Introducción al Álgebra Universal

Diego Castaño
INMABB - Depto. de Matemática
Universidad Nacional del Sur
diego.castano@uns.edu.ar

28 de mayo de 2015

El objetivo de este curso breve es presentar el objeto de estudio del álgebra universal, es decir, las **álgebras**, y las herramientas más básicas utilizadas para su descripción y estudio: subálgebras, homomorfismos, productos directos y subdirectos, congruencias, álgebras libres, ecuaciones, etc. Asimismo veremos uno de los primeros resultados importantes de esta disciplina que disparó su crecimiento enormemente: el teorema de Birkhoff. Una exposición sistemática de los conceptos básicos puede encontrarse en los siguientes textos fundamentales de introducción al álgebra universal:

- S. Burris, H. P. Sankappanavar, *A Course in Universal Algebra*, Springer-Verlag, 1981.

  Dispone de una version gratuita online revisada en 2012:

  https://www.math.uwaterloo.ca/~snburris/htdocs/ualg.html

- C. Bergman, *Universal Algebra, Fundamentals and Selected Topics*, CRC Press, 2012.
- G. Grätzer, *Universal Algebra* (Second Edition), Springer-Verlag, 2008.
- R. McKenzie, G. McNulty, W. Taylor, *Algebras, Lattices, Varieties, Volume I*, Wadsworth & Brooks/Cole Advanced Book & Software, 1987.

Índice

1. El objeto de estudio: álgebras

El álgebra tradicional moderna estudia fundamentalmente dos tipos de estructuras matemáticas:

- **Grupos**: éstos se suelen definir como un par $\langle G, \cdot \rangle$, donde G es un conjunto no vacío y $\cdot : G \times G \to G$ es una función que llamamos *operación binaria* del grupo y que satisface las siguientes condiciones:

  ($G1$) Asociatividad: para todo $x, y, z, \in G$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

  ($G2$) Existencia de elemento neutro: existe un elemento $1 \in G$ tal que $1 \cdot x = x \cdot 1 = x$ para todo $x \in G$.

  ($G3$) Existencia de inversos: para cada $x \in G$, existe un elemento $x' \in G$ tal que $x \cdot x' = x' \cdot x = 1$.

- **Anillos**: éstos se suelen definir como una terna $\langle A, +, \cdot \rangle$ donde A es un conjunto no vacío y $+$ y $\cdot$ son dos operaciones binarias, es decir, son funciones $+ : A \times A \to A$, $\cdot : A \times A \to A$, tales que:

  ($A1$) $\langle A, + \rangle$ es un grupo con elemento neutro 0.

  ($A2$) Conmutatividad de $+$: para todo $x, y \in A$, $x + y = y + x$.

  ($A3$) Asociatividad de $\cdot$: para todo $x, y, z \in A$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

  ($A4$) Distributividad a izquierda: para todo $x, y, z \in A$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

  ($A5$) Distributividad a derecha: para todo $x, y, z \in A$, $(x + y) \cdot z = x \cdot z + y \cdot z$.

Podemos observar que ambas estructuras consisten de un conjunto no vacío A de base sobre el cual están definidas una o más *operaciones binarias*. Por operación binaria entendemos una función $f : A \times A \to A$ de modo que podemos calcular $f(a_1, a_2)$ para cualesquier par $(a_1, a_2) \in A \times A$ y obtener como resultado un nuevo elemento $f(a_1, a_2)$ de A, que usualmente, por comodidad, notamos con *notación infija* $f(a_1, a_2) = a_1 \, f \, a_2$.

Sobre estas estructuras se definen muchos conceptos interesantes y se prueban mucho resultados imporantes que intentan describir lo más claramente posible su estructura. Sin embargo, en su estudio se puede apreciar que muchas de las propiedades más básicas que poseen no dependen de las propiedades específicas que verifican según su definición, sino que obedecen a su forma más básica.

El álgebra universal pretende ver los grupos y los anillos como casos particulares de estructuras mucho más generales. Estas estructuras se denominan **álgebras**[1] y constan de un conjunto no vacío de base sobre el cual están definidas operaciones. Para dar mayor generalidad a esta estructura se admiten no solamente cualquier número de operaciones, sino también operaciones de diferentes *aridades*, además de las operaciones binarias. A continuación definimos en forma precisa estos conceptos.

Definición 1.1. *Dado un conjunto no vacío A y un entero no negativo n, llamamos* **operación n-aria** *a cualquier función $f : A^n \to A$.*

- Observar que si $n = 0$, A^0 es un conjunto con un solo elemento y, por tanto, identificamos la operación $f : A^0 \to A$ con el valor de f en el único elemento de A^0; por esta razón llamamos **constantes** a las operaciones 0-arias.

- A las operaciones 1-arias, 2-arias, 3-arias, las solemos denominar **operaciones unarias, binarias, ternarias**, respectivamente.

Definición 1.2. *Un* **lenguaje (algebraico)** $\mathcal{L}$ *es un conjunto de símbolos de operaciones, cada uno con una* **aridad** *fija asociada consistente en un enterno no negativo.*

[1] No confundir con la noción de *k-álgebra* tradicional que consiste de un k-espacio vectorial dotado además de una estructura compatible de anillo.

Definición 1.3. *Dado un lenguaje $\mathcal{L}$, una* **$\mathcal{L}$-álgebra** *es un par $\mathbf{A} = \langle A, F\rangle$ donde A es un conjunto no vacío y $F = \{f^{\mathbf{A}} : f \in \mathcal{L}\}$ es una familia de operaciones sobre A de modo que $f^{\mathbf{A}}$ tiene la aridad correspondiente al símbolo f. El conjunto A es el* **universo** *del álgebra y las operaciones de F son sus* **operaciones básicas** *o* **fundamentales**. *Decimos que dos álgebras son* **similares** *si son álgebras sobre el mismo lenguaje.*

Ejemplo 1.4.

(1) Si $\mathcal{L} = \{*\}$ donde $*$ es un símbolo de operación binaria, $\mathbf{A} = \langle\{0, 1, 2\}, *^{\mathbf{A}}\rangle$ es un álgebra donde $*^{\mathbf{A}}$ está dada por

$$x *^{\mathbf{A}} y = \begin{cases} 1 & \text{si } x = y \\ x, & \text{si } x \neq y. \end{cases}$$

(2) Observando la definición de grupos y anillos dada anteirormente, se ve claramente que los grupos son álgebras sobre un lenguaje $\{\cdot\}$ con una operación binaria y los anillos son álgebras sobre un lenguaje $\{+, \cdot\}$ que posee dos operaciones binarias.

(3) **Cuerpos.** Un cuerpo es un anillo $\mathbf{K} = \langle K, +, \cdot\rangle$ que verifica las siguientes condiciones adicionales:

($C1$) Existe $1 \in K$ tal que $x \cdot 1 = 1 \cdot x = x$ para todo $x \in K$.
($C2$) $x \cdot y = y \cdot x$ para todo $x, y \in K$.
($C3$) Para todo $x \in K$, $x \neq 0$, existe $x^{-1} \in K$ tal que $x \cdot x^{-1} = 1$.

(4) **Espacios vectoriales.** Dado un cuerpo $\mathbf{K}$, un $\mathbf{K}$-espacio vectorial tradicionalmente se define como una estrctura que posee además de una estructura de grupo una operación externa $\mathbf{K} \times V \to V$ de multiplicación entre escalares del cuerpo y vectores del espacio V. Tal definición no correspondería a un álgebra en el sentido del álgebra universal. Sin embargo, es muy sencillo adaptar la definición de $\mathbf{K}$-espacios vectoriales, considerando que cada escalar $k \in K$ define una operación unaria sobre V, $k : V \to V$, tal que $v \mapsto kv$. De esta manera un $\mathbf{K}$-espacio vectorial es un álgebra $\mathbf{V} = \langle V, +, \{k\}_{k\in K}\rangle$ tal que:

($EV1$) $\langle V, +\rangle$ es un grupo con elemento neutro 0.
($EV2$) $x + y = y + x$ para todo $x, y \in V$.
($EV3$) $1x = x$.
($EV4$) $k(x + y) = kx + ky$ para todo $k \in K$, $x, y \in V$.
($EV5$) $(k_1 + k_2)x = k_1x + k_2x$ para todo $k_1, k_2 \in K$, $x \in V$.
($EV6$) $k_1(k_2x) = (k_1 \cdot k_2)x$ para todo $k_1, k_2 \in K$, $x \in V$.

(5) **Álgebra de Boole.** Un álgebra de Boole es un álgebra $\mathbf{B} = \langle B, \wedge, \vee, -, 0, 1\rangle$, donde $\wedge$ y $\vee$ son operaciones binarias, $-$ es una operación unaria y 0 y 1 son constantes, tal que para todo $x, y, z \in B$:

($B1$) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$,	$x \vee (y \vee z) = (x \vee y) \vee z$.
($B2$) $x \wedge y = y \wedge x$,	$x \vee y = y \vee x$.
($B3$) $x = x \wedge x$,	$x = x \vee x$.
($B4$) $x = x \wedge (x \vee y)$,	$x = x \vee (x \wedge y)$.
($B5$) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$,	$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.
($B6$) $x \wedge 0 = 0$,	$x \vee 1 = 1$.
($B7$) $x \wedge -x = 0$,	$x \vee -x = 1$.
($B8$) $-(-x) = x$.	
($B9$) $-(x \wedge y) = -x \vee -y$,	$-(x \vee y) = -x \wedge -y$.

2. Construcciones básicas

En esta sección veremos las nociones fundamentales asociadas a las álgebras, que no son otra cosa que generalizaciones de las correspondientes a grupos y anillos: subgrupos y subanillos, homomorfismos, grupos y anillos cociente, productos directos, etc.

2.1. Subálgebras

Definición 2.1. *Un* **subuniverso** *de* $\mathbf{A}$ *es un subconjunto* B *de* A *que es cerrado bajo las operaciones fundamentales de* $\mathbf{A}$*, es decir, si* f *es una operación fundamental* n*-aria de* $\mathbf{A}$ *y* $a_1, \ldots, a_n \in B$*, entonces* $f(a_1, \ldots, a_n) \in B$*.*

Dadas dos álgebras similares $\mathbf{A}$ *y* $\mathbf{B}$*, decimos que* $\mathbf{B}$ *es* **subálgebra** *de* $\mathbf{A}$ *si* $B \subseteq A$ *y cada operación fundamental de* $\mathbf{B}$ *es la restricción de la correspondiente operación de* $\mathbf{A}$*. Escribimos* $\mathbf{B} \leq \mathbf{A}$*.*

Observar que si B es un subuniverso no vacío del álgebra $\mathbf{A} = \langle A, \{f_i : i \in i\}\rangle$, el álgebra $\langle B, \{f_i|_B : i \in I\}\rangle$ es un subálgebra de $\mathbf{A}$. Por lo tanto, se suelen identificar las subálgebras de $\mathbf{A}$ con sus subuniversos.

Ejemplo 2.2. Tradicionalmente se ve a los grupos como estructuras de la forma $\langle G, \cdot\rangle$ con una sola operación binaria fundamental.

Observemos que si consideramos el grupo $\langle \mathbb{Z}, +\rangle$ de los números enteros, según la definición anterior $\langle \mathbb{N}, +\rangle$ es una subálgebra de $\langle \mathbb{Z}, +\rangle$, pues $\mathbb{N}$ es cerrado bajo la única operación fundamental de $\langle \mathbb{Z}, +\rangle$. Sin embargo, $\langle \mathbb{N}, +\rangle$ no es un grupo.

