

Teorema de Artin–Wedderburn

Pablo Brianese

18 de octubre 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.*

Capítulo 1

Matrices

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 $r, s \in \{1, \dots, n\}$, y E_{rs} tiene 1_R como entrada (r, s) y 0 en las demás posiciones. Para toda matriz $A = (a_{ij})$ en S

$$E_{pr}AE_{sq} = a_{rs}E_{pq} \quad (1.1)$$

Demostración. Es un cálculo directo. \square

Teorema 2. Si D es un anillo de división y $R = \text{Mat}_n D$, entonces el ideal $RE_{j_0 j_0}$ está formado por todas las matrices $A \in R$ tales que $\text{Col}_j A = 0$ ($\forall j \neq j_0$). Es decir

$$RE_{j_0 j_0} = \sum_{i=1}^n DE_{ij_0} \quad (1.2)$$

Demostración. Fijemos $j_0 \in \{1, \dots, n\}$, y escribamos $E = E_{j_0 j_0}$, $I = RE$.

Afirmamos que $I' = \{A \in R : \text{Col}_j A = 0 \ (\forall j \neq j_0)\}$ es igual a I . Lo demostraremos usando que, por la proposición 1, para toda matriz $a = (a_{ij})_{ij}$ en R

$$aE_{j_0 j_0} = I_n aE_{j_0 j_0} = \sum_{i=1}^n E_{ii} aE_{j_0 j_0} = \sum_{j=1}^n a_{ij_0} E_{ij_0} \quad (1.3)$$

Si $A \in I$, entonces existe $a \in R$ con $A = aE$. Luego $A = \sum_{i=1}^n a_{ij_0} E_{ij_0}$ pertenece a I' . Recíprocamente, si $A \in I'$, entonces $A = (A_{ij})_{ij}$ puede escribirse como $A = \sum_{i=1}^n \sum_{j=1}^n A_{ij} E_{ij} = \sum_{i=1}^n A_{ij_0} E_{ij_0} = AE_{j_0 j_0}$. \square

Argumentos análogos demuestran que

Teorema 3. Si D es un anillo de división y $R = \text{Mat}_n D$, entonces el ideal $E_{i_0 i_0} R$ está formado por todas las matrices $A \in R$ tales que $\text{Fila}_i A = 0$ ($\forall i \neq i_0$). Es decir

$$E_{i_0 i_0} R = \sum_{j=1}^n E_{i_0 j} D \quad (1.4)$$

Demostración. Fijemos $i_0 \in \{1, \dots, n\}$, y escribamos $E = E_{i_0 i_0}$, $I = ER$.

Afirmamos que $I' = \{A \in R : \text{Fila}_i A = 0 (\forall i \neq i_0)\}$ es igual a I . Lo demostraremos usando que, por la proposición 1, para toda matriz $a = (a_{ij})_{ij}$ en R

$$E_{i_0 i_0} a = E_{i_0 i_0} a I_n = \sum_{j=1}^n E_{i_0 i_0} a E_{jj} = \sum_{j=1}^n a_{i_0 j} E_{i_0 j} \quad (1.5)$$

Si $A \in I$ entonces existe $a \in R$ con $A = Ea$. Luego $A = \sum_{j=1}^n a_{i_0 j} E_{i_0 j}$ pertenece a I' . Recíprocamente, si $A \in I'$ entonces $A = (A_{ij})_{ij}$ puede escribirse como $A = \sum_{i=1}^n \sum_{j=1}^n A_{ij} E_{ij} = \sum_{j=1}^n A_{i_0 j} E_{i_0 j} = E_{i_0 i_0} A$. \square

Teorema 4. Sean D un anillo de división y $R = \text{Mat}_n D$. Entonces son simples los R -submódulos izquierdos de R

$$RE_{jj} \quad (j \in \{1, \dots, n\}) \quad (1.6)$$

Demostración. Fijemos $j_0 \in \{1, \dots, n\}$, y escribamos $E = E_{j_0 j_0}$, $I = RE$.

