Teorema de Wedderburn-Artin.

Escuela Precimpa 2014. Coclé. Panamá.

Dolores Martín Barquero

CHAPTER 1

Teorema de Wedderburn-Artin

1. Anillos

Un anillo es una estructura algebraica formada por un conjunto, R, y dos operaciones, $(R, +, \cdot)$, de forma que $(R, +)$ es un grupo conmutativo con elemento neutro que denotaremos por 0, y la segunda operación es asociativa ($(R, \cdot)$ es un semigrupo) y distributiva con respecto a la primera. Si la segunda operación es conmutativa, se dice que el anillo es conmutativo y si el anillo posee elemento neutro para esta operación se dice que es un anillo con unidad o anillo unitario. Históricamente, el conjunto $\mathbb{Z}$ de los enteros con sus dos operaciones sirvió de base para la formulación del concepto de anillo, en este caso se trata de un anillo conmutativo unitario. Un subanillo S de un anillo R es un subconjunto $S \subset R$ que verifica que es cerrado para las dos operaciones de R. Si el anillo es unitario se exigirá además que $1 \in S$. A veces, por comodidad, suprimiremos la segunda operación $(\cdot)$ por la simple concatenación. A lo largo de este tema, entenderemos por anillo a un anillo con unidad 1, no necesariamente conmutativo. Para anillos conmutativos es importante considerar los ideales del anillo. Para el caso no conmutativo tenemos que diferenciar entre ideales por la izquierda e ideales por la derecha. Cuando hablemos simplemente de ideal de R esto significará que se trata de un ideal bilátero, es decir, un ideal por la izquierda y por la derecha.

Un subconjunto I de un anillo R se dice que es un ideal por la izquierda de R si $(I, +)$ es un subgrupo de $(R, +)$ y dados cualesquiera $r \in R$ y $x \in I$ se tiene que $r \cdot x \in I$. De forma análoga se define el concepto de ideal por la derecha. Un ideal no tiene por qué ser necesariamente un subanillo, por ejemplo, en $(\mathbb{Z}, +, \cdot)$, el conjunto $2\mathbb{Z}$ es un ideal pero no es un subanillo.

Dados dos anillos R y S, diremos que una aplicación $f\colon R \to S$ es un homomorfismo de anillos si se cumplen las siguientes condiciones:

i): $f(a + b) = f(a) + f(b)$, para cualesquiera a y b en R.
ii): $f(a \cdot b) = f(a) \cdot f(b)$, para cualesquiera a y b en R.

Si R y S son anillos unitarios, con unidades 1_R y 1_S respectivamente, entonces la aplicación f se dirá que es un homomorfismo de anillos unitarios si es un homomorfismo de anillos y además se verifica

iii): $f(1_R) = 1_S$.

Así, $\mathrm{Im}(f)$ es un subanillo de S y $\mathrm{Ker}(f)$ es un ideal de R.

Un elemento a de un anillo R se dice inversible por la derecha si existe un elemento $b \in R$ tal que $a \cdot b = 1$. A este elemento b se le llama inverso

por la derecha del elemento a. De forma similar se definen los elementos inversibles por la izquierda y los inversos por la izquierda. Si a tiene inverso por la derecha b e inverso por la izquierda b', entonces

$$b' = b'(ab) = (b'a)b = b.$$

En este caso, decimos que a es inversible (o una unidad) en R y $b = b'$ es el inverso de a. El conjunto formado por los elementos inversibles de un anillo unitario $(R, +, \cdot)$, es un grupo con respecto de la multiplicación del anillo que recibe el nombre de grupo de unidades de R y es denotado por $\mathcal{U}(R)$, o a veces por R^*. Si $a \in R$ tiene un inverso por la derecha b, entonces $a \in \mathcal{U}(R)$ si y solo si $ba = 1$. Veamos un ejemplo de un anillo que posee elementos inversibles por la derecha pero no por la izquierda, y el conocido caso en que todos los elementos inversibles por un lado lo son también por el otro.

EJEMPLOS 1. Consideremos el espacio vectorial sobre el cuerpo K, $\oplus_{i\in\mathbb{N}^*} Ke_i$, donde $B = \{e_i \colon i \in \mathbb{N}^*\}$ es una base infinito numerable. Sea $R = \mathrm{End}_K(V)$ la K-álgebra de los endomorfismos sobre el K-espacio vectorial V. Si a y b son los elementos de R definidos sobre la base en la foma:

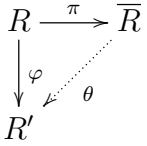
$$b(e_i) = e_{i+1}, \text{ para todo } i \geq 1, \text{ y}$$
$$a(e_1) = 0, \;\; a(e_i) = e_{i-1} \text{ para todo } i \geq 2,$$

entonces $ab = 1 \neq ba$.

Por otra parte, es sabido que si V es un espacio vectorial de dimensión finita sobre un cuerpo K entonces en $\mathrm{End}_K(V)$ todo elemento inversible por un lado lo es por el otro.