Esta discrepancia es fácilmente solucionable, pues si observamos las condiciones de la definición de grupo vemos que todo grupo posee dos operaciones importantes más además de la operación binaria:

- El elemento neutro: se puede pensar como una operación constante $1 : G^0 \to G$ que elige un elemento fijo del grupo.
- El inverso: se puede pensar como una operación unaria $^{-1} : G \to G$.

De esta manera, la nueva definición de grupo es la siguiente: un grupo es un álgebra $\mathbf{G} = \langle G, \cdot, {}^{-1}, 1\rangle$ donde $\cdot$ es una operación binaria, $^{-1}$ es una operación unaria y 1 es una constante, tal que:

$(G1)$ $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, para todo $x, y, z \in G$,

$(G2)$ $x \cdot 1 = 1 \cdot x = x$ para todo $x \in G$,

$(G3)$ $x \cdot x^{-1} = x^{-1} \cdot x = 1$ para todo $x \in G$.

Las estructuras en apariencia no cambian pero sí la noción de subálgebra asociada a ellas. Ahora un subconjunto $X \subseteq G$, para ser un subuniverso de $\langle G, \cdot, {}^{-1}, 1\rangle$ deberá ser cerrado bajo las tres operaciones, por lo tanto deberá verificar que:

- $1 \in X$,
- si $x, y \in X$, entonces $x \cdot y \in X$,
- si $x \in X$, entonces $x^{-1} \in X$.

Esta noción de subálgebra sí coincide con la noción habitual de subgrupo.

Esta forma de definir la estructura de grupo tiene la ventaja además de que las condiciones de grupo se reducen ahora a *identidades* o *ecuaciones* pues las condiciones existencias están implícitas en las operaciones fundamentales unaria y 0-aria. Veremos la importancia de este hecho cuando tratemos los conceptos de *variedad* y de *clase ecuacional*.

Ejemplo 2.3. De la misma forma que con los grupos, la definición adecuada de anillo en el contexto de álgebra universal es la siguiente: un anillo es un álgebra $\langle A, +, -, 0, \cdot \rangle$ donde $+$ y $\cdot$ son dos operaciones binarias, $-$ es una operación unaria y 0 es una constante, tales que:

$(A1)$ $\langle A, +, -, 0 \rangle$ es un grupo.

$(A2)$ $x + y = y + x$, para todo $x, y \in A$.

$(A3)$ $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ para todo $x, y, z \in A$.

$(A4)$ $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ para todo $x, y, z \in A$.

$(A5)$ $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ para todo $x, y, z \in A$.

Al igual que en grupos y anillos, la siguiente propiedad de los subuniversos de un álgebra es la clave para definir subálgebra generada.

Proposición 2.4. *Si $\{S_i : i \in I\}$ es una familia de subuniversos de un álgebra $\mathbf{A}$, entonces $\bigcap_{i \in I} S_i$ también es un subuniverso.*

Definición 2.5. *Dada un álgebra $\mathbf{A}$ y un subconjunto $X \subseteq A$, el* **subuniverso generado por** *X es $Sg^{\mathbf{A}}(X)$ es la intersección de todos los subuniversos de A que contienen a X. Si $Sg^{\mathbf{A}}(X) \neq \emptyset$ es el universo de una subálgebra que denotamos $\mathbf{Sg}^{\mathbf{A}}(X)$.*

Más interesante que la definición abstracta de subuniverso generado es obtener una manera sistemática de generar todos los elementos de dicho subuniverso a partir de los generadores (los elementos de X). El siguiente teorema resuelve el problema.

Teorema 2.6. *Sea $\mathbf{A} = \langle A, F \rangle$ un álgebra y $X \subseteq A$. Definimos, por reucursión, los conjuntos X_n:*

- $X_0 = X$,
- $X_{n+1} = X_n \cup \{f(a_1, \ldots, a_k) : a_1, \ldots, a_k \in X_n, f \in F \text{ de aridad } k\}$.

Entonces $Sg^{\mathbf{A}}(X) = \bigcup_n X_n$.

Ejemplo 2.7. Consideremos el grupo $\mathbf{Z}_{12} = \langle \mathbb{Z}_{12}, +, -, 0 \rangle$ y calculemos $Sg^{\mathbf{Z}_{12}}(\{\overline{3}\})$. Calculamos:

- $X_0 = \{\overline{3}\}$.
- $X_1 = \{\overline{3}\} \cup \{\overline{0}, \overline{3}, -\overline{3}, \overline{6}\} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$.
- $X_2 = X_1$.
- $\ldots$
- $X_n = X_1$.

Por lo tanto, $Sg^{\mathbf{Z}_{12}}(\{\overline{3}\}) = \bigcup_n X_n = X_1 = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$.

Ejemplo 2.8. Consideremos el grupo $\mathbf{Z} = \langle \mathbb{Z}, +, -, 0 \rangle$ y calculemos $Sg^{\mathbf{Z}}(\{3\})$. Calculamos:

- $X_0 = \{3\}$.
- $X_1 = \{3\} \cup \{0, -3, 6\} = \{-3, 0, 3, 6\}$.
- $X_2 = X_1 \cup \{0, 3, -3, -6, 9, 12\} = \{-6, -3, 0, 3, 6, 9, 12\}$
- etc.

Vemos que $Sg^{\mathbf{Z}}(\{3\}) = \bigcup_n X_n = \{3k : k \in \mathbb{Z}\}$.

2.2. Congruencias y álgebras cociente

En esta sección extenderemos la construcción de grupos cocientes y anillos cocientes al contexto general de álgebras.

Recordemos que si N es un subgrupo normal de un grupo G, el grupo cociente G/N se construye de la siguiente manera:

- se define una relación sobre G definiendo:

$$x \equiv y \iff xy^{-1} \in N.$$

- se prueba que $\equiv$ es una relación de equivalencia sobre G y se define $G/N := G/\equiv$ como el conjunto cociente respecto de dicha relación de equivalencia.
- se prueba que si definimos una operación binaria en G/N mediante

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y},$$

ésta resulta bien definida, es decir,

$$\text{si } x \equiv x' \text{ e } y \equiv y', \text{ entonces } x \cdot y \equiv x' \cdot y'. \tag{1}$$

De esta manera la definición anterior no depende de los representantes elegidos para las clases de equivalencia.

- se prueba que $\langle G/N, \cdot \rangle$ es un grupo.

La clave para generalizar esta construcción es basarse en la relación de equivalencia y en la propiedad (1), y no tanto en el subgrupo normal.

Definición 2.9. *Sea* $\mathbf{A}$ *un álgebra y* θ *una relación de equivalencia sobre* A*. Decimos que* θ *es una* **congruencia** *sobre* $\mathbf{A}$ *si* θ *satisface la siguiente* propiedad de compatibilidad*: para cada operación n-aria* $f^{\mathbf{A}}$ *de* $\mathbf{A}$ *y elementos* $a_i, b_i \in A$*, si* $(a_i, b_i) \in \theta$ *para* $1 \leq i \leq n$*, entonces*

$$(f^{\mathbf{A}}(a_1, \ldots, a_n), f^{\mathbf{A}}(b_1, \ldots, b_n)) \in \theta.$$

Al conjunto de todas las congruencias sobre $\mathbf{A}$ *lo denotamos* $\operatorname{Con}\mathbf{A}$*.*

La condición de compatibilidad nos permite definir una estructura algebraica sobre el conjunto cociente A/θ.

Definición 2.10. *Sea* θ *una congruencia sobre un álgebra* $\mathbf{A}$*. Definimos el* **álgebra cociente de A por** θ*, escrita* $\mathbf{A}/\theta$*, como el álgebra cuyo universo es* A/θ *y para cada operación* $f^{\mathbf{A}}$ *de* $\mathbf{A}$ *definimos la operación* $f^{\mathbf{A}/\theta}$ *sobre* A/θ *de la siguiente manera*

$$f^{\mathbf{A}/\theta}(a_1/\theta, \ldots, a_n/\theta) = f^{\mathbf{A}}(a_1, \ldots, a_n)/\theta$$

donde x/θ *denota la clase de equivalencia de* x *respecto de* θ*.*

Notemos que $\mathbf{A}$ y el álgebra cociente $\mathbf{A}/\theta$ son álgebras similares.

Ejemplo 2.11. Consideremos un grupo $\mathbf{G} = \langle G, \cdot, {}^{-1}, 1 \rangle$. ¿Cuáles son las congruencias sobre G?

Ya sabemos que si N es un subgrupo normal de G, la relación θ_N definida por

$$(x, y) \in \theta_N \iff xy^{-1} \in N$$

es una congruencia sobre G.

Recíprocamente, si consideramos una congruencia cualquiera θ sobre un grupo $\langle G, \cdot, {}^{-1}, 1\rangle$, podemos asociarle el siguiente subconjunto de G:

$$N_\theta = 1/\theta = \{x \in G : (x, 1) \in \theta\},$$

es decir, la clase de congruencia del elemento neutro 1. Es fácil probar que N_θ es un subgrupo normal de $\mathbf{G}$.

Si S es la familia de todos los subgrupos normales de $\mathbf{G}$, tenemos entonces dos aplicaciones $f : S \to \operatorname{Con}\mathbf{G}$ y $g : \operatorname{Con}\mathbf{G} \to S$ dadas por $f(N) = \theta_N$ y $g(\theta) = N_\theta = 1/\theta$. Veamos que estas funciones son una la inversa de la otra. En efecto:

- Si N es un subgrupo normal de G, entonces

  $$x \in N_{\theta_N} \iff (x, 1) \in \theta_N \iff x1^{-1} \in N \iff x \in N.$$

  Esto muestra que $N_{\theta_N} = N$.

- Si $\theta \in \operatorname{Con}\mathbf{G}$, entonces:

  $$(x, y) \in \theta_{N_\theta} \iff xy^{-1} \in N_\theta \iff (xy^{-1}, 1) \in \theta \iff (x, y) \in \theta.$$

  Luego $\theta_{N_\theta} = \theta$.

Esto prueba que hay una correspondencia biyectiva entre congruencias y subgrupos normales en todo grupo.

Es importante observar que la propiedad de que las congruencias de un álgebra estén determinadas unívocamente por subconjuntos distinguidos del álgebra no es válida en general.

En el caso de los grupos, la clase de equivalencia del elemento neutro caracteriza totalmente la congruencia. Por esta razón decimos que los grupos tienen **congruencias 1-regulares**. Más aún, en grupos vale una propiedad más fuerte todavía: la clase de equivalencia de cualquier elemento determina completamente la congruencia; se dice entonces que los grupos tienen **congruencias regulares**. En el siguiente ejemplo mostramos un álgebra que no posee congruencias regulares.

Ejemplo 2.12. En anillos, resulta que las congruencias están en correspondencia biyectiva con los ideales biláteros y dicha correspondencia es exactamente la misma que la definida para grupos. Queda como ejercicio al lector probar en detalle esta afirmación.

Ejemplo 2.13. Consideremos el álgebra $\mathbf{A} = \langle\{0, 1, 2, 3\}, \vee\rangle$, donde $x \vee y = \max\{x, y\}$.

Observemos que si θ es una congruencia sobre $\mathbf{A}$ y tomamos $a, b, c \in A$ tales que $a \leq b \leq c$ y $(a, c) \in \theta$. Entonces $(a \vee b, c \vee b) \in \theta$, es decir, $(b, c) \in \theta$. Esto muestra que si a, c están en la misma clase de congruencia, todo elemento intermedio también lo estará.

