Teorema de Artin–Wedderburn

Pablo Brianese

22 de septiembre de 2021

Teorema 1 (Lema de Zorn)**.** *Si A es un conjunto parcialmente ordenado no-vacío tal que toda cadena en A tiene una cota superior en A, entonces A contiene un elemento maximal.*

Proposición 1. *Sea R un anillo con identidad, y S el anillo formado por todas las matrices $n \times n$ sobre R. Dentro de S podemos encontrar las matrices E_{rs}, donde $r, s \in \{1, \ldots, n\}$, y E_{rs} tiene 1_R como entrada (r, s) y 0 en as demás posiciones. Para toda matriz $A = (a_{ij})$ en S*

$$E_{pr} A E_{sq} = a_{rs} E_{pq} \tag{1}$$

Demostración. Es un cálculo directo. □

Teorema 2. *Sea R un anillo con identidad y S el anillo formado por todas las matrices $n \times n$ sobre R. J es un ideal de S si y solo si J es el anillo formado por todas las matrices $n \times n$ sobre I para algún ideal I en R.*

Demostración. Sea J un ideal de S. Sea I el conjunto formado por todos los elementos de R que aparecen como entrada $(1, 1)$ de alguna matriz en J. Si $aE \in J$ donde $a \in R$ y $E = E_{11} \in S$, entonces $a \in I$. La afirmación recíproca también es verdadera. Notar que si $a \in I$, entonces existe $A = (a_{ij})$ en J con $a_{11} = a$. Al ser J un ideal (bilátero), tenemos $EAE \in J$. Pero $EAE = aE$. Entonces $aE \in J$. Hemos probado que $a \in I$ si y solo si $aE \in J$.

Afirmamos que I es un ideal. En efecto, $0 \in J$ porque J es un ideal. Luego $0 \in I$ por definición de I. Por otra parte, si $a, b \in I$, entonces $aE, bE \in J$. Pero J es un ideal. Entonces $(a+b)E = aE + bE \in J$. Luego $a + b \in I$. Para finalizar consideramos $r \in R$ y $a \in I$. Entonces $rE \in S$ y $aE \in J$. Pero J es un ideal. Entonces

$$(ra)E = (ra)E^2 = (rE)(aE) \in J \tag{2}$$

$$(ar)E = (ar)E^2 = (aE)(rE) \in J \tag{3}$$

Luego $ra, ar \in I$.

Afirmamos que $M_n(I) = J$. Sea $A = (a_{ij})$ una matriz en S. Comenzamos suponiendo $A \in J$. Consideremos $i, j \in \{1, \ldots, n\}$. Porque J es un ideal, $a_{rs}E = E_{1r}AE_{s1} \in J$. Luego $a_{rs} \in I$. Porque i, j eran arbitrarios, se deduce $A \in M_n(I)$. Recíprocamente, suponemos que $A = (a_{ij}) \in M_n(I)$. Consideramos $i, j \in \{1, \ldots, n\}$. Por hipótesis $a_{ij} \in I$. Luego $a_{ij}E \in J$. Porque J es un ideal, se deduce $E_{i1}(a_{ij}E)E_{1j} \in J$ mientras $E_{i1}(a_{ij}E)E_{1j} = a_{ij}E_{ij}$. Porque i, j eran arbitrarios, usando que J está cerrado bajo suma, se deduce $A = \sum_{ij} a_{ij}E_{ij} \in J$. □

Teorema 3. *Sea S el anillo formado por todas las matrices sobre un anillo de división D.*

1. *S no tiene ideales propios (es decir, 0 es un ideal maximal).*
2. *S tiene divisores de cero. Consecuentemente,*

a) *$S \simeq S/0$ no es un anillo de división y*

b) *0 es un ideal primo a pesar de no satisfacer la condición $ab \in I \to a \in I$ o $b \in I$ $(\forall a, b \in S)$*

Demostración. 1. Si J es un ideal de S, entonces J es el anillo formado por todas las matrices $n \times n$ sobre I para algún ideal I en D. Pero D es un anillo de división, no tiene ideales propios. Luego $I = 0$ o $I = D$, concluyendo que $J = 0$ o $J = S$. □

Demostración. 2 Para encontrar divisores de cero basta observar la fórmula $E_{r_1 s_1} E_{r_2 s_2} = \delta_{r_1 r_2} \delta_{s_1 s_2} E_{r_1 r_2}$. □

Definición 1. *Un módulo (izquierdo) A sobre un anillo R es* simple *(o* irreducible*) si $RA \neq 0$ y A no tiene submódulos propios. Un anillo R es* simple *si $R^2 \neq 0$ y R no tiene ideales (bilaterales) propios.*

Proposición 2. *Todo módulo simple A es cíclico; de hecho, $A = Ra$ para todo $a \in A$ nonulo.*