Dado un ideal I de R podemos considerar el anillo cociente $\overline{R} := R/I$ y tenemos el homomorfismo sobreyectivo natural, $\pi \colon R \to \overline{R}$ con $\pi(a) = \overline{a} = a + I \in \overline{R}$.

El núcleo de este homomorfismo es el ideal I y el anillo cociente $\overline{R}$ tiene la propiedad universal de que para cualquier homomorfismo de anillos $\varphi \colon R \to R'$ con $\varphi(I) = 0$, existe un único homomorfismo θ tal que el siguiente diagrama conmuta:



DEFINICIÓN 1. *Un anillo no nulo R se dirá simple si los únicos ideales del mismo son (0) y R.*

Un anillo no nulo R es simple si y solo si, para todo $0 \neq a \in R$, existe una expresión $\sum b_i a c_i = 1$ para adecuados $b_i, c_i \in R$. Usando este resultado es fácil comprobar que si R es conmutativo, entonces R es simple si y solo si R es un cuerpo.

DEFINICIÓN 2. *Un elemento no nulo $a \in R$ se dice que es un divisor de cero por la izquierda si existe un elemento no nulo $b \in R$ tal que $ab = 0$.*

Los divisores de cero por la derecha se definen de forma análoga. Para anillos conmutativos se hablará simplemente de divisores de cero. Si R es un anillo no conmutativo, un divisor de cero por la izquierda no necesariamente es un divisor de cero por la derecha.

EJEMPLOS 2. Consideremos R el anillo $\begin{pmatrix} \mathbb{Z} & \mathbb{Z}_2 \\ 0 & \mathbb{Z} \end{pmatrix}$, es decir, el anillo de matrices 2×2 formado por las matrices de la forma $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$, con $x, z \in \mathbb{Z}$ e $y \in \mathbb{Z}_2$ con la suma y el producto habituales.

Consideremos los elementos $a = \begin{pmatrix} 2 & \overline{0} \\ 0 & 1 \end{pmatrix}$ y $b = \begin{pmatrix} 0 & \overline{1} \\ 0 & 0 \end{pmatrix}$, está claro que $ab = 0 \in R$, por lo tanto a es un divisor de cero por la izquierda. Sin embargo, a no es un divisor de cero por la derecha ya que

$$0 = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} 2 & \overline{0} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2x & y \\ 0 & z \end{pmatrix}.$$

Así tenemos $x = z = 0$ e $y = \overline{0} \in \mathbb{Z}_2$. Observemos que $b^2 = 0$, luego b es un divisor de cero por la izquierda y por la derecha.

DEFINICIÓN 3. *Un anillo R se dice un dominio si $R \neq 0$ y $a, b \in R$ con $ab = 0$, entonces $a = 0$ o $b = 0$.*

En un dominio R no hay divisores de cero por la izquierda o por la derecha. Más adelante estudiamos brevemente el anillo de los cuaterniones de Hamilton que nos proporciona un ejemplo de dominio no conmutativo. Un anillo R se dice reducido si no tiene elementos nilpotentes no nulos, o, equivalentemente, si $a^2 = 0$ implica $a = 0$. La suma directa de cualquier familia de dominios es un anillo reducido.

Dado un anillo R definiremos el anillo opuesto de R, denotado por R^{op}, como el anillo que consta de los mismos elementos de R con la multiplicación $\cdot^{op}$ definida en la forma:

$$a \cdot^{op} b = b \cdot a, \text{ para cualesquiera } a, b \in R.$$

2. Condiciones de cadena

Recordemos algunas definiciones.

DEFINICIÓN 4. *Una familia $\{A_i : i \in I\}$ de subconjuntos de un conjunto A, se dice que satisface la condición de cadena ascendente (ACC) si no existe en la familia una cadena infinita estrictamente ascendente*

$$A_{i_1} \subsetneq A_{i_2} \subsetneq \cdots$$

Esta definición puede formularse de dos formas equivalentes:

: i) Para cualquier cadena ascendente en la familia $A_{i_1} \subset A_{i_2} \subset \cdots$, existe un natural n tal que $A_{i_n} = A_{i_{n+1}} = A_{i_{n+2}} = \cdots$.

: ii) Toda subfamilia no vacía de una familia dada tiene elemento maximal respecto de la inclusión.

La definición de cadena descendente (DCC) para una familia de subconjuntos de A se define de forma análoga y tiene sus definiciones equivalentes análogas a i) y ii).

DEFINICIÓN 5. *Sea R un anillo y M cualquier R-módulo por la izquierda o por la derecha. Diremos que M es noetheriano (respectivamente artiniano) si la familia de todos los submódulos de M satisface la condición de cadena ascendente ACC (respectivamente DCC).*

De forma más breve diremos que M satisface ACC (respectivamente DCC) sobre submódulos.