Afirmamos que I es minimal. Supongamos que J es un submódulo no nulo de I . Entonces existe $a \in J \setminus 0$. Porque $a \in I$ se sigue $a = \sum_{i=1}^n a_{i j_0} E_{i j_0}$. $a \neq 0$ implica que $a_{i_0 j_0} \neq 0$ para un $i_0 \in \{1, \dots, n\}$. Porque D es un anillo de división, existe una matriz elemental de transformación M , que actúa sobre a multiplicando (por izquierda) su fila i_0 por el elemento $a_{i_0 j_0}^{-1} \in D$. Entonces $Ma = 1_D E_{i_0 j_0} + \sum_{i \neq i_0} a_{i j_0} E_{i j_0}$. Luego, existen matrices elementales de transformación A_i ($i \in \{1, \dots, n\} \setminus i_0$), que actúan sobre a sumando a la fila i -ésima el producto (por izquierda) de $-a_{i j_0}$ con la fila i_0 -ésima. Entonces $A_1 \cdots A_n Ma = 1_D E_{i_0 j_0}$ (donde definimos $A_{i_0} = I_n$, la matriz identidad, para mejorar la notación). Finalmente, para cada $i \in \{1, \dots, n\}$, existe una matriz elemental de transformación P_i que actúa sobre a permutando las filas i e i_0 . De ese modo $P_i A_1 \cdots A_n Ma = 1_D E_{i j_0}$. Por lo tanto $1_D E_{i j_0} \in J$ para todo $i \in \{1, \dots, n\}$. Eso implica que $I = \sum_{i=1}^n D E_{i j_0} \subseteq J$. En conclusión $J = I$. \square

Teorema 5. Sean D un anillo de división y $R = \text{Mat}_n D$. Entonces son simples los R -submódulos derechos de R

$$E_{ii} R \quad (i \in \{1, \dots, n\}) \quad (1.7)$$

Demostración. Fijemos $i_0 \in \{1, \dots, n\}$, y escribamos $E = E_{i_0 i_0}$, $I = ER$.

Afirmamos que I es minimal. Supongamos que J es un submódulo no nulo de I . Entonces existe $a \in J \setminus 0$. Porque $a \in I$ se sigue $a = \sum_{j=1}^n a_{i_0 j} E_{i_0 j}$.

$a \neq 0$ implica que $a_{i_0 j_0} \neq 0$ para un $j_0 \in \{1, \dots, n\}$. Porque D es un anillo de división, existe una matriz elemental de transformación M , que actúa sobre a multiplicando (por derecha) su columna j_0 por el elemento $a_{i_0 j_0}^{-1} \in D$. Entonces $aM = E_{i_0 j_0} 1_D + \sum_{j \neq j_0} a_{i_0 j} E_{i_0 j}$. Luego, existen matrices elementales de transformación A_j ($j \in \{1, \dots, n\} \setminus j_0$), que actúan sobre a sumando a la columna j -ésima el producto (por derecha) de $-a_{i_0 j}$ con la columna j_0 -ésima. Entonces $aMA_1 \cdots A_n = E_{i_0 j_0} 1_D$ (donde definimos $A_{j_0} = I_n$, la matriz identidad, para mejorar la notación). Finalmente, para cada $j \in \{1, \dots, n\}$, existe una matriz elemental de transformación P_j que actúa sobre a permutando las columnas j y j_0 . De ese modo $aMA_1 \cdots A_n P_j = E_{i_0 j} 1_D$. Por lo tanto $E_{i_0 j} 1_D \in J$ para todo $i \in \{1, \dots, n\}$. Eso implica que $I = \sum_{j=1}^n E_{i_0 j} D \subseteq J$. En conclusión $J = I$. \square

Teorema 6. Sea $M_0 = 0$ y para $i \in \{1, \dots, n\}$ sea $M_i = R(E_{11} + \cdots + E_{ii})$. Entonces $R = M_n \supseteq M_{n-1} \supseteq \cdots \supseteq M_1 \supseteq M_0 = 0$ es una serie de composición de R -módulos izquierdos, con factores $M_i/M_{i-1} \simeq RE_{ii}$.

Demostración. Notar que $M_i \subseteq RE_{11} + \cdots + RE_{ii}$. Usando el teorema 2, se sigue $\text{Col}_j A = 0$ ($\forall j \in \{i+1, \dots, n\}$) para toda $A \in M_i$.