Demostración. Ambos Ra (con $a \in A$ nonulo) y $B = \{c \in A : Rc = 0\}$ son submódulos de A, de aquí que por simplicidad cada uno de ellos sea igual a 0 o A. También por simplicidad $RA \neq 0$, esto implica $B \neq A$ y $B = 0$. Luego $a \notin B$ y $Ra \neq 0$. En conclusión $Ra = A$. □

Definición 2. *Un módulo (izquierdo) A es* fiel *si su aniquilador (izquierdo) $\mathcal{A}(A)$ es 0. Un anillo R es* primitivo *(*izquierdo*) si existe un R-módulo simple y fiel.*

Los anillos primitivos derechos se definen análogamente. Sí existen anillos primitivos derechos que no son primitivos izquierdos. De aquí en más *primitivo* siempre significará *primitivo izquierdo*. Sin embargo, todos los resultados probados para anillos primitivos izquierdos son verdaderos, mutatis mutandis, para anillos primitivos derechos.

Definición 3. *Sea V un espacio vectorial izquierdo sobre un anillo de división D. Un subanillo R del anillo de endomorfismos $Hom_D(V, V)$ es un* anillo denso de endomorfismos *de V (o un* subanillo denso *de $Hom_D(V, V)$) si para todo entero positivo n, cada subconjunto linealmente independiente $\{u_1, \ldots, u_n\}$ de V y cada subconjunto arbitrario $\{v_1, \ldots, v_n\}$ de V, existe $\theta \in R$ tal que $\theta(u_i) = v_i$ $(\forall i \in \{1, \ldots, n\})$.*

Lema 1. *Sea A un módulo simple sobre un anillo R. Consideramos A como un espacio vectorial sobre el anillo de división $D = Hom_R(A, A)$. Si V es un subespacio finito-dimensional del D-espacio vectorial A y $a \in A \setminus V$, entonces existe $r \in R$ tal que $ra \neq 0$ y $rV = 0$.*

Demostración. La prueba es por inducción sobre $n = \dim_D V$. Comenzamos por el caso base. Si $n = 0$, entonces $V = 0$ y $a \neq 0$. Porque A es simple, $a \neq 0$ implica $Ra = A$. Consecuentemente existe $r \in R$ tal que $ra = a \neq 0$ y $rV = r0 = 0$.

En el paso inductivo, supongamos $\dim_D V = n > 0$ y que el teorema es verdadero para dimensiones menores a n. Sea $\{u_1, \ldots, u_{n-1}, u\}$ una D-base de V y sea W el subespacio $(n-1)$-dimensional generado por $\{u_1, \ldots, u_{n-1}\}$ (siendo $W = 0$ cuando $n = 1$). Entonces $V = W \oplus Du$ (suma directa de espacios vectoriales). Nuestra hipótesis inductiva tiene dos consecuencias importantes:

1. para todo $v \in A \setminus W$ existe $r \in R$ tal que $ru \neq 0$ y $rW = 0$;

2. para todo $v \in A$, si $rv = 0$ para todo $r \in R$ entonces $v \in W$.

La primera consecuencia implica que existe $r \in R$ tal que $ru \neq 0$ y $rW = 0$. Pero $rW = 0$ si y solo si $r \in \mathcal{A}(W)$, siendo $I = \mathcal{A}(W)$ un ideal izquierdo de R. Además $ru \in Iu \setminus 0$, siendo Iu un submódulo de A. Por simplicidad, este submódulo nonulo debe ser $Iu = A$.

Para terminar el argumento inductivo, debemos encontrar $r \in R$ tal que $ra \neq 0$ y $rV = 0$. Si no existe tal r, entonces podemos definir una aplicación $\theta : A \to A$ como sigue. Para $ru \in Iu = A$ definimos $\theta(ru) = ra \in A$. Afirmamos que θ está bien definida. Sean $r_1, r_2 \in I$ tales que $r_1 u = r_2 u$. Por hipótesis $(r_1 - r_2)a = 0$ o $(r_1 - r_2)V \neq 0$. Ahora bien, porque $r_1 - r_2 \in I = \mathcal{A}(W)$ tenemos $(r_1 - r_2)W = 0$; y porque $D = \mathrm{Hom}_D(A, A)$, para cada $d \in D$ tenemos $(r_1 - r_2)(d \cdot u) = (r_1 - r_2)d(u) = d((r_1 - r_2)u) = d(0) = 0$. Juntos, estos dos datos implican $(r_1 - r_2)V = (r_1 - r_2)(W \oplus Du) = 0$. Consecuentemente, por hipótesis $(r_1 - r_2)a = 0$. Por lo tanto $\theta(r_1 u) = r_1 a = r_2 a = \theta(r_2 u)$. Podemos mostrar que $\theta \in \mathrm{Hom}_D(A, A) = D$. Luego para cada $r \in I$, $0 = \theta(ru) - ra = r\theta(u) - ra = r(\theta(u) - a)$. De aquí que $\theta(u) - a \in W$, por la segunda consecuencia de la hipótesis inductiva. Consecuentemente $a = \theta u - (\theta u - a) \in Du + W = V$, lo cual contradice el hecho $a \notin V$. Por lo tanto, existe $r \in R$ tal que $ra \neq 0$ y $rV = 0$. □