OBSERVACIÓN 1. Es sabido que:

(1) M es noetheriano si y sólo si todo submódulo de M es finitamente generado.
(2) M es noetheriano y artiniano si y sólo si M tiene una serie de composición finita,
(3) Sea N un submódulo de M. Entonces M es noetheriano (respectivamente artiniano) si y sólo si N y M/N son noetherianos (respectivamente artinianos). En particular, la suma directa de dos módulos noetherianos (respectivamente artinianos) es noetheriana (respectivamente artiniana).

Un anillo R se dirá noetheriano por la izquierda (respectivamente por la derecha) si R es noetheriano visto como R-módulo por la izquierda (respectivamente por la derecha). Si R es noetheriano por la izquierda y por la derecha diremos simplemente que es noetheriano. Podemos consultar ejemplos en los que se puede observar que el carácter noetheriano por la izquierda y por la derecha son independientes (veáse [**5**], pág. 19). Así, la condición de que un anillo sea noetheriano es mucho más fuerte que ser noetheriano por un lado.

3. Módulos simples y semisimples. Anillos semisimples

Comenzaremos por estudiar los anillos semisimples que serán objeto de nuestro teorema de estructura.

DEFINICIÓN 6. *Sea R un anillo, y M un R-módulo por la izquierda.*

(1) *Diremos que M es un R-módulo simple o irreducible si $M \neq 0$ y no tiene más R-submódulos que (0) y M.*
(2) *Diremos que M es un R-módulo semisimple o completamente reducible si cada R-submódulo de M es un sumando directo de M.*

Obsérvese que el módulo cero es semisimple pero no simple. Evidentemente Si ${}_RM$ es simple entonces también es semisimple.

LEMA 1. *Sea M un R-módulo por la izquierda. Son equivalentes:*

(1) *M es semisimple.*
(2) *Todo submódulo de M es semisimple.*

DEMOSTRACIÓN . Evidentemente $(2) \Rightarrow (1)$. Veamos la otra implicación. Sea N un submódulo de M veamos que es semisimple. Consideremos un submódulo T de N, por ser M semisimple tenemos $M = N \oplus N'$ y $M = T \oplus T'$, veamos que $N = T \oplus (T' \cap N)$. Es claro que $T \oplus (T' \cap N) \subset N$. Por otra parte, si $n \in N \subset M$, entonces $n = t + t'$ con $t \in T$ y $t' \in T'$. Como $t' = n - t \in N$ tenemos $t' \in T' \cap N$, luego $N \subset T \oplus (T' \cap N)$. □

LEMA 2. *Todo cociente de un R-módulo semisimple es semisimple.*

DEMOSTRACIÓN . Sea M un R-módulo semisimple y N un submódulo de M. Veamos que M/N es semisimple. Sea H/N un submódulo de M/N, luego $N \subseteq H \subseteq M$. Por ser M semisimple tenemos $M = H \oplus H'$. Veamos $M/N = H/N \oplus (H' + N)/N$. Como $m = h + h'$, entonces $m + N = h + N + h' + N$, luego $M/N = H/N + (H' + N)/N$. Si $x + N \in (H/N) \cap ((H' + N)/N)$, entonces $x \in H \cap (H' + N)$, por tanto, $x = h' + n$ con $h' \in H'$ y $n \in N$. Tenemos $x - n \in H \cap H' = (0)$, así $x = n$ y $x + N = N$.□

LEMA 3. *Todo R-módulo por la izquierda semisimple no nulo M contiene un submódulo simple.*

DEMOSTRACIÓN . Sea m un elemento no nulo fijo de M. Es suficiente considerar el caso $M = R \cdot m$ ya que si este R-módulo (semisimple ya que M lo es) tiene un submódulo simple, entonces nuestro M inicial también lo tendrá. Consideremos la familia $\mathcal{F} = \{N \leq M / m \notin N\}$. Como $m \neq 0$ se tiene $m \notin \{0\}$ luego $\mathcal{F} \neq \emptyset$ ya que $\{0\} \in \mathcal{F}$. Consideramos el conjunto ordenado $(\mathcal{F}, \subset)$. Toda cadena $\{N_\alpha\}_{\alpha \in \Lambda}$ tiene una mayorante $N_0 = \cup_\alpha N_\alpha$ que es un submódulo gracias a que son cadena. Usando el Lema de Zorn, existe un submódulo N de M maximal con respecto a la propiedad de que $m \notin N$. Tomemos el R-módulo N', necesariamente no nulo, tal que $M = N \oplus N'$. Si $0 \neq N'' \leq N'$, entonces $N \subset N \oplus N''$ y $m \in N \oplus N''$ ya que N es maximal, luego $M = N \oplus N''$ y como $N'' \subset N'$ tenemos $N' = N''$. Así N' es simple. □

El lema anterior nos va a permitir dar otras caracterizaciones de los módulos semisimples. A menudo, estas caracterizaciones son utilizadas como definiciones alternativas de la semisimplicidad.