Es fácil probar entonces que $\mathbf{A}$ posee 8 congruencias cuyos conjuntos cocientes son:

- $A/\theta_1 = \{\{0\}, \{1\}, \{2\}, \{3\}\}$.
- $A/\theta_2 = \{\{0\}, \{1\}, \{2, 3\}\}$.
- $A/\theta_3 = \{\{0\}, \{1, 2\}, \{3\}\}$.
- $A/\theta_4 = \{\{0, 1\}, \{2\}, \{3\}\}$.
- $A/\theta_5 = \{\{0, 1\}, \{2, 3\}\}$.
- $A/\theta_6 = \{\{0\}, \{1, 2, 3\}\}$.
- $A/\theta_7 = \{\{0, 1, 2\}, \{3\}\}$.

- $A/\theta_8 = \{\{0,1,2,3\}\}$.

En este caso la clase de equivalencia de ninguno de los elementos determina por completo la relación de congruencia, es decir, $\mathbf{A}$ no es a-regular para ningún $a \in A$.

Dada un álgebra $\mathbf{A}$, $(\operatorname{Con}\mathbf{A}, \subseteq)$ es un conjunto parcialmente ordenado con primer y último elemento. La congruencia identidad

$$\Delta = \{(a,a) \in A^2 : a \in A\}$$

es el primer elemento y el último elemento es la congruencia total

$$\nabla = A \times A.$$

Observación 2.14. Las congruencias también nos permiten generalizar las nociones de grupo simple y anillo simple. Recordemos que un grupo es simple si sus únicos subgrupos normales son los triviales: (e) y G. Análogamente, un anillo es simple si sus únicos ideales biláteros son los triviales (0) y A.

En el contexto del álgebra universal, diríamos que los grupos simples y los anillos simples poseen únicamente las congruencias triviales: Δ y ∇. Por eso decimos, en general, que un álgebra es simple si sus únicas congruencias son Δ y ∇, es decir, $\operatorname{Con}\mathbf{A} = \{\Delta, \nabla\}$.

2.3. Homomorfismos

En esta sección vamos a generalizar la definición de homomorfismos conocida para grupos y anillos así como la relación entre los homomorfismos y las estructuras cociente.

Definición 2.15. *Sean* $\mathbf{A}$ *y* $\mathbf{B}$ *dos álgebras similares. Una aplicación* $h : A \to B$ *se llama* **homomorfismo** *de* $\mathbf{A}$ *en* $\mathbf{B}$ *si se verifica*

$$h(f^{\mathbf{A}}(a_1, \ldots, a_n)) = f^{\mathbf{B}}(h(a_1), \ldots, h(a_n))$$

para toda operación n-aria $f^{\mathbf{A}}$ *de* $\mathbf{A}$ *y su correspondiente* $f^{\mathbf{B}}$ *de* $\mathbf{B}$ *y para todo* $a_1, \ldots, a_n \in A$. *Escribimos* $h : \mathbf{A} \to \mathbf{B}$.

- *Si* h *es sobreyectivo, decimos que* $\mathbf{B}$ *es una* **imagen homomorfa** *de* $\mathbf{A}$.
- *Si* h *es biyectivo, decimos que* h *es un* **isomorfismo** *y que* $\mathbf{A}$ *y* $\mathbf{B}$ *son* **isomorfas**. *Escribimos* $\mathbf{A} \cong \mathbf{B}$.

Ejemplo 2.16.

1. Los homomorfismos de grupos y de anillos son todos ejemplos del concepto general de homomorfismo. Pero debemos notar que para definir la noción de homomorfismo entre las álgebras $\mathbf{A}$ y $\mathbf{B}$ no es necesario que pertenezcan ambas a ninguna clase especial, sólo basta con que compartan el mismo lenguaje, de modo que se correspondan las aridades de las operaciones de una y de otra. Cuando hablamos de homomorfismos *de grupos* o *de anillos* sólo queremos indicar que la aplicación es un homomorfismo *respecto del lenguaje* $\{\cdot, {}^{-1}, e\}$ *o* $\{+, -, 0, \cdot\}$, respectivamente.
2. Si $\mathbf{A} = \langle\{0,1,2,3\}, \vee\rangle$ donde $x \vee y = \max\{x, y\}$ para $x, y \in A$, la aplicación $h : A \to A$ tal que $h(0) = h(1) = 1$ y $h(2) = h(3) = 2$ es un homomorfismo de $\mathbf{A}$ en $\mathbf{A}$.

Veremos ahora que los homomorfismos están estrechamente relacionados con las congruencias. De hecho, las congruencias nos permiten calcular todas las imágenes homomorfas de un álgebra dada. Para ello, queremos asociar a cada homomorfismo $h : \mathbf{A} \to \mathbf{B}$ una congruencia sobre $\mathbf{A}$. Si $\mathbf{A}$ y $\mathbf{B}$ son grupos esto se hace tomando la imagen completa inversa del elemento neutro de $\mathbf{B}$, es decir, $h^{-1}(e_{\mathbf{B}}) = \{a \in A : h(a) = e_{\mathbf{B}}\}$, que se denomina *núcleo* de h. Se obtiene así siempre un subgrupo normal del grupo $\mathbf{A}$. En nuestro caso debemos asociar a h una congruencia sobre $\mathbf{A}$, más que un subconjunto especial.

Definición 2.17. *Sea $h : \mathbf{A} \to \mathbf{B}$ un homomorfismo. Definimos el* **núcleo** *de h, escrito $\ker h$, como*

$$\ker h = \{(a, b) \in A^2 : h(a) = h(b)\}.$$

Teorema 2.18. *Sea $h : \mathbf{A} \to \mathbf{B}$ un homomorfismo. Entonces el núcleo de h es una congruencia sobre $\mathbf{A}$.*

Demostración. Es claro que $\ker h$ es una relación de equivalencia sobre A. Veamos que $\ker h$ verifica la propiedad de compatibilidad. Supongamos que $f^{\mathbf{A}}$ es una operación n-aria de $\mathbf{A}$ y que $(a_i, b_i) \in \ker h$ para $1 \leq i \leq n$. Luego $h(a_i) = h(b_i)$ para $1 \leq i \leq n$, por lo tanto

$$h(f^{\mathbf{A}}(a_1, \ldots, a_n)) = f^{\mathbf{B}}(h(a_1), \ldots, h(a_n)) = f^{\mathbf{B}}(h(b_1), \ldots, h(b_n)) = h(f^{\mathbf{A}}(b_1, \ldots, b_n))$$

de donde

$$(f^{\mathbf{A}}(a_1, \ldots, a_n), f^{\mathbf{A}}(b_1, \ldots, b_n)) \in \ker h.$$

■

Recíprocamente, para cada congruencia θ sobre un álgebra $\mathbf{A}$ podemos definir un homomorfismo de $\mathbf{A}$ en $\mathbf{A}/\theta$.

Definición 2.19. *Sea $\mathbf{A}$ un álgebra y $\theta \in \operatorname{Con} \mathbf{A}$. Definimos la* **aplicación canónica** *$\nu_\theta : A \to A/\theta$ por $\nu_\theta(a) = a/\theta$.*

Teorema 2.20. *Dada un álgebra $\mathbf{A}$ y una congruencia θ sobre $\mathbf{A}$, la aplicación canónica ν_θ es un homomorfismo sobreyectivo de $\mathbf{A}$ sobre $\mathbf{A}/\theta$.*

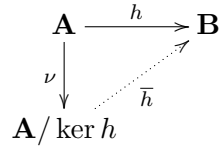
Demostración. Claramente ν_θ es sobreyectiva por lo que sólo debemos verificar que es un homomorfismo. Para esto sea $f^{\mathbf{A}}$ una operación n-aria sobre $\mathbf{A}$ y $a_1, \ldots, a_n \in A$. En efecto, tenemos

$$\begin{aligned} \nu_\theta(f^{\mathbf{A}}(a_1, \ldots, a_n)) &= f^{\mathbf{A}}(a_1, \ldots, a_n)/\theta \\ &= f^{\mathbf{A}/\theta}(a_1/\theta, \ldots, a_n/\theta) \\ &= f^{\mathbf{A}/\theta}(\nu_\theta(a_1), \ldots, \nu_\theta(a_n)). \end{aligned}$$

■

El siguiente teorema conocido como "Primer Teorema de Isomorfsimo"o "Teorema del Triángulo"afirma que toda imagen homomorfa de un álgebra $\mathbf{A}$ es isomorfa a un cociente de $\mathbf{A}$ por una congruencia.

Teorema 2.21 (Primer Teorema de Isomorfismo)**.** *Sea $h : \mathbf{A} \to \mathbf{B}$ un homomorfismo sobreyectivo. Entonces existe un isomorfismo $\overline{h}$ entre $\mathbf{A}/\ker h$ y $\mathbf{B}$ definido por $h = \overline{h} \circ \nu$, donde ν es el homomorfismo canónico de $\mathbf{A}$ en $\mathbf{A}/\ker h$.*



Demostración. Sea $\theta = \ker h$. Notemos que si $h = \overline{h} \circ \nu$, entonces $\overline{h}(a/\theta) = h(a)$ para todo $a \in A$. Por la definición de θ, esta ecuación permite definir adecuadamente la función $\overline{h} : A/\theta \to B$.

Veamos que $\overline{h}$ es un homomorfismo. Para ello consideremos una operación n-aria f y elementos $a_1, \ldots, a_n \in A$, luego

$$\begin{aligned} \overline{h}(f^{\mathbf{A}/\theta}(a_1/\theta, \ldots, a_n/\theta)) &= \overline{h}(f^{\mathbf{A}}(a_1, \ldots, a_n)/\theta) \\ &= h(f^{\mathbf{A}}(a_1, \ldots, a_n)) \\ &= f^{\mathbf{B}}(h(a_1), \ldots, h(a_n)) \\ &= f^{\mathbf{B}}(\overline{h}(a_1/\theta), \ldots, \overline{h}(a_n/\theta)). \end{aligned}$$

Resta ver que $\overline{h}$ es una biyección. En efecto, si suponemos $\overline{h}(a/\theta) = \overline{h}(b/\theta)$ obtenemos $h(a) = h(b)$ con lo cual $a/\theta = b/\theta$. Esto muestra que $\overline{h}$ es inyectiva.

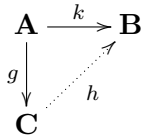
Veamos ahora la sobreyectividad de $\overline{h}$. Dado $b \in B$, como h es sobreyectiva, existe $a \in A$ tal que $h(a) = b$, luego $\overline{h}(a/\theta) = b$.

Por lo tanto, $\overline{h}$ es un isomorfismo entre $\mathbf{A}/\theta$ y $\mathbf{B}$. ■

Se puede probar una versión un poco más general del teorema anterior que es de mucha utilidad práctica.

Teorema 2.22. *Sean* $\mathbf{A}$, $\mathbf{B}$ *y* $\mathbf{C}$ *tres álgebras similares,* $k : \mathbf{A} \to \mathbf{B}$, $g : \mathbf{A} \to \mathbf{C}$ *homomorfismos tales que* $\ker g \subseteq \ker k$ *y* g *es sobreyectivo. Entonces existe un homomorfismo* $h : \mathbf{C} \to \mathbf{B}$ *tal que* $k = h \circ g$. *Además:*

- h *es inyectivo si y sólo si* $\ker g = \ker k$.
- h *es sobreyectivo si y sólo si* k *es sobreyectivo.*



Demostración. Dado $c \in C$, como g es sobreyectivo, existe $a \in A$ tal que $g(a) = c$. Luego definimos $h(c) = k(a)$.