Notar que si $A \in M_i$ con $A = r(E_{11} + \cdots + E_{ii})$ para un $r \in R$, entonces $AE_{ii} = rE_{ii}$. En efecto

$$AE_{ii} = r(E_{11} + \cdots + E_{ii})E_{ii} \quad (1.8)$$

$$= r(E_{11}E_{ii} + \cdots + E_{i-1,i-1}E_{ii} + E_{ii}^2) \quad (1.9)$$

$$= r(0 + \cdots + 0 + E_{ii}) \quad (1.10)$$

$$= rE_{ii} \quad (1.11)$$

Por este motivo $A + M_{i-1} = AE_{ii} + M_{i-1}$. Calculamos

$$A + M_{i-1} = r(E_{11} + \cdots + E_{ii}) + M_{i-1} \quad (1.12)$$

$$= r(E_{11} + \cdots + E_{i-1,i-1}) + rE_{ii} + M_{i-1} \quad (1.13)$$

$$= rE_{ii} + M_{i-1} \quad (1.14)$$

$$= AE_{ii} + M_{i-1} \quad (1.15)$$

Supongamos que $A + M_{i-1} = B + M_{i-1}$. Entonces $AE_{ii} + M_{i-1} = BE_{ii} + M_{i-1}$. Escribamos $C = (A - B)E_{ii}$. Por un lado $C \in M_{i-1}$ y por el otro $C \in RE_{ii}$. El primer dato implica $\text{Col}_j C = 0$ para $j \in \{i, \dots, n\}$. El segundo dato implica $\text{Col}_j C = 0$ para $j \in \{1, \dots, n\} \setminus i$. Luego $C = 0$. Es decir $AE_{ii} = BE_{ii}$.

Esto nos permite definir una función $\phi : M_i/M_{i-1} \rightarrow RE_{ii}$ dada por $A + M_{i-1} \mapsto AE_{ii}$. Así definida, es un homomorfismo de R -módulos. Es además un monomorfismo. Si $\phi(A + M_{i-1}) = 0$ entonces $AE_{ii} = 0$ y $\text{Col}_i A = 0$. Además, $A \in M_i$ implica $\text{Col}_j A = 0$ ($\forall j > i$). Luego $\text{Col}_j A = 0$ ($\forall j \in \{i, \dots, n\}$), y $A \in M_{i-1}$. Entonces $A + M_{i-1} = 0 + M_{i-1}$. También es un epimorfismo. Dado $AE_{ii} \in RE_{ii}$, tenemos $AE_{ii} \in M_i$. Calculamos $\phi(AE_{ii} + M_{i-1}) = (AE_{ii})E_{ii} = AE_{ii}^2 = AE_{ii}$. Por lo tanto $AE_{ii} \in \text{Im } \phi$. Concluimos que $\phi : M_i/M_{i-1} \rightarrow RE_{ii}$ es un isomorfismo. \square

Teorema 7. Sea $M_0 = 0$ y para $i \in \{1, \dots, n\}$ sea $M_i = (E_{11} + \dots + E_{ii})R$. Entonces $R = M_n \supseteq M_{n-1} \supseteq \dots \supseteq M_1 \supseteq M_0 = 0$ es una serie de composición de R -módulos derechos, con factores $M_i/M_{i-1} \simeq E_{ii}R$.

Demostración. Notar que $M_{i_0} \subseteq E_{11}R + \dots + E_{i_0 i_0}R$. Usando el teorema 3, se sigue $\text{Fila}_i A = 0$ ($\forall i \in \{i_0 + 1, \dots, n\}$) para toda $A \in M_{i_0}$.