TEOREMA 1. *Para un R-módulo $M =_R M$, las siguientes tres propiedades son equivalentes:*

(1) *M es semisimple.*
(2) *M es suma directa de una familia de submódulos simples.*
(3) *M es suma de una familia de submódulos simples.*

DEMOSTRACIÓN . Por convenio la suma y la suma directa de una familia de submódulos vacía serán ambas el módulo nulo. Esta convención

hará los siguientes argumentos válidos en todos los casos, incluido el caso $M = (0)$.

Veamos $(1) \Rightarrow (3)$. Sea M_1 la suma de todos los submódulos simples de M, escribimos $M = M_1 \oplus M_2$ donde M_2 es un R-submódulo conveniente. Si $M_2 \neq (0)$, aplicando los lemas anteriores tenemos que M_2 contiene un R-submódulo simple, pero este último debe estar en M_1 lo que nos lleva a una contradicción. Por tanto, $M_2 = (0)$, es decir, $M = M_1$.

Veamos $(3) \Rightarrow (1)$. Escribimos $M = \sum_{i \in I} M_i$, con los M_i submódulos simples de M. Consideremos $N \leq M$ un submódulo dado. Para demostrar que N es un sumando directo de ${}_RM$, consideremos una familia de conjuntos $J \subseteq I$ verificando las siguientes propiedades:

(1) $\sum_{j \in J} M_j$ es una suma directa.
(2) $N \cap \sum_{j \in J} M_j = (0)$.

Podemos aplicar el Lema de Zorn a la familia de tales subconjuntos J, con respecto a la inclusión usual. Esta familia es no vacía ya que contiene al conjunto vacío. Así, podemos seleccionar al conjunto J maximal. Para este conjunto J tenemos:

$$M' := N + \sum_{j \in J} M_j = N \oplus \bigoplus_{j \in J} M_j.$$

Veamos que $M = M'$, lo que quiere decir que N es un sumando directo de M. Para demostrar esto será suficiente demostrar que $M_i \subseteq M'$ para todo $i \in I$. Si algún $M_i \not\subseteq M'$, la simplicidad de M_i implica que $M' \cap M_i = (0)$. Tenemos entonces

$$M' + M_i = N \oplus \sum_{j \in J} M_j \oplus M_i,$$

en contradicción con la maximalidad e J.

$(3) \Rightarrow (2)$ se obtiene aplicando el argumento anterior a $N = (0)$.

$(2) \Rightarrow (3)$ es una tautología. □

Recordemos algunas definiciones.

DEFINICIÓN 7. *Una sucesión exacta es una sucesión*

$$\cdots \to A_n \xrightarrow{\alpha_n} A_{n+1} \xrightarrow{\alpha_{n+1}} A_{n+2} \to \cdots$$

de R-módulos A_i y homomorfismos de R-módulos α_i tales que

$$\textit{ker}(\alpha_n + 1) = \textit{Im}(\alpha_n).$$

Una sucesión exacta de la forma:

$$0 \to A \to B \to C \to 0,$$

se llamará sucesión exacta corta.

DEFINICIÓN 8. *Sea la sucesión exacta corta*

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0,$$

diremos que es escindida si existe $i'\colon M'' \to M$ *tal que* $pi' = 1_{M''}$ *o, equivalentemente, existe* $p'\colon M \to M'$ *tal que* $p'i = 1_{M'}$. *Esto es equivalente a que* $M = i(M') \oplus X$ *para cierto submódulo* X *de* M.

TEOREMA 2. *Dado un anillo* R *las siguientes afirmaciones son equivalentes:*

(1) *Todas las sucesiones exactas cortas de* R*-módulos por la izquierda son escindidas.*
(2) *Todos los* R*-módulos por la izquierda son semisimples.*
(3) *Todos los* R*-módulos por la izquierda finitamente generados son semisimples.*
(4) *Todos los* R*-módulos por la izquierda cíclicos son semisimples.*
(5) *El* R*-módulo regular por la izquierda* ${}_RR$ *es semisimple.*

Si cualquiera de estas condiciones se verifica se dice que R *es un anillo semisimple por la izquierda.*

DEMOSTRACIÓN . Podemos observar que (1) y (2) son equivalentes. Veamos $(1) \Rightarrow (2)$. Sea N un submódulo del R-módulo M. Consideremos la sucesión exacta corta

$$0 \to N \xrightarrow{i} M \xrightarrow{\pi} M/N \to 0.$$

Al ser escindida tenemos $M = N \oplus M/N$, luego M es semisimple. Para la otra implicación, si consideramos la sucesión exacta corta

$$0 \to M' \xrightarrow{i} M \xrightarrow{\pi} M'' \to 0,$$

con $i(M')$ un submódulo de M y M semisimple, entonces $M = i(M') \oplus X$, es decir, la sucesión exacta corta es escindida.

