Damos los rudimentos de la teoría de retículos, el teorema HSP de Garrett Birkhoff sobre clases ecuacionales, y mencionamos tres áreas de investigación del álgebra universal.
Clasificación del AMS (2000): 08-02, 06B05.

1. Introducción.

Al final del siglo XIX, las matemáticas disponían de una variedad de estructuras algebraicas tales como grupos, álgebras de Lie, espacios vectoriales, álgebras de Boole, etc. En 1898 apareció el libro de Whitehead *A Treatise on Universal Algebra* ([9]), cuyo autor trataba de unificar todas esas estructuras por medio de una teoría ecuacional. Sin embargo, los conceptos del álgebra universal tal como la conocemos hoy día tardaron otros treinta años para ser descubiertos. Algunos de ellos se encuentran implícitos en el manual de Van der Waerden *Moderne Algebra* ([8], 1931), pero quien empezó a desarollar el campo de manera más formal fue Birkhoff ([1], [2], 1933-1935).

En este artículo presentamos los conceptos básicos de este campo muy activo de las matemáticas (Sección 2), así como del subcampo que constituye la teoría de retículos (Sección 3). En la Sección 4, enunciamos el Teorema HSP de Birkhoff, y la última sección está dedicada a tres áreas recientes de investigación.

Todas las notaciones usadas se pueden encontrar en [6].

2. Conceptos básicos.

Definición 2.1. Un *álgebra* (*universal*) es una pareja $\mathbf{A} = \langle A, f_i(i \in I)\rangle$ donde A es un conjunto no vacío llamado *universo* del álgebra, y cada f_i es una *operación n_i-aria* o *de rango n_i* sobre A, es decir una función de A^{n_i} a A, con $n_i \geq 0$. Cuando n_i es igual a cero, la operación es simplemente una constante, y se le llama operación *nularia*. Para operaciones de rango uno, dos y tres, decimos *unaria*, *binaria* y *ternaria* respectivamente.

Nótese que $\mathbf{A}$ denota un álgebra, mientras que A es un simple conjunto.

El *tipo* del álgebra $\mathbf{A}$ es la familia de sus rangos $\langle n_i, i \in I\rangle$. Dos álgebras son *similares* si tienen el mismo tipo.

Ejemplos. 1) Un grupo es un álgebra $\mathbf{G} = \langle G, ., ^{-1}, e\rangle$ de tipo $\langle 2, 1, 0\rangle$ que satisface, para todos $x, y, z \in G$, las *ecuaciones*

(i) $x.(y.z) = (x.y).z$ (asociatividad),

(ii) $x.e = e.x = x$ (e es neutro para el producto),

(iii) $x.x^{-1} = x^{-1}.x = e$ (x^{-1} es el inverso multiplicativo de x).

2) Un espacio vectorial es un álgebra $\mathbf{V} = \langle V, +, -, 0, f_\lambda, (\lambda \in K)\rangle$ tal que $\langle V, +, -, 0\rangle$ es un grupo abeliano, las f_λ son operaciones unarias indexadas por un campo K y se cumplen las siguientes ecuaciones para todos $x, y \in V$ y $\alpha, \beta \in K$:

(i) $f_1(x) = x$,

(ii) $f_\alpha(x + y) = f_\alpha(x) + f_\alpha(y)$,

(iii) $f_{\alpha+\beta}(x) = f_\alpha(x) + f_\beta(x)$,

(iv) $f_{\alpha\beta}(x) = f_\alpha(f_\beta(x))$.

Definición 2.2. Sea $\mathbf{A} = \langle A, f_i(i \in I)\rangle$ un álgebra. Un *subuniverso* de $\mathbf{A}$ es un subconjunto U de A que es *cerrado* bajo las operaciones del álgebra, i.e. para toda operación n_i-aria f_i y todos $u_0, ..., u_{n_{i-1}} \in U$, tenemos $f(u_0, ..., u_{n_{i-1}}) \in U$.

Si U es un subuniverso no vacío de $\mathbf{A}$, se dice que $\mathbf{U} = \langle U, f_i|_{U^{n_i}}\rangle$ es una *subálgebra* de $\mathbf{A}$. Claramente, $\mathbf{U}$ tiene el mismo tipo que $\mathbf{A}$.