Teorema 4 (de Densidad de Jacobson)**.** *Sea R un anillo primitivo y A un R–módulo simple y fiel. Considerar A como espacio vectorial sobre el anillo de división $Hom_R(A, A) = D$. Entonces R es isomorfo a un anillo denso de endomorfismos de D–espacio vectorial A.*

Demostración. Para cada $r \in R$ la aplicación $\alpha_r : A \to A$ dada por $\alpha_r(a) = ra$ es facilmente identificada como un D–endomorfismo de A: esto es, $\alpha_r \in \mathrm{Hom}_D(A, A)$. Además para todo par $r, s \in R$ se verifican $\alpha_{(r+s)} = \alpha_r + \alpha_s$ y $\alpha_{rs} = \alpha_r \alpha_s$. Consecuentemente la aplicación $\alpha : R \to \mathrm{Hom}_D(A, A)$ definida por $\alpha(r) = \alpha_r$ es un homomorfismo de anillos bien definido. Dado que A es un R–módulo fiel, $\alpha_r = 0$ si y solo si $r \in \mathcal{A}(A) = 0$. De aquí que α es un monomorfismo, y R es isomorfo al subanillo $\mathrm{Im}\,\alpha$ de $\mathrm{Hom}_D(A, A)$.

Para completar la prueba debemos mostrar que $\mathrm{Im}\,\alpha$ es un subanillo denso de $\mathrm{Hom}_D(A, A)$. Dado un subconjunto D–linealmente independiente $\{u_1, \ldots, u_n\}$ de A, y un subconjunto arbitrario $\{v_1, \ldots, v_n\}$ de A, debemos encontrar $\alpha_r \in \mathrm{Im}\,\alpha$ tal que $\alpha_r(u_i) = v_i$ $(\forall i \in \{1, \ldots, n\})$. Para cada i sea V_i el D–subespacio de A generado por $\{u_j : j \neq i\}$. Dado que $\{u_1, \ldots, u_n\}$ es linealmente independiente, $u_i \notin V_i$. Consecuentemente, por el lema **??** existe $r_i \in R$ tal que $r_i u_i \neq 0$

y $r_iV_i = 0$. Después aplicamos el lema **??** al subespacio nulo y a elemento nonulo r_iu_i: existe $s_i \in R$ tal que $s_ir_iu_i \neq 0$ y $s_i0 = 0$. Siendo $s_ir_iu_i \neq 0$, el R submódulo $R(r_iu_i)$ de A es nonulo, luego $R(r_iu_i) = A$ por simplicidad. Por esto existe $t_i \in R$ tal que $t_ir_iu_i = v_i$. Sea $r = t_1r_1 + t_2r_2 + \cdots + t_nr_n$. Recordar que $u_i \in V_j$ para $i \neq j$, luego $t_jr_ju_i \in t_j(r_jV_i) = t_j0 = 0$. Consecuentemente $\alpha_r(u_i) = (t_1r_1 + \cdots + t_nr_n)u_i = r_ir_iu_i = v_i$. Por lo tanto $\operatorname{Im}\alpha$ es un anillo denso de endomorfismos de D–espacio vectorial A. $\square$

Definición 4. *Decimos que un módulo A satisface la* condición de la cadena ascendente (ACC) sobre submódulos *(o decimos que es* noetheriano*) si para toda cadena $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$ de submódulos de A, existe un entero m tal que $B_i = B_m$ para todo $i \geq m$.*

Si un anillo R es pensado como módulo izquierdo (resp. derecho) sobre si mismo, entonces es facil ver que los submódulos de R son precisamente los ideales izquierdos (resp. derechos) de R. Consecuentemente, en este caso se acostumbra hablar de condiciones de cadena sobre ideales (izquierdos o derechos) en lugar de submódulos.