Como tenemos la sucesión trivial de implicaciones

$$(2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (5),$$

únicamente nos queda por demostrar $(5) \Rightarrow (2)$. Sea M cualquier R-módulo por la izquierda con R verificando (5). Consideremos el homomorfismo de R-módulos $\varphi\colon R \to R \cdot m$ donde m es un elemento fijo de M, tenemos $R/\text{Ker}\varphi \cong \text{Im}\varphi = R \cdot m$, luego aplicando el lema 2 tenemos que $R \cdot m$ es semisimple. Podemos escribir $M = \sum_{m \in M} R \cdot m$ y aplicando la caracterización (3) del teorema 1 tenemos que M es semisimple. □

Si M es un R-módulo por la izquierda, una cadena de longitud n es una sucesión de submódulos de M de la forma:

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M.$$

Si la cadena es máxima, es decir, no admite la insercción de más submódulos, se dice que es una serie de composición de longitud n de M. Esto es equivalente a decir que los cocientes M_j/M_{j-1} son R-módulos simples.

Sea R un anillo semisimple por la izquierda, si usamos la última caracterización del teorema anterior tenemos una descomposición $R = \oplus_{i \in I} \mathcal{U}_i$ en R-módulos simples por la izquierda $\mathcal{U}_i$ que son ideales por la izquierda

minimales de R. Como $1 \in R$ esta suma directa es en realidad una suma directa finita. Para esta descomposición finita podemos escribir una serie de composición de ${}_RR$ en la que los factores de la serie son $\{{}_R\mathcal{U}_i\}$. Así aplicando la afirmación (2) de la observación 1 tenemos que ${}_RR$ satisface las condiciones de cadena descendente y de cadena ascendente para R-módulos.

COROLARIO 1. *Un anillo R semisimple por la izquierda es noetheriano por la izquierda y artiniano por la izquierda.*

4. Teorema de Wedderburn-Artin

TEOREMA 3. *Sea R un anillo y $\mathcal{M}_n(R)$ el anillo de matrices $n \times n$ sobre R. Entonces todo ideal I de $\mathcal{M}_n(R)$ es de la forma $\mathcal{M}_n(\mathcal{U})$ para un ideal $\mathcal{U}$ de R determinado de forma única. En particular, si R es un anillo simple también lo es $\mathcal{M}_n(R)$.*

DEMOSTRACIÓN . Si $\mathcal{U}$ es un ideal de R, claramente $\mathcal{M}_n(\mathcal{U})$ es un ideal de $\mathcal{M}_n(R)$. Si $\mathcal{U}$ y $\mathcal{B}$ son dos ideales de R, es también claro que $\mathcal{U} = \mathcal{B}$ si y solo si $\mathcal{M}_n(\mathcal{U}) = \mathcal{M}_n(\mathcal{B})$. Consideremos I cualquier ideal de $\mathcal{M}_n(R)$ y sea $\mathcal{U}$ el conjunto:

$$\mathcal{U} := \{x \in R \colon \exists (m_{ij}) \in I, x = m_{11}\}$$

Fácilmente puede verse que $\mathcal{U}$ es un ideal de R y habremos completado la demostración si vemos que $I = \mathcal{M}_n(\mathcal{U})$. Para cualquier matriz $M = (m_{ij})$, tenemos

$$E_{ij} M E_{kl} = m_{jk} E_{il}, \tag{1}$$

donde E_{ij} denota la matriz que tiene un 1 en el lugar ij y cero en los demás. Supongamos que $M \in I$. Tomando $i = l = 1$, la igualdad anterior nos dice que $m_{jk} \in \mathcal{U}$ para cualesquiera j, k. Esto demuestra que $I \subseteq \mathcal{M}_n(\mathcal{U})$. Recíprocamente, tomemos $(a_{ij}) \in \mathcal{M}_n(\mathcal{U})$. Para demostrar que $(a_{ij}) \in I$ es suficiente demostrar que cada una de las matrices $a_{il}E_{il}$ pertenece a I para cada i, l, ya que (a_{ij}) es suma de todas estas matrices. Por definición de $\mathcal{U}$, podemos encontrar una matriz $M \in I$ que tiene al elemento a_{il} en el lugar 11, por ejemplo. Entonces, para $j = k = 1$ usando la igualdad (1) tenemos

$$a_{il}E_{il} = m_{11}E_{il} = E_{i1} M E_{1l} \in I.$$

Lo que nos demuestra el teorema. □

DEFINICIÓN 9. *Un anillo de división es un anillo unitario en el que todo elemento distinto de cero es inversible y por tanto una unidad.*

EJEMPLOS 3. Todo cuerpo es un anillo de división. Así, los anillos de división eran también llamados cuerpos no conmutativos en la antigüedad, ya que la conmutatividad es la única propiedad que los diferencia.