Notar que se $A \in M_{i_0}$ con $A = (E_{11} + \dots + E_{i_0 i_0})r$ para un $r \in R$, entonces $E_{i_0 i_0} A = E_{i_0 i_0} r$. En efecto

$$E_{i_0 i_0} A = E_{i_0 i_0} (E_{11} + \dots + E_{i_0 i_0})r \quad (1.16)$$

$$= (E_{i_0 i_0} E_{11} + \dots + E_{i_0 i_0} E_{i_0-1, i_0-1} + E_{i_0 i_0}^2)r \quad (1.17)$$

$$= (0 + \dots + 0 + E_{i_0 i_0})r \quad (1.18)$$

$$= E_{i_0 i_0} r \quad (1.19)$$

Por este motivo $A + M_{i_0-1} = AE_{i_0 i_0} + M_{i_0-1}$. Calculamos

$$A + M_{i_0-1} = (E_{11} + \dots + E_{i_0 i_0})r + M_{i_0-1} \quad (1.20)$$

$$= (E_{11} + \dots + E_{i_0-1, i_0-1})r + E_{i_0 i_0} r + M_{i_0-1} \quad (1.21)$$

$$= E_{i_0 i_0} r + M_{i_0-1} \quad (1.22)$$

$$= E_{i_0 i_0} A + M_{i_0-1} \quad (1.23)$$

Supongamos que $A + M_{i_0-1} = B + M_{i_0-1}$. Entonces $E_{i_0 i_0} A + M_{i_0-1} = E_{i_0 i_0} B + M_{i_0-1}$. Escribamos $C = E_{i_0 i_0} (A - B)$. Por un lado $C \in M_{i_0-1}$ y por el otro $C \in E_{i_0 i_0} R$. El primer dato implica $\text{Fila}_i C = 0$ para $i \in \{i_0, \dots, n\}$. El segundo dato implica $\text{Fila}_i C = 0$ para $i \in \{1, \dots, n\} \setminus i_0$. Luego $C = 0$. Es decir $E_{i_0 i_0} A = E_{i_0 i_0} B$.

Esto nos permite definir una función $\phi : M_{i_0}/M_{i_0-1} \rightarrow E_{i_0 i_0} R$ dada por $A + M_{i_0-1} \mapsto E_{i_0 i_0} A$. Así definida, es un homomorfismo de R -módulos. Es además un monomorfismo. Si $\phi(A + M_{i_0-1}) = 0$ entonces $E_{i_0 i_0} A = 0$ y $\text{Fila}_{i_0} A = 0$. Además $A \in M_{i_0}$ implica $\text{Fila}_i A = 0$ ($\forall i \in \{i_0, \dots, n\}$), y $A \in M_{i_0-1}$. Entonces $A + M_{i_0-1} = 0 + M_{i_0-1}$. También es un epimorfismo. Dado $E_{i_0 i_0} A \in E_{i_0 i_0} R$, tenemos $E_{i_0 i_0} A \in M_i$. Calculamos $\phi(E_{i_0 i_0} A + M_{i_0-1}) = E_{i_0 i_0} (E_{i_0 i_0} A) = E_{i_0 i_0}^2 A = E_{i_0 i_0} A$. Por lo tanto $E_{i_0 i_0} A \in \text{Im } \phi$. Concluimos que $\phi : M_{i_0}/M_{i_0-1} \rightarrow E_{i_0 i_0} R$ es un isomorfismo. \square

1.1. módulos

Teorema 8. Si R es un anillo y B es un submódulo de un R -módulo A , entonces existe una correspondencia uno-a-uno entre el conjunto de los submódulos de A que contienen a B y el conjunto de todos los submódulos de A/B , dada por $C \mapsto C/B$. Por tanto todo submódulo de A/B es de la forma C/B , donde C es un submódulo de A que contiene a B .

1.2. cadenas de ideales

Definición 1. Decimos que un módulo A satisface la condición de la cadena ascendente sobre submódulos (o decimos que es noetheriano) si para toda cadena $A_1 \subseteq A_2 \subseteq A_3 \subseteq \dots$ de submódulos de A , existe un entero m tal que $B_i = B_m$ para todo $i \geq m$.

Decimos que un módulo B satisface la condición de la cadena descendente sobre submódulos (o que es artiniano) si para toda cadena $B_1 \supseteq B_2 \supseteq B_3 \supseteq \dots$ de submódulos de B , 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 sí mismo, entonces es fácil 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 2. Un anillo R es noetheriano izquierdo (resp. derecho) si R satisface la condición de la cadena ascendente sobre sus 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 descendente sobre sus ideales izquierdos (resp. derechos). Se dice que R es artiniano si R es artiniano izquierdo y derecho a la vez.