Debemos probar que esta definición de h es independiente de la elección del elemento a. Supongamos que existe $a' \in A$ tal que $g(a') = c$. Luego $g(a) = g(a')$, de donde $(a, a') \in \ker g \subseteq \ker k$. Luego $k(a) = k(a')$, lo que muestra que nuestra definición de h es buena.

Además, por la definición, es claro que $k = h \circ g$.

Veamos que h es un homomorfismo. Sea f un símbolo de operación n-aria del lenguaje y $c_1, \ldots, c_n \in C$. Sean $a_1, \ldots, a_n \in A$ tales que $g(a_i) = c_i$, $1 \leq i \leq n$. Luego

$$\begin{aligned} h(f^{\mathbf{C}}(c_1, \ldots, c_n)) &= h(f^{\mathbf{C}}(g(a_1), \ldots, g(a_n))) \\ &= h(g(f^{\mathbf{A}}(a_1, \ldots, a_n))) \\ &= k(f^{\mathbf{A}}(a_1, \ldots, a_n)) \\ &= f^{\mathbf{B}}(k(a_1), \ldots, k(a_n)) \\ &= f^{\mathbf{B}}(h(g(a_1)), \ldots, h(g(c_n))) \\ &= f^{\mathbf{B}}(h(c_1), \ldots, h(c_n)) \end{aligned}$$

- Supongamos que h es inyectivo y veamos que $\ker k \subseteq \ker h$. En efecto, si $(a, a') \in \ker k$, entonces $k(a) = k(a')$. Luego $h(g(a)) = h(g(a'))$ y como h es inyectivo, resulta que $g(a) = g(a')$, es decir, $(a, a') \in \ker g$.

  Recíprocamente, supongamos que $\ker g = \ker k$ y veamos que h es inyectivo. Supongamos que $h(c) = h(c')$ para $c, c' \in C$. Sena $a, a' \in A$ tales que $g(a) = c$ y $g(a') = c'$. Luego $h(g(a)) = h(g(a')$, de donde $k(a) = k(a')$, es decir, $(a, a') \in \ker k$. Luego $(a, a') \in \ker g$, es decir, $g(a) = g(a')$, de donde $c = c'$.

- La demostración de que h es sobreyectivo si y sólo si k lo es es muy sencilla y se deja como ejercicio.

■

Proposición 2.23. *Si $h : \mathbf{A} \to \mathbf{B}$ es un homomorfismo, entonces la imagen de h, $h(A)$, es un subuniverso de $\mathbf{B}$.*

Demostración. Sean $a_1, \ldots, a_n \in A$ y f una operación n-aria del lenguaje. Entonces

$$f^{\mathbf{B}}(h(a_1), \ldots, h(a_n)) = h(f^{\mathbf{A}}(a_1, \ldots, a_n)).$$

Esto muestra que $h(A)$ es cerrada bajo f. ■

Corolario 2.24. *Si $h : \mathbf{A} \to \mathbf{B}$ es un homomorfismo, entonces $\mathbf{A}/\ker h$ es isomorfo a una subálgebra de $\mathbf{B}$.*

2.4. Producto directo

Otra construcción básica conocida para los grupos y los anillos que es fácilmente generalizable es la de producto directo. Dadas dos álgebras similares $\mathbf{A}_1$ y $\mathbf{A}_2$, es posible definir operaciones inducidas en el producto cartesiano de sus universos $A_1 \times A_2$ de tal forma que se obtiene una nueva álgebra (similar). En general, tenemos la siguiente definición:

Definición 2.25. *Sea $\{\mathbf{A}_i\}_{i\in I}$ una familia indexada de álgebras similares. Definimos el* **producto directo** *$\mathbf{A} = \prod_{i\in I} \mathbf{A}_i$ como un álgebra cuyo universo es el producto cartesiano $\prod_{i\in I} A_i$ y tal que para cada operación n-aria f y elementos $a_1, \ldots, a_n \in \prod_{i\in I} A_i$ se tiene*

$$f^{\mathbf{A}}(a_1, \ldots, a_n)(i) = f^{\mathbf{A}_i}(a_1(i), \ldots, a_n(i)), \quad i \in I$$

es decir, $f^{\mathbf{A}}$ se define coordenada a coordenada. Si $I = \emptyset$, el producto es el álgebra trivial con universo $\{\emptyset\}$.

Definimos asimismo para cada $j \in I$ la **proyección**

$$\pi_j : \prod_{i\in I} A_i \to A_j$$

de modo que

$$\pi_j(a) = a(j).$$

Ejemplo 2.26. Si $\mathbf{G}_1$ y $\mathbf{G}_2$ son grupos, en el álgebra $\mathbf{G}_1 \times \mathbf{G}_2$ vale, por definición:

- $(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2')$.
- $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$.

Sin embargo, es importante notar que la estructura algebraica (las operaciones) se puede definir sobre el conjunto $G_1 \times G_2$ simplemente porque $\mathbf{G}_1$ y $\mathbf{G}_2$ son álgebras similares. En este caso particular, además, el hecho de que $\mathbf{G}_1$ y $\mathbf{G}_2$ sean grupos implica que $\mathbf{G}_1 \times \mathbf{G}_2$ también es un grupo.

Esto no ocurre con otras clases de estructuras. Por ejemplo, $\mathbb{R}$ es un cuerpo, pero $\mathbb{R} \times \mathbb{R}$ con las operaciones inducidas por las operaciones de $\mathbb{R}$ no es un cuerpo. Esto sucede porque ciertas propiedades son preservadas bajo la formación de productos directos y otras, en cambio, no.

Proposición 2.27. *Dado un producto directo $\mathbf{A} = \prod_{i\in I} \mathbf{A}_i$, cada proyección π_j, $j \in I$, es un homomorfismo sobreyectivo de $\mathbf{A}$ en $\mathbf{A}_j$.*

Demostración. Es claro que π_j es sobreyectiva. Sólo debemos ver que es un homomorfismo. Para esto, sea f una operación n-aria y consideremos $a_1, \ldots, a_n \in A$, luego

$$\begin{aligned} \pi_j(f^{\mathbf{A}}(a_1, \ldots, a_n)) &= f^{\mathbf{A}}(a_1, \ldots, a_n)(j) \\ &= f^{\mathbf{A}_j}(a_1(j), \ldots, a_n(j)) \\ &= f^{\mathbf{A}_j}(\pi_j(a_1), \ldots, \pi_j(a_n)). \end{aligned}$$

■

2.5. Producto subdirecto

Una noción más débil que la de producto directo es la de *producto subdirecto*. Esta noción es de fundamental importancia en álgebra universal porque vamos a ver que podemos obtener un teorema de representación general de cualquier álgebra como producto subdirecto de álgebras especiales, llamadas *subdirectamente irreducibles*.

Definición 2.28. *Un álgebra* $\mathbf{A}$ *es* **producto subdirecto** *de una familia de álgebras* $\{\mathbf{A}_i\}_{i\in I}$ *si verifica las siguientes condiciones:*

(*i*) *existe una inmersión (homomorfismo inyectivo)* $h : \mathbf{A} \to \prod_{i\in I} \mathbf{A}_i$,

(*ii*) *si* $\pi_j : \prod_{i\in I} \mathbf{A}_i \to \mathbf{A}_j$ *es la proyección sobre la* j*-ésima coordenada, entonces la composición* $\pi_j \circ h : \mathbf{A} \to \mathbf{A}_j$ *es sobreyectiva.*

Si $I = \emptyset$, $\mathbf{A}$ *debe ser isomorfa al álgebra trivial con universo* $\{\emptyset\}$.

Definición 2.29. *Un álgebra* $\mathbf{A}$ *es* **subdirectamente irreducible** *si verifica:*

(*i*) $|A| > 1$, *donde* $|A|$ *denota el cardinal del conjunto* A,

(*ii*) *si* $\mathbf{A}$ *es producto subdirecto de* $\{\mathbf{A}_i\}_{i\in I}$ *con inmersión* h, *entonces existe* $j \in I$ *tal que* $\pi_j \circ h$ *es un isomorfismo.*

Si $\mathbb{K}$ es una clase de álgebras similares, indicaremos con $\mathbb{K}_{si}$ a la clase de álgebras subdirectamente irreducibles de $\mathbb{K}$.

La siguiente es una caracterización de las álgebras subdirectamente irreducibles en términos de sus congruencias.

Teorema 2.30. *Un álgebra* $\mathbf{A}$ *es subdirectamente irreducible si y sólo si* $\{\theta \in \operatorname{Con}\mathbf{A} : \theta \neq \Delta\}$ *posee primer elemento, es decir, el conjunto ordenado* $\langle \operatorname{Con}\mathbf{A}, \subseteq\rangle$ *tiene el siguiente aspecto*

Demostración. Sea $\mathbf{A}$ subdirectamente irreducible. Como $|A| > 1$, existen al menos dos congruencias sobre $\mathbf{A}$. Sea $T = \{\theta \in \operatorname{Con}\mathbf{A} : \theta \neq \Delta\}$ y supongamos que T no posee primer elemento. Luego $\bigcap_{\phi\in T} \phi = \Delta$. Consideremos el homomorfismo $h : \mathbf{A} \to \prod_{\phi\in T} \mathbf{A}/\phi$ dado por $h(a) = (a/\phi)_{\phi\in T}$, $a \in A$. Observemos que h es inyectiva, pues si $h(a) = h(b)$, entonces $a/\phi = b/\phi$ para toda $\phi \in T$ y luego $a/\Delta = b/\Delta$, es decir, $a = b$. Además, para cualquier $\phi \in T$, $\pi_\phi \circ h = \nu_\phi$ es sobreyectivo.

Esto muestra que $\mathbf{A}$ es producto subdirecto de las álgebras $\mathbf{A}/\phi$, $\phi \in T$. Como ninguna congruencia en T es la identidad, ninguna aplicación $\pi_\phi \circ h = \nu_\phi$ es inyectiva, lo que contradice el hecho de que $\mathbf{A}$ es subdirectamente irreducible.

Probemos ahora la implicación recíproca. Supongamos que T posee primer elemento y sea θ dicho elemento. Como existen congruencias no triviales sobre $\mathbf{A}$, $|A| > 1$. Supongamos que $\mathbf{A}$ es producto subdirecto de la familia $\{\mathbf{A}_i\}_{i\in I}$ con inmersión $h : \mathbf{A} \to \prod_{i\in I} \mathbf{A}_i$. Luego $\Delta = \ker h = \bigcap_{i\in I} \ker(\pi_i \circ h)$. Debe existir entonces $j \in I$ tal que $\ker(\pi_j \circ h) = \Delta$, es decir, $\pi_j \circ h$ es un isomorfismo. Esto muestra que $\mathbf{A}$ es subdirectamente irreducible. ■

Ejemplo 2.31. Todas las álgebras simples (aquellas que sólo poseen dos congruencias: Δ y ∇) son claramente subdirectamente irreducibles. Pero hay álgebras subdirectamente irreducibles que no son simples. Por ejemplo, dado un primo p el grupo $\mathbb{Z}_{p^2}$ posee tres subgrupos (normales) $N_1 = \{\overline{0}\}$, $N_2 = p\mathbb{Z}_{p^2}$ y $N_3 = \mathbb{Z}_{p^2}$. Por lo tanto, $\mathbb{Z}_{p^2}$ posee exactamente tres congruencias: $\Delta \subset \theta \subset \nabla$. Por el teorema anterior es un grupo subdirectamente irreducible, pero no simple.