El anillo de los cuaterniones de Hamilton $\mathbb{H}$, formado por los elementos de la forma $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, con α_0, α_1, α_2 y $\alpha_3 \in \mathbb{R}$ con la suma natural y el producto según la siguiente tabla

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

es un anillo de división que extiende al cuerpo de los números complejos.

Si $\alpha = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ con α_0, α_1, α_2 y $\alpha_3 \in \mathbb{R}$, definimos y notamos el conjugado de α como $\overline{\alpha} = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$. Tenemos que $\alpha\overline{\alpha} = {\alpha_0}^2 + {\alpha_1}^2 + {\alpha_2}^2 + {\alpha_3}^2 \in \mathbb{R}$. Así si $\alpha \neq 0$, entonces $\alpha \in U(\mathbb{H})$ y $\alpha^{-1} = ({\alpha_0}^2 + {\alpha_1}^2 + {\alpha_2}^2 + {\alpha_3}^2))^{-1}\overline{\alpha}$. Por lo que efectivamente $\mathbb{H}$ es un anillo de división. Los cuaterniones forman un álgebra de división asociativa normada 4-dimensional sobre el cuerpo de los números reales y también un dominio. El centro de este anillo está formado por los elementos de la forma $\alpha_0 + 0i + 0j + 0k$ y por tanto es isomorfo al cuerpo de los números reales. El centro de un anillo de división es un cuerpo. Los anillos de división se pueden clasificar según su dimensión sobre su centro, cuando la dimensión es finita se dice que son una extensión finita de su centro.

Otro ejemplo de anillo de división es el anillo de división de los cuaterniones racionales, formado por los elementos de la forma $a + bi + cj + dk$ con $a, b, c, d \in \mathbb{Q}$ forman una $\mathbb{Q}$-álgebra de división 4-dimensional a la que llamamos R_1. En R_1 tenemos el subanillo R_2 formado por los elementos de la forma $a + bi + cj + dk$ con $a, b, c, d \in \mathbb{Z}$. R_2 no es un anillo de división. Su grupo de unidades es $U(R_2) = \{\pm 1, \pm i, \pm j, \pm k\}$, el grupo de los cuaterniones.

Recordemos que si R es un anillo y V es un R-módulo por la izquierda, con $E = \text{End}({}_R V)$ considerado como anillo de operadores por la derecha de V, entonces $V = {}_R V_E$ es un (R, E)-bimódulo. En el siguiente teorema estudiamos los anillos de matrices sobre un anillo de división.

LEMA 4 (**Lema de Schur**). *Sea R un anillo, y ${}_R V$ un R-módulo por la izquierda simple. Entonces End$({}_R V)$ es un anillo de división.*

DEMOSTRACIÓN . Consideremos $f \in \text{End}({}_R V)$. Entonces $\text{Im}(f) \neq 0$ y $\ker(f) \neq V$. Como $\text{Im}(f) \neq 0$ y $\ker(f) \neq V$ son ambos submódulos de V que es simple, entonces $\text{Im}(f) = V$ y $\ker(f) = 0$, es decir, f es inversible en $\text{End}({}_R V)$. □

LEMA 5. *Sea R un anillo entonces $R \cong$ End$({}_R R)$.*

DEMOSTRACIÓN . Consideremos la aplicación $\theta \colon R \to \text{End}({}_R R)$ definida como $\theta(a) = \varphi_a$, donde $\varphi_a \colon R \to R$ con $\varphi_a(x) := xa$. Evidentemente es un endomorfismo de anillos. Veamos que es monomorfismo, si $\varphi_a = 0$, entonces $xa = 0$ para todo $x \in R$, en particular para la unidad, luego

$a = 0$. Por otra parte, si $T \in \text{End}({}_R R)$ tenemos $T(x) = T(x1) = xT(1) = \varphi_{T(1)}(x)$, luego $T = \varphi_{T(1)}$ y θ es un isomorfismo. $\square$

LEMA 6. *Sea R un anillo y L un R-módulo simple. Se tiene entonces que End$(L^n) \cong \mathcal{M}_n(\Delta)$ con $\Delta =$ End$_R(L)$ un anillo de división.*

DEMOSTRACIÓN . Es claro que $\Delta = \text{End}_R(L)$ es un anillo de división por el Lema de Schur. Podemos construir el homomorfismo de anillos $\Phi\colon \text{End}(L^n) \to \mathcal{M}_n(\Delta)$ de forma que para $f \in \text{End}(L^n)$ tenemos $\Phi(f) = (f_{ij})_{i,j=1}^n$ con $f_{ij} = \pi_j f e_i$ donde $e_i\colon L \to L^n$ se define como $e_i(x) = (\overbrace{0, \ldots, 0}^{i-1)}, x, 0, \ldots, 0)$ y $\pi_j\colon L^n \to L$ definida $\pi_j(x_1, x_2, \ldots, x_n) = x_j$. Así, el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} L^n & \xrightarrow{f} & L^n \\ \downarrow{\scriptstyle e_i} & & \downarrow{\scriptstyle \pi_j} \\ L & \xrightarrow{f_{ij}} & L \end{array}$$