Sea $\langle \mathbf{A}_j(j \in J)\rangle$ una familia de álgebras similares. El *producto* $\mathbf{A} = \prod_J \mathbf{A}_j$ de la familia es el álgebra de mismo tipo cuyo universo es el producto de los conjuntos A_j y en el cual las operaciones están definidas por $f_i(\langle a_0^j\rangle_{j\in J}, ..., \langle a_{n_i-1}^j\rangle_{j\in J}) = \langle f(a_0^j, ..., a_{n_i-1}^j)\rangle_{j\in J}$.

Una *congruencia* de $\mathbf{A}$ es una relación de equivalencia sobre A que, vista como subconjunto de A^2, constituye un subuniverso de $\mathbf{A}^2$. El conjunto de congruencias de $\mathbf{A}$ se denota CON $\mathbf{A}$.

Ejemplo 2.3. Sea $\mathbf{N}$ un subgrupo normal de un grupo $\mathbf{G}$. La relación binaria $\theta = \{\langle x, y\rangle \in G^2 : x.y^{-1} \in \mathbb{N}\}$ es una congruencia de $\mathbf{G}$. Recíprocamente, para cualquier congruencia θ de $\mathbf{G}$, la clase e/θ del neutro e es un subgrupo normal de $\mathbf{G}$. Esta correspondencia biyectiva entre subgrupos normales y congruencias de un grupo muestra que la noción de congruencia constituye una generalización de la de subgrupo normal.

Definición 2.4. Sean $\mathbf{A}$ y $\mathbf{B}$ dos álgebras del mismo tipo y $\theta \in$ CON $\mathbf{A}$. El **álgebra cociente** de $\mathbf{A}$ por θ es el álgebra $\mathbf{A}/\theta$ del mismo tipo que $\mathbf{A}$, con universo el conjunto A/θ de las clases de equivalencia de θ, donde las operaciones son definidas por $f_i(a_0/\theta, ..., a_{n_i-1}/\theta) = f_i(a_0, ..., a_{n_i-1})/\theta$.

Un *homomorfismo* de $\mathbf{A}$ a $\mathbf{B}$ es una función h entre los conjuntos A y B tal que para todos $i \in I$ y $a_0, ..., a_{n_i-1} \in A$, se cumple $hf_i(a_0, ..., a_{n_i-1}) = f_i(h(a_0), ..., h(a_{n_i-1}))$.

El siguiente teorema, conocido como Teorema de homomorfismos, generaliza los clásicos teoremas del mismo nombre, en teoría de grupos o de anillos.

Teorema 2.5. *Sean* $\mathbf{A}$ *y* $\mathbf{B}$ *dos álgebra del mismo tipo,* h *un homomorfismo suprayectivo de* $\mathbf{A}$ *a* $\mathbf{B}$*,* θ *una congruencia de* $\mathbf{A}$ *y* $g : A \to A/\theta$ *el mapeo cociente, que a cada elemento de* A *asocia su clase bajo* θ*.*

(i) *El núcleo* $\ker h = \{\langle x, y\rangle \in A^2 : h(x) = h(y)\}$ *de* h *es una congruencia de* $\mathbf{A}$*.*

(ii) g *es un homomorfismo suprayectivo.*

(iii) *Si* $\ker h = \theta$*, entonces la única función* $f : A/\theta \to B$ *tal que* $fg = h$ *es un homomorfismo entre* $\mathbf{A}/\theta$ *y* $\mathbf{B}$*.*

3. Retículos.

El concepto de retículo tiene su origen en la formalización de la lógica proposicional (De Morgan 1847, Boole 1854). Los matemáticos que dieron una definición abstracta de esta estructura fueron Peirce (1880), Schröder (1890-1905) y Dedekind (1897).

Definición 3.1. Un *retículo* es un álgebra $\mathbf{L} = \langle L, \wedge, \vee\rangle$, donde $\wedge$ y $\vee$ son operaciones binarias conmutativas y asociativas que satisfacen, para todos $x, y \in L$:

(i) $x \wedge x = x \vee x = x$ (*idempotencia*),
(ii) $x \wedge (x \vee y) = x \vee (x \wedge y) = x$ (*leyes de absorción*).

Es fácil ver que existe una correspondencia biunívoca entre retículos y conjuntos ordenados en los cuales cualquier pareja de elementos x y y tiene ínfimo $x \wedge y$ y supremo $x \vee y$. La relación de orden se define por $x \leq y \Leftrightarrow x \wedge y = x$.

Un ejemplo muy conocido de retículo es el dado por los subconjuntos de un conjunto, con la intersección y la unión como operaciones. En este caso, el retículo es *completo*, es decir que cualquier subfamilia tiene ínfimo y supremo.