Definición 3. Un módulo A satisface la condición maximal [resp. minimal] sobre submódulos si todo conjunto no vacío de submódulos de A contiene un elemento maximal [resp. minimal] (con respecto al orden dado por la inclusión de conjuntos).

Teorema 9. Un módulo satisface la condición de la cadena ascendente [resp. descendente] 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 $A_1 \supseteq A_2 \supseteq \dots$ 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 descendente de la cadena.

Recíprocamente supongamos que A satisface la condición de la cadena descendente, y S es un conjunto no vacío 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 $f : S \rightarrow S$ mediante $B \mapsto B'$. Por el Teorema de la Recursión, existe una función $\phi : \mathbb{N} \rightarrow S$ 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 $B_0 \supset B_1 \supset \dots$ es una cadena descendente

que viola la condición descendente de la cadena. Por lo tanto, S debe tener un elemento minimal. Concluimos que A satisface la condición minimal.

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

1.3. series subnormales

Definición 4. Una serie subnormal de un grupo G es una cadena de subgrupos $G = G_0 \geq G_1 \geq \cdots \geq G_n = \langle e \rangle$ tal que G_{i+1} es normal en G_i para $1 \leq i \leq n$. Los factores de la serie son los grupos cociente G_i/G_{i+1} . La longitud de la serie es el número de inclusiones estrictas (alternativamente, el número de factores con orden mayor a 1). Una serie subnormal es una serie de composición si cada factor G_i/G_{i+1} es simple.

Una serie normal para un módulo A es una cadena de submódulos: $A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_n$. Los factores de la serie son los módulos cociente A_i/A_{i+1} ($0 \leq i < n$). La longitud de la serie es el número de inclusiones propias (igual al número de factores no triviales). Un refinamiento propio es un refinamiento con longitud mayor a la serie original. Dos series normales son equivalentes si existe una correspondencia uno-a-uno entre los factores no triviales tal que factores correspondientes sean isomorfos. De tal modo, series equivalentes tienen igual longitud. Una serie de composición para A es una serie normal $A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_n = 0$ tal que cada factor A_k/A_{k+1} ($0 \leq k < n$) es un módulo no nulo sin submódulos propios. Si R es unitario, decimos que un módulo unitario sin submódulos propios es simple.

La Teoría de Series Normales y Subnormales para grupos puede trasladarse al caso de los módulos. Como consecuencia de esta tenemos el siguiente teorema.

Teorema 10. Cualesquiera dos series normales de un módulo A tienen refinamientos que son equivalentes. Cualesquiera dos series de composición de A son equivalentes.

Teorema 11. Un módulo no nulo A tiene una serie de composición si y solo si A satisface tanto la condición de la cadena descendente como la ascendente.

Demostración. Supongamos que A tiene una serie de composición S de longitud n . Si alguna de las condiciones de la cadena falla, podemos encontrar submódulos $A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n \supset A_{n+1}$ que forman una serie normal T de longitud $n + 1$. Por el teorema 10, S y T tienen refinamientos equivalentes. Esto es una contradicción porque series equivalentes tienen igual longitud. Todo refinamiento de la serie de composición S tiene longitud n al igual que S , pero todo refinamiento de T tiene longitud al menos $n + 1$. Por lo tanto A satisface ambas condiciones de la cadena.

Recíprocamente, suponemos que B es un submódulo no nulo de A , definimos $S(B)$ como el conjunto formado por todos los submódulos C de B con $C \neq B$. De tal modo que si B no tiene submódulos propios, entonces $S(B) = \{0\}$. También definimos $S(0) = \{0\}$. Para cada B , el conjunto $S(B)$ tiene un elemento