Se deja como ejercicio al lector comprobar que la aplicación Φ es un homomorfismo de anillos. Obsérvese que para todo $x = (x_1, x_2, \ldots, x_n) \in L^n$ tenemos:

$$f(x) = f(x_1, x_2, \ldots, x_n) =$$

$$f(x_1, 0, \ldots, 0) + f(0, x_2, \ldots, 0) + \cdots + f(0, \ldots, 0, x_n) =$$

$$fe_1(x) + fe_2(x) + \cdots fe_n(x) =$$

$$(\pi_1 f e_1(x), \pi_2 f e_1(x), \ldots, \pi_n f e_1(x)) + (\pi_1 f e_2(x), \pi_2 f e_2(x), \ldots, \pi_n f e_2(x)) +$$

$$\cdots + (\pi_1 f e_n(x), \pi_2 f e_n(x), \ldots, \pi_n f e_n(x)) =$$

$$(\sum_{i=1}^n \pi_1 f e_i(x), \sum_{i=1}^n \pi_2 f e_i(x), \ldots, \sum_{i=1}^n \pi_n f e_i(x)) =$$

$$(\sum_{i=1}^n f_{i1}(x), \sum_{i=1}^n f_{i2}(x), \ldots, \sum_{i=1}^n f_{in}(x)).$$

Evidentemente Φ es monomofismo ya que si $f_{ij} = 0$ para todo $i, j = 1, \ldots n$ entonces $f = 0$. Además, es sobreyectivo ya que para cada

$$(f_{ij})_{i,j=1}^n \in \mathcal{M}_n(\text{End}_R(L))$$

podemos definir $f \in \text{End}(L^n)$ de la forma

$$f(x_1, x_2, \ldots, x_n) := (\sum_{i=1}^n f_{i1}(x), \sum_{i=1}^n f_{i2}(x), \ldots, \sum_{i=1}^n f_{in}(x))$$

verificándose $\phi(f) = (f_{ij})_{i,j=1}^n$. $\square$

TEOREMA 4 (**Teorema de Wedderburn-Artin**). *Sea R un anillo semisimple por la izquierda. Entonces $R \cong \mathcal{M}_{n_1}(\Delta_1) \oplus \cdots \oplus \mathcal{M}_{n_r}(\Delta_r)$ para anillos de división $\Delta_1, \ldots, \Delta_r$ y enteros positivos $n_1, \ldots, n_r$. El número r está determinado de forma única, así como los pares $(n_1, \Delta_1), \ldots, (n_r, \Delta_r)$ (salvo permutación). Hay exactamente r R-módulos simples por la izquierda no isomorfos dos a dos.*

DEMOSTRACIÓN . Aplicando el apartado (2) del teorema 1 a R, tenemos ${}_RR \cong \oplus_{i\in I} L_i$. Veamos que $|I|$ es finito. Como R es unitario $1 = e_{i1} + e_{i2} + \ldots + e_{is}$, luego para todo $r \in R$, $r = re_{i1} + re_{i2} + \ldots + re_{is}$ con $e_{ij} \in L_{k_{ij}}$, por tanto $R = \oplus_{k=1}^{s} L_k$.

Así, $R \cong L_1^{n_1} \oplus L_2^{n_2} \oplus \cdots \oplus L_k^{n_k}$ con $L_i \ncong L_j$ si $i \neq j$ y $\text{End}({}_RR) \cong \text{End}(L_1^{n_1} \oplus L_2^{n_2} \oplus \cdots \oplus L_k^{n_k})$. Además si $f \in \text{End}(L_1^{n_1} \oplus L_2^{n_2} \oplus \cdots \oplus L_k^{n_k})$ y L_i, L_j son R-módulos simples con $i \neq j$ tenemos que $\pi_j f e_i$ es el homomorfismo de R-módulos que hace conmutativo el diagrama:

$$\begin{array}{ccc} L_1^{n_1} \oplus \cdots \oplus L_k^{n_k} & \xrightarrow{f} & L_1^{n_1} \oplus \cdots \oplus L_k^{n_k} \\ {\scriptstyle e_i}\uparrow & & \downarrow{\scriptstyle \pi_j} \\ L_i & \xrightarrow{\pi_j f e_i} & L_j \end{array}$$

Si $i \neq j$ se verifica $\pi_j f e_i = 0$ lo que quiere decir que $f(L_i^{n_i}) \subseteq L_i^{n_i}$ y podemos definir el homomorfismo de anillos

$$\theta\colon \text{End}(L_1^{n_1} \oplus L_2^{n_2} \oplus \cdots \oplus L_k^{n_k}) \to \text{End}(L_1^{n_1}) \oplus \text{End}(L_2^{n_2}) \oplus \cdots \oplus \text{End}(L_k^{n_k})$$

en la forma $\theta(f) = (f|L_1^{n_1}, f|L_2^{n_2}, \ldots, f|L_k^{n_k})$. Es claro que según su definición es inyectivo y sobreyectivo. □