De este ejemplo se ve inmediatamente que los grupos $\mathbb{Z}_{p^n}$ para p primo y $n \in \mathbb{N}$ son todos subdirectamente irreducibles. Dado un primo p, también es subdirectamente irreducible el grupo $\mathbb{Z}_{p^\infty}$, consistente en las raíces complejas p^n-ésimas de la unidad con n variando en $\mathbb{N}$.

Más aún, se puede demostrar que todo grupo *abeliano* (i.e. tal que $xy = yx$ para todo $x, y \in G$) subdirectamente irreducible es isomorfo a algún $\mathbb{Z}_{p^n}$ o $\mathbb{Z}_{p^\infty}$. El detalle de la demostración puede verse en C. Bergman, *Universal Algebra, Fundamentals and Selected Topics*, CRC Press, 2012.

El siguiente es un teorema de representación subdirecta debido a G. Birkhoff y constituye uno de los resultados más básicos del álgebra universal.

Teorema 2.32 (G. Birkhoff)**.** *Toda álgebra* $\mathbf{A}$ *es producto subdirecto de álgebras subdirectamente irreducibles, las cuales son imágenes homomorfas de* $\mathbf{A}$*.*

Demostración. Si $|A| = 1$, $\mathbf{A}$ es producto subdirecto de una familia vacía de álgebras subdirectamente irreducibles. Supongamos entonces que $|A| > 1$.

Dados $a, b \in A$, $a \neq b$, consideremos el conjunto

$$T_{a,b} = \{\theta \in \operatorname{Con} \mathbf{A} : (a, b) \notin \theta\}.$$

$T_{a,b}$ está ordenado por la inclusión de conjuntos y es fácil verificar que toda cadena en $T_{a,b}$ está acotada superiormente. Por el Lema de Zorn, debe existir un elemento maximal $\theta_{a,b}$ en $T_{a,b}$.

Veamos que $\mathbf{A}/\theta_{a,b}$ es subdirectamente irreducible. Como $a/\theta_{a,b} \neq b/\theta_{a,b}$, existen congruencias no triviales sobre $\mathbf{A}/\theta_{a,b}$. Sea Φ una de ellas y definamos una relación ϕ sobre A de la siguiente manera

$$(x, y) \in \phi \text{ si y sólo si } (x/\theta_{a,b}, y/\theta_{a,b}) \in \Phi.$$

Es fácil verificar que ϕ es una congruencia sobre $\mathbf{A}$.

Observemos que $\theta_{a,b} \subseteq \phi$ pues si $(x, y) \in \theta_{a,b}$, entonces $x/\theta_{a,b} = y/\theta_{a,b}$ con lo cual $(x/\theta_{a,b}, y/\theta_{a,b}) \in \Phi$ y luego $(x, y) \in \phi$.

Supongamos que $(a/\theta_{a,b}, b/\theta_{a,b}) \notin \Phi$. Entonces $(a, b) \notin \phi$ y por la maximalidad de $\theta_{a,b}$, concluimos que $\theta_{a,b} = \phi$ con lo cual Φ es la identidad sobre $\mathbf{A}/\theta_{a,b}$, contradicción. Luego $(a/\theta_{a,b}, b/\theta_{a,b}) \in \Phi$.

Como $a/\theta_{a,b} \neq b/\theta_{a,b}$ y Φ es arbitraria, hemos probado que

$$\Psi = \bigcap \{\Phi \in \operatorname{Con} \mathbf{A}/\theta_{a,b} : \Phi \neq \Delta\} \neq \Delta.$$

Luego $\mathbf{A}/\theta_{a,b}$ es subdirectamente irreducible.

Consideremos ahora el homomorfismo $h : \mathbf{A} \to \prod_{a \neq b} \mathbf{A}/\theta_{a,b}$ dado por $h(x) = (x/\theta_{a,b})_{a \neq b}$. Se ve fácilmente que $\bigcap_{a \neq b} \theta_{a,b} = \Delta$, y esto implica que h es una inmersión. Además, es claro que $\pi_{a,b} \circ h = \nu_{\theta_{a,b}}$ es sobreyectiva. Esto muestra que $\mathbf{A}$ es producto subdirecto de la familia $\{\mathbf{A}/\theta_{a,b}\}_{a \neq b}$ de álgebras subdirectamente irreducibles. ■

Corolario 2.33. *Toda álgebra finita es producto subdirecto de un número finito de álgebras subdirectamente irreducibles finitas.*

Ejemplo 2.34. Vimos en el Ejemplo 2.31 que todo grupo abeliano subdirectamente irreducible es isomorfo a $\mathbb{Z}_{p^n}$ o a $\mathbb{Z}_{p^\infty}$ para algún primo p (y natural n). El Teorema 2.32, nos asegura entonces que todo grupo ablieano es producto subdirecto de algunos de estos grupos. En particular, todo grupo abeliano es isomorfo a un subgrupo de un producto directo de algunos de estos grupos.

3. Variedades

Para facilitar el estudio de las álgebras conviene agruparlas en clases. Uno de los tipos más importantes de clases de álgebras son las variedades[2], las cuales definimos a continuación. Para ello necesitaremos estudiar ciertos operadores entre clases de álgebras.

Definición 3.1. *Sea $\mathbb{K}$ una clase de álgebras similares. Definimos:*

- *$I(\mathbb{K})$ es la clase de álgebras isomorfas a miembros de $\mathbb{K}$.*
- *$H(\mathbb{K})$ es la clase de imágenes homomorfas de miembros de $\mathbb{K}$.*
- *$S(\mathbb{K})$ es la clase de subálgebras de miembros de $\mathbb{K}$.*
- *$P(\mathbb{K})$ es la clase de productos directos de familias de miembros de $\mathbb{K}$.*

Si $\mathbb{K} = \{\mathbf{A}\}$, escribiremos $I(\mathbf{A})$, $H(\mathbf{A})$, $S(\mathbf{A})$ y $P(\mathbf{A})$, en lugar de $I(\{\mathbf{A}\})$, $H(\{\mathbf{A}\})$, $S(\{\mathbf{A}\})$ y $P(\{\mathbf{A}\})$.

Si O_1 y O_2 son dos operadores entre clases de álgebras (como los cuatro recién definidos), notaremos O_1O_2 a la composición entre estos dos operadores. Escribimos $O_1 \leq O_2$ si $O_1(\mathbb{K}) \subseteq O_2(\mathbb{K})$ para cualquier clase de álgebras $\mathbb{K}$.

Lema 3.2. *Los operadores I, H, S y P verifican:*

- *$SH \leq HS$, $PS \leq SP$, $PH \leq HP$,*
- *$HH = H$, $SS = S$, $IPIP = IP$.*

Demostración. Supongamos que $\mathbf{A} \in SH(\mathbb{K})$. Luego existe un álgebra $\mathbf{B} \in \mathbb{K}$ y un homomorfismo sobreyectivo $h : \mathbf{B} \to \mathbf{C}$ tal que $\mathbf{A} \leq \mathbf{C}$. Es fácil ver que $h^{-1}(\mathbf{A}) \leq \mathbf{B}$, luego $h|_{h^{-1}(\mathbf{A})} : h^{-1}(\mathbf{A}) \to \mathbf{A}$ es un homomorfismo sobreyectivo. Esto muestra que $\mathbf{A} \in HS(\mathbb{K})$.

Consideremos ahora $\mathbf{A} \in PS(\mathbb{K})$. Luego $\mathbf{A} = \prod_{i\in I} \mathbf{A}_i$, donde $\mathbf{A}_i \leq \mathbf{B}_i \in \mathbb{K}$ para $i \in I$. Como $\prod_{i\in I} \mathbf{A}_i \leq \prod_{i\in I} \mathbf{B}_i$, concluimos que $\mathbf{A} \in SP(\mathbb{K})$.

Sea $\mathbf{A} \in PH(\mathbb{K})$. Entonces $\mathbf{A} = \prod_{i\in I} \mathbf{A}_i$ y existen homomorfismos sobreyectivos $h_i : \mathbf{B}_i \to \mathbf{A}_i$ con $\mathbf{B}_i \in \mathbb{K}$, $i \in I$. Es simple ver que la aplicación $h : \prod_{i\in I} \mathbf{B}_i \to \prod_{i\in I} \mathbf{A}_i$ dada por

$$h(b)(i) = h_i(b(i)), \quad i \in I,$$

es un homomorfismo sobreyectivo. Luego $\mathbf{A} \in HP(\mathbb{K})$.

Las tres igualdades restantes se verifican muy fácilmente. ■

Definición 3.3. *Una clase $\mathbb{V}$ de álgebras similares forma una* **variedad** *si es cerrada bajo la formación de imágenes homomorfas, subálgebras y productos directos, es decir, si*

$$H(\mathbb{V}) = S(\mathbb{V}) = P(\mathbb{V}) = \mathbb{V}.$$

Definición 3.4. *Si $\mathbb{V}$ y $\mathbb{W}$ son variedades tales que todo miembro de $\mathbb{W}$ pertenece a $\mathbb{V}$, diremos que $\mathbb{W}$ es una* **subvariedad** *de $\mathbb{V}$.*

Ejemplo 3.5. Sea $\mathbb{G}$ la clase de todos los grupos en lenguaje $\{\cdot, {}^{-1}, 1\}$. Como las subálgebras de los grupos son grupos, las imágenes homomorfas de grupos son grupos y los productos directos de grupos son grupos, concluimos que $\mathbb{G}$ es una variedad.

De la misma manera la clase $\mathbb{A}$ de los anillos es una variedad en el lenguaje $\{+, -, 0, \cdot\}$.

Sin embargo, la clase $\mathbb{K}$ de los cuerpos no es una variedad. En efecto:

[2]No confundir la noción de variedad de álgebra universal con las variedades algebraicas de geometría algebraica o las variedades diferenciables de geometría diferencial.

- $\mathbb{K}$ no es cerrada bajo S: por ejemplo, el cuerpo $\mathbb{R}$ de los números reales posee como subálgebra (respecto del lenguaje de anillos) al anillo $\mathbb{Z}$ de los enteros, que no es un cuerpo.
- $\mathbb{K}$ no es cerrado bajo P: por ejemplo, $\mathbb{R} \times \mathbb{R}$ no es un cuerpo ya que el elemento $(1, 0)$ no posee inverso.

Sin embargo, $\mathbb{K}$ es cerrado trivialmente bajo H. ¿Por qué?

Como la intersección de una clase de variedades es claramente una variedad y como la clase de todas las álgebras sobre un mismo lenguaje constituye una variedad, podemos decir que para toda clase $\mathbb{K}$ de álgebras similares existe la menor variedad que contiene a $\mathbb{K}$.

Definición 3.6. *Si $\mathbb{K}$ es una clase de álgebras similares, sea $V(\mathbb{K})$ la menor variedad que contiene a $\mathbb{K}$. Decimos que $V(\mathbb{K})$ es la* **variedad generada por** $\mathbb{K}$.
Si $\mathbb{K} = \{\mathbf{A}\}$ notaremos $V(\mathbf{A})$ en lugar de $V(\{\mathbf{A}\})$.

Uno de los primeros resultados importantes en el estudio general de las variedades es el siguiente, que caracteriza el operador "variedad generada"en términos de los operadores H, S y P.