maximal B' (por el Teorema 9). Sea S el conjunto de todos los submódulos de A . Definimos una aplicación $f : S \rightarrow S$ mediante $f(B) = B'$ (usando el Axioma de Elección). Por el Teorema de la Recursión, existe una función $\phi : \mathbb{N} \rightarrow S$ tal que $\phi(0) = a$ y $\phi(n+1) = f(\phi(n))$. Si $A_i = \phi(i)$, entonces $A \supseteq A_1 \supseteq A_2 \supseteq \cdots$ es una cadena descendiente por construcción. Luego para un n , $A_i = A_n$ ($\forall i \geq n$). Dado que $A_{n+1} = f(A_n)$, la definición de f muestra que $A_{n+1} = A_n$ solo si $A_n = 0 = A_{n+1}$. Sea m el menor entero tal que $A_m = 0$. Entonces $m \leq n$ y $A_k \neq 0$ ($\forall k < m$). Más aún, para cada $k < m$, A_{k+1} es un submódulo maximal de A_k tal que $A_k \supseteq A_{k+1}$. Consecuentemente, cada A_k/A_{k+1} es no nulo y no tiene submódulos propios por el teorema 8. Por lo tanto $A \supseteq A_1 \supseteq \cdots \supseteq A_m = 0$ es una serie de composición para A . \square

1.4. Conclusión

Corolario 1. *Si D es un anillo de división, entonces el anillo $\text{Mat}_n D$ formado por todas las matrices $n \times n$ sobre D es a la vez artiniiano y noetheriano.*

Demostración. Es una consecuencia del teorema 11. En efecto, usando tal resultado, el teorema 6 implica que $\text{Mat}_n D$ es artiniiano y noetheriano izquierdo; y el teorema 7 implica que $\text{Mat}_n D$ es artiniiano y noetheriano derecho. \square

Teorema 12. Sea R un anillo con identidad. Las siguientes condiciones sobre un R -módulo unitario F son equivalentes:

1. F tiene una base novacia;
2. F es la suma directa (interna) de una familia de R -módulos cíclicos, cada uno de los cuales es isomorfo (como R -módulo izquierdo) a R ;
3. F es isomorfo (como R -módulo) a una suma directa de copias del R -módulo izquierdo R ;
4. existe un conjunto novacio X y una función $\iota : X \rightarrow F$ con la siguiente propiedad: dado un R -módulo unitario A y una función $f : X \rightarrow A$, existe un único homomorfismo de R -módulos $\bar{f} : F \rightarrow A$ tal que $\bar{f}\iota = f$. En otras palabras, F es un objeto libre en la categoría de R -módulos unitarios.

Un módulo unitario F sobre un anillo R con identidad, que satisface las condiciones del teorema, recibe el nombre de R -módulo libre sobre el conjunto X . La cuarta propiedad hace de F un objeto libre en la categoría formada por los

Teorema 13. Todo espacio vectorial V sobre un anillo de división D tiene una base y es por tanto un D -módulo libre. Con mayor generalidad, cada subconjunto linealmente independiente de V está contenido en una base de V .

Teorema 14. Sean A y B ambos R -módulos.

1. el conjunto $\text{Hom}_R(A, B)$ formado por los homomorfismos de R -módulos $A \rightarrow B$ es un grupo abeliano con $f + g : A \rightarrow B$ dada por $a \mapsto f(a) + g(a)$. El elemento identidad es la aplicación nula.
2. $\text{Hom}_R(A, A)$ es un anillo con identidad, donde la multiplicación es la composición de funciones. $\text{Hom}_R(A, A)$ es el anillo de endomorfismos de A .
3. A es un $\text{Hom}_R(A, A)$ -módulo izquierdo con $fa = f(a)$ ($\forall a \in A$) ($\forall f \in \text{Hom}_R(A, A)$).

Teorema 15. Sea R un anillo con identidad y E un R -módulo izquierdo libre con una base finita de n elementos. Entonces existe un isomorfismo de anillos

$$\text{Hom}_R(E, E) \simeq \text{Mat}_n(R^{\text{op}}) \quad (1.24)$$

En particular, este isomorfismo existe para todo espacio vectorial E sobre un anillo de división R con dimensión n , en cuyo caso R^{op} también es un anillo de división.

Observación 1. Cuando R es conmutativo $R = R^{\text{op}}$. La fórmula del teorema resulta $\text{Hom}_R(E, E) \simeq \text{Mat}_n R$.