Definición 5. *Un anillo R es* noetheriano izquierdo *(resp.* derecho*) si R satisface la condición de la cadena ascendente sobre ss ideales izquierdos (resp. derechos). Se dice que R es* noetheriano *si R es noetheriano izquierdo y derecho a la vez.*

Un anillo R es artiniano izquierdo *(resp.* derecho*) si R satisface la condición de la cadena descendiente sobre sus ideales izquierdos (resp. derechos). Se dice que R es artiniano si R es artiniano izquierdo y derecho a la vez.*

Definición 6. *Un módulo A satisface la* condición maximal *[resp.* minimal*]* sobre submódulos *si todo conjunto novacío de submódulos de A contiene un elemento maximal [resp. minimal] (con respecto al orden dado por la inclusión de conjuntos).*

Teorema 5. *Un módulo satisface la condición de la cadena ascendente [resp. descencendente] sobre submódulos si y solo si satisface la condición maximal [resp. minimal] sobre submódulos.*

Demostración. Supongamos que el módulo A satisface la condición minimal sobre submódulos y que $A_1 \supseteq A_2 \supseteq \cdots$ es una cadena de submódulos. Entonces el conjunto $\{A_i \mid i \geq 1\}$ tiene un elemento minimal, digamos A_n. Consecuentemente, para $i \geq n$ tenemos $A_n \supseteq A_i$ por hipótesis y $A_n \subseteq A_i$ por minimalidad, luego $A_i = A_n$ para todo $i \geq n$. Por lo tanto, A satisface la condición descendiente de la cadena.

REcíprocamente supongamos que A satisface la condición de la cadena descendente, y S es un conjunto novacío de submódulos de A. Entonces existe $B_0 \in S$. Si S no tiene elemento minimal, entonces para todo submódulo B en S existe al menos un submódulo B' en S tal que $B \supset B'$. Para cada B en S, elegimos uno de estos B' (Axioma de Elección). Esta elección define una función $f : S \to S$ mediante $B \mapsto B'$. Por el Teorema de la Recursión, existe una función $\phi : \mathbb{N} \to S$ tal que $\phi(0) = B_0$ y $\phi(n+1) = f(\phi(n))$ $(\forall n \in \mathbb{N})$. Por tanto si $B_n = \phi(n)$ $(\forall n \in \mathbb{N})$, entonces $B_0 \supset B_1 \supset \cdots$ es una cadena descendiente que viola la condición descendiente de la cadena. Por lo tanto, S debe tener un elemento minimal. Concluímos que A satisface la condición minimal.

La prueba para las condiciones de la cadena ascendente y maximal es análoga. $\square$

Teorema 6 (de Artin–Wedderburn). *Las siguientes condiciones sobre un anillo artiniano izquierdo R son equivalentes.*

1. *R es simple;*
2. *R es primitivo;*
3. *R es isomorfo al anillo de endomorfismos de un espacio vectorial nonulo sobre un anillo de división D;*
4. *para algún entero positivo n, R es isomorfo al anillo formado por las matrices $n \times n$ sobre un anillo de división.*

Demostración. $1 \Rightarrow 2$. Primero observamos que $I = \{r \in R \mid Rr = 0\}$ es un ideal de R, con la propiedad $IR = 0$. Pero R es simple: no tiene ideales propios, por lo cual $I = R$ o $I = 0$; y $RR \neq 0$, por lo cual $I = 0$.

Consideremos el conjunto $\mathcal{S}$ formado por todos los ideales izquierdos nonulos de R. Dado que R es artiniano izquierdo, satisface la condición de la cadena descendiente sobre ideales izquierdos. En particular, para toda sucesión $\{S_i\}_{i\in\mathbb{N}}$ en $\mathcal{S}$ con $S_0 \supseteq S_1 \supseteq S_2 \supseteq \cdots$, existe un $m \in \mathbb{N}$ tal que $S_m = S_i$ para todo $i \geq m$. El Lema de Zorn permite deducir de esto la existencia de un elemento minimal $J \in \mathcal{S}$, tal que $J \supseteq J' \to J = J'$ para todo $J' \in \mathcal{S}$. Esta minimalidad hace que J no tenga R–submódulos propios (un R–submódulo de J es un ideal izquierdo de R contenido en J).

Afirmamos que el aniquilador izquierdo $\mathcal{A}(J)$ de J en R es cero. De otro modo $\mathcal{A}(J) = R$ por simplicidad y $Ru = 0$ para cada $u \in J$ nonulo. Consecuentemente, cada uno de estos u nonulos pertenece a $I = 0$, lo cual es una contradicción. Por lo tanto $\mathcal{A}(J) = 0$ y $RJ \neq 0$. En conclusión, J es un R–módulo simple y fiel, y R es primitivo.

$2 \Rightarrow 3$ Por el Teorema de Densidad de Jacobson **??**, R es isomorfo a un anillo denso T compuesto por endomorfismos de un espacio vectorial V sobre un anillo de división D. Porque R es artiniano izquierdo, $R \simeq T = \mathrm{Hom}_D(V, V)$ por el teorema **??**.

$3 \Leftrightarrow 4$ Teorema **??**

$4 \Leftrightarrow 1$ Ejercicio **??** $\square$