Teorema 3.7. *Dada cualquier clase $\mathbb{K}$ de álgebras similares,*

$$V(\mathbb{K}) = HSP(\mathbb{K}).$$

Demostración. Como una variedad es cerrada bajo H, S y P, se sigue inmediatamente que $HSP(\mathbb{K}) \subseteq V(\mathbb{K})$. Para probar la igualdad es suficiente probar que $HSP(\mathbb{K})$ es, de hecho, una variedad. En efecto, por el Lema 3.2 tenemos:

- $H(HSP) = HHSP = HSP$,
- $S(HSP) = SHSP \leq HSSP = HSP$,
- $P(HSP) = PHSP \leq HPSP \leq HSPP \leq HSIPIP = HSIP \leq HSHP \leq HHSP = HSP$.

■

Del Teorema 2.32 se obtiene como corolario el siguiente teorema.

Teorema 3.8. *Toda variedad está generada por las álgebras subdirectamente irreducibles pertenecientes a la variedad, es decir, si $\mathbb{V}$ es un variedad, entonces*

$$\mathbb{V} = V(\mathbb{V}_{si}).$$

Demostración. Como $\mathbb{V}_{si} \subseteq \mathbb{V}$ y $\mathbb{V}$ es una variedad, es claro que $V(\mathbb{V}_{si}) \subseteq \mathbb{V}$. Recíprocamente, si $\mathbf{A} \in \mathbb{V}$, por el Teorema 2.32, $\mathbf{A}$ es producto subdirecto de cierta familia $\{\mathbf{A}_i\}_{i\in I}$ de álgebras subdirectamente irreducibles. Como las álgebras $\mathbf{A}_i$, $i \in I$, son imágenes homomorfas de $\mathbf{A}$, $\mathbf{A}_i \in \mathbb{V}_{si}$ para $i \in I$. Luego $\mathbf{A}$ es isomorfa a una subálgebra del producto directo de la familia $\{\mathbf{A}_i\}_{i\in I}$, es decir, $\mathbf{A} \in ISP(\mathbb{V}_{si}) \subseteq HSP(\mathbb{V}_{si}) = V(\mathbb{V}_{si})$. ■

Ejemplo 3.9. Sea $\mathbb{G}_{ab}$ la clase de los grupos abelianos, es decir, aquellos grupos que satisfacen la igualdad $x \cdot y = y \cdot x$ para todo par de elementos x, y. Es fácil verificar que $\mathbb{G}_{ab}$ es una variedad probando que $\mathbb{G}_{ab}$ es cerrada bajo H, S y P. Además, vimos en el Ejemplo 2.31 que todo grupo abeliano subdirectamente irreducible es isomorfo a $\mathbb{Z}_{p^n}$ o a $\mathbb{Z}_{p^\infty}$ para algún primo p (y natural n). El teorema anterior prueba entonces que

$$\mathbb{G}_{ab} = HSP(\{\mathbb{Z}_{p^n} : p \text{ primo, } n \text{ natural}\} \cup \{\mathbb{Z}_{p^\infty} : p \text{ primo}\}).$$

En este caso, podemos mejorar un poco el resultado observando que los grupos $\mathbb{Z}_{p^n}$ son subgrupos de $\mathbb{Z}_{p^\infty}$. Por lo tanto, para generar la variedad de los grupos abelianos los grupos basta con los $\mathbb{Z}_{p^\infty}$, es decir,

$$\mathbb{G}_{ab} = HSP(\{\mathbb{Z}_{p^\infty} : p \text{ primo}\}).$$

Más aún, se puede probar[3] que $\mathbb{Z}_{p^\infty} \in ISHP(\{\mathbb{Z}_p\})$, con lo cual obtenemos que

$$\mathbb{G}_{ab} = HSP(\{\mathbb{Z}_p : p \text{ primo}\}).$$

Y finalmente, observando que $\mathbb{Z}_p \in H(\mathbb{Z})$ para todo p primo, resulta que

$$\mathbb{G}_{ab} = HSP(\mathbb{Z}).$$

4. Álgebras libres

En esta sección veremos el concepto general de álgebra libre, que generaliza los conceptos conocidos de grupos libres, anillos libres, módulos libres, etc. Veremos además cómo contruir un álgebra libre general y condiciones suficientes sobre una clase de álgebras para que ésta posea álgebra libres.

Definición 4.1. *Sea $\mathbb{K}$ una clase de álgebras similares y sea $\mathbf{U}$ un álgebra similar generada por X (no necesariamente en $\mathbb{K}$).*

- *Si para toda álgebra $\mathbf{A} \in \mathbb{K}$ y para toda aplicación $h : X \to A$, existe un homomorfismo $\overline{h} : \mathbf{U} \to \mathbf{A}$ que extiende a h, decimos que $\mathbf{U}$ es* **libre para $\mathbb{K}$ sobre X**.
- *Si, además, $\mathbf{U} \in \mathbb{K}$, decimos que $\mathbf{U}$ es* **libre en $\mathbb{K}$ sobre X**.

Ejemplo 4.2.

- Un ejemplo paradigmático de álgebra libre la constituyen los espacios vectoriales. Si $\mathbf{V}$ es un $\mathbf{K}$-espacio vectorial y B es una base de $\mathbf{V}$, entonces dado cualquier $\mathbf{K}$-espacio vectorial $\mathbf{W}$ y cualquier aplicación $h : B \to W$, existe un homomorfismo $\overline{h}$ (transformación lineal) de $\mathbf{V}$ en $\mathbf{W}$ que extiende a h.
- $\mathbb{Z}$ es un grupo libre generado por $\{1\}$. En efecto, si $\mathbf{G}$ es un grupo cualquiera y $h : \{1\} \to G$ es una aplicación cualquiera, entonces existe un homomorifsmo $\overline{h} : \mathbb{Z} \to \mathbf{G}$ tal que $\overline{h}(1) = h(1)$. En efecto, basta definir $\overline{h}(k) = h(1)^k$ para $k \in \mathbb{Z}$.
- Los anillos con unidad se definen como álgebras en el lenguaje $\{+, -, 0, \cdot, 1\}$ tales que son anillos respecto de las operaciones $\{+, -, 0, \cdot\}$ y además poseen un elemento distinguido 1 tal que $x \cdot 1 = 1 \cdot x = x$ para todo x.

  $\mathbb{Z}[x]$, el anillo de polinomios con coeficientes enteros en una indeterminada, es un anillo con unidad libre generado por $\{x\}$. En efecto, si tomamos un anillo con unidad arbitrario $\mathbf{A}$ y un elemento arbitrario $a \in A$, podemos definir un homomorfismo $\overline{h} : \mathbb{Z}[x] \to \mathbf{A}$ de la siguiente manera: $\overline{h}(\sum_i k_i x^i) = k_i a^i$.

Lema 4.3. *Sean $\mathbf{A}$ y $\mathbf{B}$ dos álgebras similares y X un conjunto de generadores de $\mathbf{A}$. Si h_1 y h_2 son dos homomorfismos de $\mathbf{A}$ en $\mathbf{B}$ tales que $h_1|_X = h_2|_X$, entonces $h_1 = h_2$.*

[3]Para probarlo podemos usar un teorema importante de teoría de modelos (o de álgebra universal) que puede consultarse en S. Burris, H. P. Sankappanavar, *A Course in Universal Algebra*, Springer-Verlag, 1981 (Teorema 2.14). Dicho teorema afirma, entre otras cosas, que toda álgebra $\mathbf{A}$ pertence a $ISHP$ de sus subálgebras finitamente generadas. En este caso las subálgebras finitamente generadas de $\mathbb{Z}_{p^\infty}$ son todas isomorfas a grupos cíclicos $\mathbb{Z}_{p^n}$.

Demostración. Sea $T = \{x \in A : h_1(x) = h_2(x)\}$. Veamos que T es un subuniverso de $\mathbf{A}$. En efecto, sea f una operación n-aria y consideremos $x_1, \ldots, x_n \in T$, entonces

$$\begin{aligned} h_1(f^{\mathbf{A}}(x_1, \ldots, x_n)) &= f^{\mathbf{B}}(h_1(x_1), \ldots, h_1(x_n)) \\ &= f^{\mathbf{B}}(h_2(x_1), \ldots, h_2(x_n)) \\ &= h_2(f^{\mathbf{A}}(x_1, \ldots, x_n)). \end{aligned}$$

Como $X \subseteq T$ y X genera $\mathbf{A}$, debemos tener $T = A$. Luego $h_1 = h_2$. ■

Una consecuencia inmediata de este lema es la siguiente propiedad de las álgebras libres.

Lema 4.4. *Supongamos que* $\mathbf{U}$ *es libre para* $\mathbb{K}$ *sobre* X*. Entonces dada* $\mathbf{A} \in \mathbb{K}$ *y* $h : X \to A$*, existe una* única *extensión* $\overline{h}$ *de* h *tal que* $\overline{h}$ *es un homomorfismo de* $\mathbf{U}$ *en* $\mathbf{A}$*.*

Teorema 4.5. *Sea* $\mathbb{K}$ *una clase de álgebras y* $\mathbf{U}_1, \mathbf{U}_2$ *dos álgebras* libres en $\mathbb{K}$ *sobre* X_1 *y* X_2*, respectivamente. Si* $|X_1| = |X_2|$*, entonces* $\mathbf{U}_1 \cong \mathbf{U}_2$*.*

Demostración. Primero notemos que, por el lema anterior, la aplicación identidad $id_j : X_j \to X_j$, $j = 1, 2$, tiene como única extensión al homomorfismo identidad de $\mathbf{U}_j$ en $\mathbf{U}_j$, $j = 1, 2$.

Consideremos ahora una biyección $h : X_1 \to X_2$, luego existe un homomorfismo $h_1 : \mathbf{U}_1 \to \mathbf{U}_2$ que extiende a h y un homomorfismo $h_2 : \mathbf{U}_2 \to \mathbf{U}_1$ que extiende a h^{-1}.

El homomorfismo $h_1 \circ h_2 : \mathbf{U}_2 \to \mathbf{U}_2$ extiende a la identidad en X_2, con lo cual $h_1 \circ h_2 = id$. Análogamente, $h_2 \circ h_1 = id$.

Esto muestra que $\mathbf{U}_1 \cong \mathbf{U}_2$. ■

Este teorema asegura que *dentro* de una clase de álgebras $\mathbb{K}$ existe, salvo isomorfismo, a lo sumo un álgebra libre en $\mathbb{K}$ sobre un conjunto de variables con un determinado cardinal.

Bajo ciertas hipótesis sobre la clase $\mathbb{K}$, queremos dar una construcción de álgebras libres en $\mathbb{K}$. Vamos a comenzar construyendo un álgebra libre para todas las álgebras sobre un lenguaje fijo: el álgebra de términos.

Definición 4.6. *Sea* X *un conjunto cuyos elementos llamamos* **variables** *y sea* $\mathcal{L}$ *un lenguaje de álgebras. El conjunto* $T(X)$ *de* **términos** *de tipo* $\mathcal{L}$ *sobre* X*, o* $\mathcal{L}$**-términos**, *se define inductivamente como sigue:*

(*i*) $X \subseteq T(X)$*.*

(*ii*) *Todo símbolo correspondiente a una operación* 0*-aria pertenece a* $T(X)$*.*

(*iii*) *Si* $t_1, t_2, \ldots, t_n \in T(X)$ *y* f *es un símbolo de* $\mathcal{L}$ *correspondiente a una operación* n*-aria, entonces* $f(t_1, \ldots, t_n) \in T(X)$*.*

Si $p \in T(X)$*, escribimos* $p(x_1, \ldots, x_n)$ *para indicar que las variables que aparecen en el término* p *están en el conjunto* $\{x_1, \ldots, x_n\}$*. Decimos entonces que* p *es un término* n**-ario**.

Ejemplo 4.7.