Para cualquier álgebra $\mathbf{A}$, los subuniversos de $\mathbf{A}$ forman un retículo **SUB A**, en el cual $U \wedge V = U \cap V$ para todos subuniversos U, V, y $U \vee V$ es el *subuniverso generado* por $U \cup V$, o sea la intersección de todos los subuniversos de $\mathbf{A}$ que contienen a $U \cup V$. El retículo **SUB A** es completo. De manera similar, las congruencias de $\mathbf{A}$ forman un retículo completo **CON A**.

Un conjunto ordenado finito (o discreto) puede ser representado por un *diagrama de Hasse*, donde los elementos son representados por puntos, $x < y$ implica que el punto que representa x está más abajo que el que representa y en el diagrama, y se pone una arista entre dos puntos cada vez que hay una relación de *cobertura* entre los elementos correspondientes, es decir *y cubre* a x si y sólo si $y > x$ y para todo z tal que $x \leq z \leq y$, tenemos $z = x$ o $z = y$. En las Figuras 1 y 2 se encuentran diagramas de Hasse de los retículos $\mathbf{N_5}$ y $\mathbf{M_3}$ mencionados en los Teoremas 3.1 y 3.3.

Definición 3.2. Un retículo $\mathbf{L}$ es *modular* si para todos $x, y, z \in L$, $x \leq z$ implica que $x \vee (y \wedge z) = (x \vee y) \wedge z$. Se dice que $\mathbf{L}$ es *distributivo* si para todos $x, y, z \in L$ tenemos $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. Es claro que todo retículo distributivo es modular.

Teorema 3.3 (Dedekind 1900). (i) *El retículo de congruencias de cualquier grupo es modular.*

(ii) *Un retículo* $\mathbf{L}$ *es modular si y sólo si no contiene subretículos isomorfos a* $\mathbf{N_5}$.

Teorema 3.4 (Funayama-Nakayama 1942). *El retículo de congruencias de cualquier retículo es distributivo.*

Teorema 3.5. *Un retículo es distributivo si y sólo si no tiene subretículos isomorfos a* $\mathbf{N_5}$ *o a* $\mathbf{M_3}$.

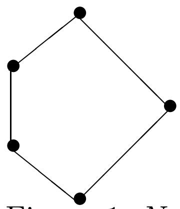

Figura 1: N_5

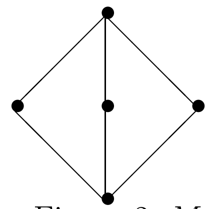

Figura 2: M_3

4. El teorema HSP de Birkhoff.

Una *variedad* es una clase de álgebras del mismo tipo cerrada bajo la formación (salvo isomorfismos) de imágenes homomorfas, subálgebras y productos. Estas formaciones de nuevas álgebras corresponden a operadores que actúan dentro de una misma variedad y se denotan respectivamente por H, S y P. Se puede demostrar que para una clase $\mathcal{K}$ de álgebras del mismo tipo, la variedad generada por $\mathcal{K}$ es $HSP(\mathcal{K})$, es decir que es suficiente cerrar la clase formando primero productos, luego subálgebras y al final imágenes homomorfas para obtener una variedad.

Una *clase ecuacional* es una clase de álgebras del mismo tipo que es definida por un conjunto de ecuaciones, es decir fórmulas que utilizan únicamente variables, los símbolos de operaciones del tipo dado, el símbolo de igualdad y el cuantificador universal. Por ejemplo, los grupos forman una variedad que tiene subvariedades como la subclase formada por los grupos abelianos. Los retículos distributivos forman una subvariedad de la variedad de retículos. Para ver que los retículos modulares también forman una variedad, es necesario dar una definición equivalente a la ley modular que no use el símbolo $\leq$ ni la implicación. Esta definición es la ecuación $((x \wedge z) \vee y) \wedge z) = (x \wedge z) \vee (y \wedge z)$.

El muy importante teorema HSP de Birkhoff, cuya demostración tiene varias páginas e implica la formación de álgebras libres, es el siguiente:

Teorema 4.1. *Sea $\mathcal{K}$ una clase de álgebras similares. Entonces $\mathcal{K}$ es una variedad si y sólo si es una clase ecuacional.*

5. Subcampos recientes de investigación.

El álgebra universal cuenta con numerosos adeptos que se encuentran principalmente en Estados Unidos, Europa del Este y Canadá. En esta última sección, mencionaremos brevemente tres de los temas más importantes que se siguen desarrollando a la fecha.