Dado el anillo $R = \mathcal{M}_n(\Delta)$ la trasposición de matrices nos proporciona un isomorfismo $\theta\colon R \to R^{op}$. Así, las propiedades que se verifican por la izquierda también se verifican por la derecha. En general, como $\mathcal{M}_{n_1}(\Delta_1) \oplus \cdots \oplus \mathcal{M}_{n_r}(\Delta_r)$ es un anillo semisimple por la derecha es también semisimple por la izquierda, entonces tenemos la siguiente consecuencia.

COROLARIO 2. *Todo anillo R semisimple por la izquierda es semisimple por la derecha y viceversa.*

EJEMPLOS 4. A modo de aplicación, tratemos de encontrar todas las álgebras unitarias complejas simples A de dimensión finita. Como A es un anillo artiniano (por tener dimensión finita) y A tiene unidad, es fácil ver que es simple como anillo (cualquier ideal del anillo A es automáticamente un ideal del álgebra A). Por el teorema de Wedderburn-Artin $A \cong \mathcal{M}_n(\Delta)$ donde Δ es un anillo de división. Además como $\Delta \cong \text{End}_A(L)$ donde L es el A-módulo simple al que nos referimos en el teorema, entonces podemos dotar de estructura de $\mathbb{C}$ espacio vectorial a L y por tanto a $\Delta \cong \text{End}_A(L)$. Definimos la estructura de $\mathbb{C}$ espacio vectorial sobre L mediante:

$$\mathbb{C} \times L \to L$$

$$k \cdot x \to (k \cdot 1) \cdot x$$

Luego Δ es un álgebra de división compleja (necesariamente de dimensión finita ya que A lo es). Ahora bien, la única álgebra compleja de división de dimensión finita es el cuerpo de los complejos $\mathbb{C}$ (véase [**2**] Proposition 5.4.5, página 150). Por lo tanto, $A \cong \mathcal{M}_n(\mathbb{C})$. Además, el entero n está determinado de forma única por A: sabemos que n es la dimensión del (necesariamente único salvo isomorfismo) A-modulo simple. En el caso real la situación es ligeramente más complicada por el hecho de que según el teorema de Frobenius, hay tres álgebras reales de división de dimensión finita salvo isomorfismo. Estas álgebras son $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{H}$ (los cuaterniones de Hamilton). Aplicando el mismo razonamiento que antes, se llega a que las únicas álgebras reales simples de dimensión finita son salvo isomorfismo $\mathcal{M}_n(\mathbb{R})$, $\mathcal{M}_n(\mathbb{C})$ y $\mathcal{M}_n(\mathbb{H})$. Nuevamente, el número n, así como el álgebra de coordenadas ($\mathbb{R}$, $\mathbb{C}$ o $\mathbb{H}$) quedan determinadas de forma única por A.

Sobre otros cuerpos la situación puede ser más compleja. Por ejemplo, si A es una K-algebra simple de dimensión finita y $K = \mathbf{F}_{p^m}$ es el cuerpo finito de p^m elementos, entonces como antes $A \cong \mathcal{M}_n(\Delta)$ donde Δ es una $\mathbf{F}_{p^m}$-algebra de división y de dimensión finita. Esto implica que Δ es un álgebra de división finita. Por el Teorema pequeño de Wedderburn, toda álgebra de división finita es un cuerpo (véase [**1**], Theorem 1.13, página 265). Por lo tanto, Δ es un cuerpo (finito) extensión de $\mathbf{F}_{p^m}$. En consecuencia, $\Delta \cong \mathbf{F}_{p^{mk}}$ para algún $k \geq 1$ y tenemos $A \cong \mathcal{M}_n(\mathbf{F}_{p^{mk}})$. Luego en este caso disponemos de una cantidad infinito numerable de clases de isomorfía de álgebras de coordenadas.

La situación es mucho más compleja sobre el cuerpo de los racionales: además de todos los cuerpos extensión de $\mathbf{Q}$, existen álgebras de división sobre $\mathbf{Q}$ que no son cuerpos. Las posibilidades para Δ se amplian enormemente en este caso y por tanto el número de clases de isomorfía se dispara.

Bibliography

[1] P. M. Cohn. Algebra. Volumen III. John Wiley & Sons. 1991.
[2] P. M. Cohn. Basic Algebra. Groups, Rings and Fields. Springer. 2005.
[3] N. Jacobson. Basic algebra, I. Dover. 2009.
[4] N. Jacobson. Basic algebra, II. Dover. 2009.
[5] T. Y. Lam. A First Course in Noncommutative Rings. Springer. 2001.
[6] http://es.wikipedia.org/wiki/Wikipedia:Portada

Contents