1. Si f es un símbolo unario de $\mathcal{L}$ y x es una variable entonces x, $f(x)$, $f(f(x))$, etc., son $\mathcal{L}$-términos, y si c es una constante en el lenguaje, entonces c, $f(c)$, $f(f(c))$, etc., también lo son.

2. En el lenguaje de los anillos $\mathcal{L} = \{+, \cdot, -, 0\}$, los siguientes son términos sobre las variables $X = \{x, y\}$: 0, x, $0 + 0$, $x \cdot y$, -0, $-(x \cdot (y + x))$, etc.

De forma natural, podemos transformar al conjunto de términos $T(X)$ en un álgebra.

Definición 4.8. *Dado un lenguaje de álgebras $\mathcal{L}$, si $T(X) \neq \emptyset$, entonces el* **álgebra de términos** *de tipo $\mathcal{L}$ sobre X, que escribimos $\mathbf{T}(X)$, tiene como universo al conjunto $T(X)$ y las operaciones fundamentales están dadas por:*

$$f^{\mathbf{T}(X)}(p_1, \ldots, p_n) = f(p_1, \ldots, p_n)$$

para cada $f \in \mathcal{L}$, $p_i \in T(X)$, $1 \leq i \leq n$.

Notemos que en el miembro izquierdo de la ecuación anterior $f^{\mathbf{T}(X)}$ es la operación n-aria definida sobre $T(X)$, mientras que en el miembro derecho f es simplemente un símbolo.

Ejemplo 4.9. Consideremos el lenguaje $\{\cdot\}$ que posee una única operación binaria y el conjunto de variables $X = \{x, y\}$. Entonces $T(X)$ consta de todas las expresiones que podemos armar en ese lenguaje con esas variables, tales como, xy, xx, $x(yx)$, $(xy)(yx)$, $(x(xy))y$, etc. (Aquí, como es costumbre, omitimos el símbolo $\cdot$ por comodidad). ¿Cuál es el resultado de operar el término xy con el término y? Simplemente $(xy)y$.

Teorema 4.10. *Para cualquier lenguaje $\mathcal{L}$ y cualquier conjunto X de variables, si $T(X) \neq \emptyset$, el álgebra de términos $\mathbf{T}(X)$ es libre en la clase de todas las álgebras con lenguaje $\mathcal{L}$ sobre X.*

Demostración. Sea $\mathbf{A}$ un álgebra con lenguaje $\mathcal{L}$ y $h : X \to A$ una aplicación cualquiera. Definimos $\overline{h} : T(X) \to A$ recursivamente por:

- $\overline{h}(x) = h(x)$ para $x \in X$.
- $\overline{h}(c) = c^{\mathbf{A}}$ si c es una operación 0-aria.
- $\overline{h}(f(t_1, \ldots, t_n)) = f^{\mathbf{A}}(\overline{h}(t_1), \ldots, \overline{h}(t_n))$, para $t_1, \ldots, t_n \in T(X)$ y f un símbolo de operación n-aria.

Claramente $\overline{h}$ extiende a h y es un homomorfismo por su definición. ■

Como consecuencia del teorema anterior, el álgebra de términos $\mathbf{T}(X)$ es libre para cualquier clase de álgebras $\mathbb{K}$ del tipo correspondiente. Desearíamos hallar un álgebra libre *en* $\mathbb{K}$. Esto no siempre es posible.

Veremos que podemos construir un álgebra libre para $\mathbb{K}$ que pertenece a $ISP(\mathbb{K})$. Por lo tanto, si $\mathbb{K}$ es cerrada bajo I, S y P (en particular, si $\mathbb{K}$ es una variedad), posee álgebras libres.

Definición 4.11. *Sea $\mathbb{K}$ una clase de álgebras con lenguaje $\mathcal{L}$. Dado un conjunto X de variables, definimos la congruencia $\theta_{\mathbb{K}}(X)$ sobre $\mathbf{T}(X)$ por*

$$\theta_{\mathbb{K}}(X) = \bigcap_{\phi \in \Phi_{\mathbb{K}}(X)} \phi$$

donde

$$\Phi_{\mathbb{K}}(X) = \{\phi \in \operatorname{Con} \mathbf{T}(X) : \mathbf{T}(X)/\phi \in IS(\mathbb{K})\}.$$

Luego definimos $\mathbf{F}_{\mathbb{K}}(\overline{X})$ como

$$\mathbf{F}_{\mathbb{K}}(\overline{X}) = \mathbf{T}(X)/\theta_{\mathbb{K}}(X),$$

donde

$$\overline{X} = \{x/\theta_{\mathbb{K}}(X) : x \in X\}.$$

Observación 4.12.

(1) Como X genera $\mathbf{T}(X)$, $\overline{X}$ genera $\mathbf{F}_{\mathbb{K}}(\overline{X})$.

(2) Si $\mathbb{K}$ contiene un álgebra no trivial $\mathbf{A}$, las variables de X no están relacionadas entre sí mediante la congruencia $\theta_{\mathbb{K}}(X)$ pues dados $x, y \in X$, $x \neq y$, existe un homomorfismo $h : \mathbf{T}(X) \to \mathbf{A}$ tal que $h(x) \neq h(y)$ y luego $\ker h \in \Phi_{\mathbb{K}}(X)$ es una congruencia que separa x e y. Por lo tanto, en este caso tenemos que $|\overline{X}| = |X|$.

(3) Si $|X| = |Y|$, entonces claramente $\mathbf{F}_{\mathbb{K}}(\overline{X}) \cong \mathbf{F}_{\mathbb{K}}(\overline{Y})$ bajo un isomorfismo que aplica $\overline{X}$ en $\overline{Y}$ pues $\mathbf{T}(X) \cong \mathbf{T}(Y)$ bajo un isomorfismo que aplica X en Y. Luego $\mathbf{F}_{\mathbb{K}}(\overline{X})$ está determinada, salvo isomorfismo, por $\mathbb{K}$ y $|X|$.

Teorema 4.13 (G. Birkhoff)**.** $\mathbf{F}_{\mathbb{K}}(\overline{X})$ *es libre para* $\mathbb{K}$ *sobre* $\overline{X}$*.*

Demostración. Dada $\mathbf{A} \in \mathbb{K}$, sea $h : \overline{X} \to A$ una aplicación cualquiera. Sea $\nu : \mathbf{T}(X) \to \mathbf{F}_{\mathbb{K}}(\overline{X})$ la aplicación canónica. Entonces $h \circ \nu$ aplica X en A, y luego, como $\mathbf{T}(X)$ es libre para cualquier álgebra, existe un homomorfismo $g : \mathbf{T}(X) \to \mathbf{A}$ que extiende a $h \circ \nu|_X$.

Por el Teorema de Isomorfismo, $\ker g \in \Phi_{\mathbb{K}}(X)$ y luego $\ker \nu = \theta_{\mathbb{K}}(X) \subseteq \ker g$. Es fácil ver entonces que existe un homomorfismo $\overline{h} : \mathbf{F}_{\mathbb{K}}(\overline{X}) \to \mathbf{A}$ definido por $g = \overline{h} \circ \nu$. Dicho homomorfismo verifica

$$\overline{h}(\overline{x}) = (\overline{h} \circ \nu)(x) = g(x) = (h \circ \nu)(x) = h(\overline{x}),$$

con lo cual $\overline{h}$ extiende a h. Esto muestra que $\mathbf{F}_{\mathbb{K}}(\overline{X})$ es libre para $\mathbb{K}$ sobre $\overline{X}$. ■

Si $\mathbf{F}_{\mathbb{K}}(\overline{X}) \in \mathbb{K}$, por el Teorema 4.5, es entonces, salvo isomorfismo, la única álgebra libre en $\mathbb{K}$ sobre un conjunto de generadores de cardinal $|\overline{X}|$.

Teorema 4.14 (G. Birkhoff)**.** *Si* $\mathbb{K}$ *es una clase no vacía de álgebras similares, entonces* $\mathbf{F}_{\mathbb{K}}(\overline{X}) \in ISP(\mathbb{K})$*. Por lo tanto, si* $\mathbb{K}$ *es cerrada bajo* I*,* S *y* P*, en particular si* $\mathbb{K}$ *es una variedad, entonces* $\mathbf{F}_{\mathbb{K}}(\overline{X}) \in \mathbb{K}$*.*

Demostración. Para cada $\phi \in \Phi_{\mathbb{K}}(X)$, sea $\nu_\phi : \mathbf{T}(X) \to \mathbf{T}(X)/\phi$ el homomorfismo canónico. Definimos un homomorfismo

$$h : \mathbf{T}(X) \to \prod_{\phi \in \Phi_{\mathbb{K}}(X)} \mathbf{T}(X)/\phi$$

dado por

$$h(t) = (\nu_\phi(t))_{\phi \in \Phi_{\mathbb{K}}(X)}$$

para cada $t \in T(X)$.

Es fácil ver que

$$\ker h = \bigcap_{\phi \in \Phi_{\mathbb{K}}(X)} \phi = \theta_{\mathbb{K}}(X).$$

Luego, por el Teorema de Isomorfismo,

$$\mathbf{F}_{\mathbb{K}}(\overline{X}) = \mathbf{T}(X)/\theta_{\mathbb{K}}(X) \cong h(\mathbf{T}(X)) \leq \prod_{\phi \in \Phi_{\mathbb{K}}(X)} \mathbf{T}(X)/\phi.$$

Por lo tanto,

$$\mathbf{F}_{\mathbb{K}}(\overline{X}) \in ISP(\{\mathbf{T}(X)/\phi : \phi \in \Phi_{\mathbb{K}}(X)\}).$$

Como $\mathbf{T}(X)/\phi \in IS(\mathbb{K})$ para cada $\phi \in \Phi_{\mathbb{K}}(X)$, concluimos que

$$\mathbf{F}_{\mathbb{K}}(\overline{X}) \in ISPIS(\mathbb{K}).$$

Finalmente, se puede mostrar fácilmente que $ISPIS \leq ISPS$ y, aplicando el Lema 3.2, tenemos que $ISPIS \leq ISPS \leq ISSP = ISP$. Luego

$$\mathbf{F}_{\mathbb{K}}(\overline{X}) \in ISP(\mathbb{K}).$$

■

Observación 4.15. Este teorema asegura que toda variedad posee álgebras libres para cualquier cardinal. En particular, asegura la existencia de grupos libres y anillos libres. Un problema típico en álgebra universal es buscar, bajo condiciones más restrictivas o en un caso particular, una descripción concreta y útil de las álgebras libres. Lamentablemente esto no siempre es posible, pero, a pesar de ello, las álgebras libres son un objeto muy útil a la hora de probar propiedades de las álgebras con que uno está trabajando. En la sección siguiente veremos como las álgebras libres son la clave para demostrar el Teorema de Birkhoff.

5. Identidades y el teorema de Birkhoff

En esta sección vamos a demostrar uno de los primeros teoremas importantes del álgebra universal, probado por G. Birkhoff (1935), resultado que impulsó en gran medida el desarrollo de esta disciplina. Este resultado afirma que las variedades (clases cerradas bajo H, S y P) son exactamente aquellas clases de álgebras caracterizables mediantes identidades (ecuaciones).

Vamos primero a formalizar el concepto de identidad y de que un álgebra satisfaga una identidad para probar luego el Teorema de Birkhoff.