5.1. Los clones.

Un *clon* sobre un conjunto A es un conjunto de operaciones en A cerrado bajo todo tipo de composiciones y contiene todas la *proyecciones* $\pi_i^n : A^n \rightarrow A$ definidas por $p_i^n(x_0, ..., x_{n-1}) = x_i$. Los clones sobre A forman un retículo completo $\mathbf{C}(\mathbf{A})$. Este retículo es en general muy complejo, por lo cual los investigadores de este tema se restringen a regiones bien definidas para su estudio. En particular, los clones *minimales*, es decir los que cubren el clon de las proyecciones, y los clones *maximales* , i.e. que son cubiertos por el clon de todas las operaciones, han dado lugar a numerosos artículos. A continuación enunciamos cuatro teoremas importantes de la teoría de los clones.

Teorema 5.1 (Post 1921). $C(\{0,1\})$ *es numerable.*

Teorema 5.2 (Yanov-Muchnik 1959). *Si A es finito y tiene más de dos elementos, entonces* $|C(A)| = 2^{\aleph_0}$.

Teorema 5.3 (Rosenberg 1976). *Si A es infinito, entonces* $|C(A)| = 2^{2^{|A|}}$.

El siguiente resultado es de los más importantes de esta área. Sería demasiado largo presentarlo con todas las definiciones que se necesitarían, así que lo mencionamos en forma abreviada.

Teorema 5.4 (Rosenberg 1965). *Sea A un conjunto finito. Un clon sobre A es maximal si y sólo si tiene una de seis formas, definidas a partir de relaciones sobre A.*

5.2. El conmutador.

Si $\mathbf{H}$ y $\mathbf{K}$ son subgrupos normales de un grupo $\mathbf{G}$, el *conmutador* $[H, K]$ es el subuniverso de $\mathbf{G}$ generado por los elementos de la forma $x^{-1}.y^{-1}.x.y$, con $x \in H$ y $y \in K$. El subgrupo resultante es normal, y es el subgrupo más pequeño $\mathbf{G}'$ de $\mathbf{G}$ contenido en $H \cap K$ tal que en $\mathbf{G}/\mathbf{G}'$, todo elemento de H/G' conmuta con todo elemento de K/G'. La teoría del conmutador generaliza esta definición para álgebras que pertenecen a variedades *modulares*, es decir cuyos miembros tienen su retículo de congruencias modular. Esta área fue desarrollada por Smith (1976), Hagemann y Herrmann (1979) y Freese y McKenzie (1987).

5.3. Teoría de las congruencias domadas.

En los años ochenta, Hobby y McKenzie empezaron a desarrollar lo que se convertiría en el subcampo más en voga del álgebra universal: la teoría de las congruencias domadas, o *Tame congruence theory* en inglés. Esta teoría se basa en una clasificación de todas las álgebras finitas en cinco tipos, definidos a partir de sus congruencias. Estos tipos son denominados respectivamente el tipo *unario*, el *afín*, el *Booleano*, el tipo *retículo* y el tipo *semiretículo*. Es decir que cada álgebra finita se comporta localmente como el álgebra que corresponde a su tipo. A partir de esta división se prueban teoremas muy potentes, y muchos artículos que usan estos conceptos se siguen escribiendo.

Referencias

[1] G. Birkhoff, On the combination of subalgebras, *Proc. Cambridge Philos. Soc.* **29**, 441-464, 1933.

[2] G. Birkhoff, On the structure of abstract algebras, *Proc. Cambridge Philos. Soc* **31**, 433-454, 1935.

[3] S. Burris and H.P. Sankappanavar, A Course in Universal Algebra, Springer-Verlag, 1981.

[4] R. Freese and R. McKenzie, Commutator Theory for Congruence Modular Varieties, London Math. Soc., Lecture Notes Series 125, 1987.

[5] D. Hobby and R. McKenzie, The Structure of Finite Algebras, Amer. Math. Soc. Contemporary Mathematics, Volume 76, 1988.

[6] R. McKenzie, G. McNulty and W. Taylor, Algebras, Lattices, Varieties, vol. I, Wadsworth & Brooks/Cole Math. Series, Monterey, CA, 1987.

[7] A. Szendrei, Clones in Universal Algebra, Séminaire de Mathématiques Supérieures, Les Presses de lÚniversité de Montréal, 1986.

[8] B.L. Van der Waerden, Moderne Algebra, Julius Springer, Berlin, 1931.

[9] A. N. Whitehead, A Treatise on Universal Algebra, Cambridge University Press, U.K., 1898.