Definición 5.1. *Dado un término $p(x_1, \dots, x_n)$ de tipo $\mathcal{L}$ sobre algún conjunto X y dada un álgebra $\mathbf{A}$ con lenguaje $\mathcal{L}$, definimos la aplicación $p^{\mathbf{A}} : A^n \to A$ como sigue:*

- *si p es una variable x_i, entonces*
$$p^{\mathbf{A}}(a_1, \dots, a_n) = a_i$$
para todo $a_1, \dots, a_n \in A$;
- *si p es de la forma $f(p_1(x_1, \dots, x_n), \dots, p_k(x_1, \dots, x_n))$ donde f es un símbolo k-ario del lenguaje $\mathcal{L}$, entonces*
$$p^{\mathbf{A}}(a_1, \dots, a_n) = f^{\mathbf{A}}(p_1^{\mathbf{A}}(a_1, \dots, a_n), \dots, p_k^{\mathbf{A}}(a_1, \dots, a_n))$$
para todo $a_1, \dots, a_n \in A$. En particular si $p = f$ un símbolo 0-ario, entonces $p^{\mathbf{A}} = f^{\mathbf{A}}$.

Definición 5.2. *Dado un lenguaje de álgebras $\mathcal{L}$, una* **identidad** *de tipo $\mathcal{L}$ sobre un conjunto de variables X es una expresión de la forma $p \approx q$ donde $p, q \in T(X)$.*

Un álgebra $\mathbf{A}$ con lenguaje $\mathcal{L}$ **satisface** *una identidad $p(x_1, \dots, x_n) \approx q(x_1, \dots, x_n)$ si para cualesquiera $a_1, \dots, a_n \in A$, se verifica $p^{\mathbf{A}}(a_1, \dots, a_n) = q^{\mathbf{A}}(a_1, \dots, a_n)$ donde $p^{\mathbf{A}}$ y $q^{\mathbf{A}}$ son las funciones que corresponden en el álgebra $\mathbf{A}$ a los términos p y q, respectivamente. Escribimos $\mathbf{A} \models p \approx q$.*

Una clase $\mathbb{K}$ de álgebras satisface $p \approx q$ y escribimos $\mathbb{K} \models p \approx q$ si toda álgebra de $\mathbb{K}$ satisface $p \approx q$.

Lema 5.3. *Dada una clase $\mathbb{K}$ de álgebras con lenguaje $\mathcal{L}$ y dados dos términos $p, q \in T(X)$ de tipo $\mathcal{L}$, se tiene que las siguientes condiciones son equivalentes:*

(I) $\mathbb{K} \models p \approx q$.

(II) $\mathbf{F}_{\mathbb{K}}(\overline{X}) \models p \approx q$.

(III) $(p, q) \in \theta_{\mathbb{K}}(X)$.

Demostración. Sea $\mathbf{F} = \mathbf{F}_{\mathbb{K}}(\overline{X})$, $p = p(x_1, \dots, x_n)$, $q = q(x_1, \dots, x_n)$, y consideremos la aplicación canónica $\nu : \mathbf{T}(X) \to \mathbf{F}$.

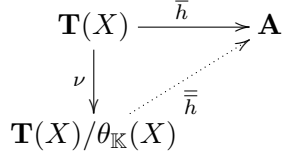
- Supongamos que $\mathbb{K} \models p \approx q$. Como $\mathbf{F} \in ISP(\mathbb{K})$, es fácil demostrar que entonces $\mathbf{F} \models p \approx q$.
- Si $\mathbf{F} \models p \approx q$, en particular debemos tener que
$$p^{\mathbf{F}}(x_1/\theta_{\mathbb{K}}(X), \dots, x_n/\theta_{\mathbb{K}}(X)) = q^{\mathbf{F}}(x_1/\theta_{\mathbb{K}}(X), \dots, x_n/\theta_{\mathbb{K}}(X)),$$
es decir,
$$p(x_1, \dots, x_n)/\theta_{\mathbb{K}}(X) = q(x_1, \dots, x_n)/\theta_{\mathbb{K}}(X).$$

- Finalmente, si $(p,q) \in \theta_{\mathbb{K}}(X)$, entonces $\nu(p) = \nu(q)$. Debemos probar entonces que $\mathbb{K} \models p \approx q$. Para ello, sea $\mathbf{A} \in \mathbb{K}$ y $a_1, \ldots, a_n \in A$.

  Sea $h : X \to A$ una aplicación cualquiera tal que $h(x_i) = a_i$ para $1 \leq i \leq n$. Como el álgebra de términos $\mathbf{T}(X)$ es libre para $\mathbb{K}$, existe un homomorfismo $\overline{h} : \mathbf{T}(X) \to \mathbf{A}$ que extiende la función h. Luego, por el Primer Teorema de Isomorfismo, $\mathbf{T}(X)/\ker \overline{h} \cong \overline{h}(\mathbf{T}(X)) \leq \mathbf{A}$. Entonces $\mathbf{T}(X)/\ker \overline{h} \in IS(\mathbf{A})$. Esto significa, por definición, que $\ker \overline{h} \in \Phi_{\mathbb{K}}(X)$, con lo cual

  $$\theta_{\mathbb{K}}(X) \subseteq \ker \overline{h}.$$

  Utilizando ahora el Teorema 2.22, obtenemos que existe un homomorfismo $\overline{\overline{h}} : \mathbf{T}(X)/\theta_{\mathbb{K}}(X) \to \mathbf{A}$ tal que $\overline{h} = \overline{\overline{h}} \circ \nu$.

  Luego,

  $$\begin{aligned} p^{\mathbf{A}}(a_1, \ldots, a_n) &= p^{\mathbf{A}}(\overline{h}(x_1), \ldots, \overline{h}(x_n)) \\ &= \overline{h}(p^{\mathbf{T}(X)}(x_1, \ldots, x_n)) \\ &= \overline{\overline{h}}(\nu(p^{\mathbf{T}(X)}(x_1, \ldots, x_n))) \\ &= \overline{\overline{h}}(\nu(q^{\mathbf{T}(X)}(x_1, \ldots, x_n))) \\ &= \overline{h}(q^{\mathbf{T}(X)}(x_1, \ldots, x_n)) \\ &= q^{\mathbf{A}}(\overline{h}(x_1), \ldots, \overline{h}(x_n)) \\ &= q^{\mathbf{A}}(a_1, \ldots, a_n). \end{aligned}$$

  Esto muestra que $\mathbf{A} \models p \approx q$ para cualquier $\mathbf{A} \in \mathbb{K}$.

■

Definición 5.4.

- *Dada una clase de álgebras similares* $\mathbb{K}$*, denotamos con* $Id(\mathbb{K})$ *al conjunto de todas las identidades válidas en* $\mathbb{K}$*.*
- *Sea* Σ *un conjunto de identidades sobre un lenguaje* $\mathcal{L}$*, definimos* $Mod(\Sigma)$ *como la clase de álgebras* $\mathbf{A}$ *que satisfacen las identidades en* Σ*.*
- *Una clase* $\mathbb{K}$ *de álgebras es una* **clase ecuacional** *si existe un conjunto de identidades* Σ *tal que* $\mathbb{K} = Mod(\Sigma)$*. En este caso, decimos que* $\mathbb{K}$ *está* **definida** *o* **axiomatizada** *por* Σ*.*

Estamos ya en condiciones de probar uno de los principales resultados del álgebra universal.

Teorema 5.5 (G. Birkhoff)**.** *Una clase* $\mathbb{K}$ *de álgebras es una clase ecuacional si y sólo si es una variedad.*

Demostración. Si $\mathbb{K}$ es una clase ecuacional es fácil ver que es cerrada bajo H, S y P, pues basta con verificar que la validez de una identidad se preserva bajo la formación de imágenes homomorfas, subálgebras y productos directos. (Ejercicio)

Supongamos ahora que $\mathbb{K}$ es una variedad y veamos que existe un conjunto de identidades Σ tal que $\mathbb{K} = Mod(\Sigma)$.

Sea $\Sigma = Id(\mathbb{K})$, es decir, el conjunto de todas las identidades válidas en todas las álgebras de la clase $\mathbb{K}$. Vamos a probar que $\mathbb{K} = Mod(\Sigma)$.

Claramente $\mathbb{K} \subseteq Mod(\Sigma)$. Para ver la recíproca, consideremos un álgebra $\mathbf{A} \in Mod(\Sigma)$. Sea X un conjunto suficientemente grande como para que existe una función *sobreyectiva* $h : X \to A$. Como el álgebra de términos $\mathbf{T}(X)$ es libre para todas las álgebras sobre el mismo lenguaje, h se puede extender a un homomorfismo $\overline{h} : \mathbf{T}(X) \to \mathbf{A}$, que resultará sobreyectivo claramente.

Recordemos que, como $\mathbb{K}$ es cerrada bajo I, S y P, posee álgebras libres y, concretamente, $\mathbf{F}_{\mathbb{K}}(\overline{X}) \in \mathbb{K}$. Sea $\nu : \mathbf{T}(X) \to \mathbf{F}_{\mathbb{K}}(\overline{X})$ la aplicación canónica.

Afirmamos que $\ker \nu \subseteq \ker \overline{h}$. En efecto, usando el Lema 5.3,

$$\begin{aligned}
(p,q) \in \ker \nu &\Longrightarrow \nu(p) = \nu(q) \\
&\Longrightarrow p/\theta_{\mathbb{K}}(X) = q/\theta_{\mathbb{K}}(X) \\
&\Longrightarrow \mathbb{K} \models p \approx q \\
&\Longrightarrow (p \approx q) \in \Sigma \\
&\Longrightarrow \mathbf{A} \models p \approx q \\
&\Longrightarrow p^{\mathbf{A}}(\overline{h}(x_1), \ldots, \overline{h}(x_n)) = q^{\mathbf{A}}(\overline{h}(x_1), \ldots, \overline{h}(x_n)) \\
&\Longrightarrow \overline{h}(p^{\mathbf{T}(X)}(x_1, \ldots, x_n)) = \overline{h}(q^{\mathbf{T}(X)}(x_1, \ldots, x_n)) \\
&\Longrightarrow (p,q) \in \ker \overline{h}.
\end{aligned}$$

Luego existe un homomorfismo $\overline{\overline{h}} : \mathbf{F}_{\mathbb{K}}(\overline{X}) \to \mathbf{A}$, que es sobreyectivo por serlo $\overline{h}$. Luego $\mathbf{A}$ es una imagen homomorfa de un álgebra libre $\mathbf{F}_{\mathbb{K}}(\overline{X})$ que está en $\mathbb{K}$. Como $\mathbb{K}$ es una variedad, $\mathbf{A} \in \mathbb{K}$. ■

Ejemplo 5.6. Vimos en el Ejemplo 3.5 que la clase $\mathbb{G}$ de los grupos es una variedad por ser cerrada bahi H, S y P. Luego debe haber un conjunto de ecuaciones que los definan. En este caso, es muy fácil hallar dicho conjunto porque resulta inmediato de la definición que dimos de grupos:

- $x \cdot (y \cdot z) \approx (x \cdot y) \cdot z$.
- $x \cdot 1 \approx x$.
- $1 \cdot x \approx x$.
- $x \cdot x^{-1} \approx 1$.
- $x^{-1} \cdot x \approx 1$.

Ejemplo 5.7. Vimos ya que la clase $\mathbf{K}$ de los cuerpos no es una variedad porque no es cerrada bajo la formación de subálgebras ni productos directos. El teorema anterior nos dice entonces que es imposible dar una caracterización de los cuerpos utilizando únicamente identidades. Si observamos la definición de cuerpo, detectamos que la condición:

- para todo $x \in K$, $x \neq 0$, existe $y \in K$ tal que $xy = 1$,

no es una identidad ni es equivalente a una identidad.