Teorema 16. 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

$$(ra)E = (ra)E^2 = (rE)(aE) \in J \quad (1.25)$$

$$(ar)E = (ar)E^2 = (aE)(rE) \in J \quad (1.26)$$

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 $i, j \in \{1, \dots, n\}$. 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 $i, j \in \{1, \dots, n\}$. 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 $A = \sum_{ij} a_{ij}E_{ij} \in J$. \square

Teorema 17. 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 $ab \in I \rightarrow a \in I$ 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 $J = S$. \square

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

Definición 5. 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 $Ra = A$. \square

Teorema 18. *Sea B un subconjunto de un módulo izquierdo sobre un anillo R . Entonces $\mathcal{A}(B) = \{r \in R \mid rb = 0 (\forall b \in B)\}$ es un ideal izquierdo de R . Si B es un submódulo de A , entonces $\mathcal{A}(B)$ es un ideal.*

$\mathcal{A}(B)$ es el *aniquilador (izquierdo)* de B . El aniquilador derecho de un módulo derecho se define análogamente.

Definición 6. *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 7. *Sea V un espacio vectorial izquierdo sobre un anillo de división D . Un subanillo R del anillo de endomorfismos $\text{Hom}_D(V, V)$ es un anillo denso de endomorfismos de V (o un subanillo denso de $\text{Hom}_D(V, V)$) si para todo entero positivo n , cada subconjunto linealmente independiente $\{u_1, \dots, u_n\}$ de V y cada subconjunto arbitrario $\{v_1, \dots, v_n\}$ de V , existe $\theta \in R$ tal que $\theta(u_i) = v_i$ ($\forall i \in \{1, \dots, n\}$).*

Lema 1. *Sea A un módulo simple sobre un anillo R . Consideramos A como un espacio vectorial sobre el anillo de división $D = \text{Hom}_R(A, A)$. 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 $\{u_1, \dots, u_{n-1}, u\}$ una D -base de V y sea W el subespacio $(n-1)$ -dimensional generado por $\{u_1, \dots, u_{n-1}\}$ (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 no nulo 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 $\theta : A \rightarrow A$ 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 $r_1u = r_2u$. 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 $D = \text{Hom}_D(A, A)$, 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 $\theta(r_1u) = r_1a = r_2a = \theta(r_2u)$. Podemos mostrar que $\theta \in \text{Hom}_D(A, A) = D$. 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 $rV = 0$. \square

Teorema 19 (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 $\text{Hom}_R(A, A) = D$. Entonces R es isomorfo a un anillo denso de endomorfismos de D -espacio vectorial A .*

Demostración. Para cada $r \in R$ la aplicación $\alpha_r : A \rightarrow A$ dada por $\alpha_r(a) = ra$ es fácilmente identificada como un D -endomorfismo de A : esto es, $\alpha_r \in \text{Hom}_D(A, A)$. 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 $\alpha : R \rightarrow \text{Hom}_D(A, A)$ 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 $\text{Im } \alpha$ de $\text{Hom}_D(A, A)$.

Para completar la prueba debemos mostrar que $\text{Im } \alpha$ es un subanillo denso de $\text{Hom}_D(A, A)$. Dado un subconjunto D -linealmente independiente $\{u_1, \dots, u_n\}$ de A , y un subconjunto arbitrario $\{v_1, \dots, v_n\}$ de A , debemos encontrar $\alpha_r \in \text{Im } \alpha$ tal que $\alpha_r(u_i) = v_i$ ($\forall i \in \{1, \dots, n\}$). Para cada i sea V_i el D -subespacio de A generado por $\{u_j : j \neq i\}$. Dado que $\{u_1, \dots, u_n\}$ es linealmente independiente, $u_i \notin V_i$. Consecuentemente, por el lema 1 existe $r_i \in R$ tal que $r_i u_i \neq 0$ y $r_i V_i = 0$. Después aplicamos el lema 1 al subespacio nulo y a elemento no nulo $r_i u_i$: existe $s_i \in R$ tal que $s_i r_i u_i \neq 0$ y $s_i 0 = 0$. Siendo $s_i r_i u_i \neq 0$, el R submódulo $R(r_i u_i)$ de A es no nulo, luego $R(r_i u_i) = A$ por simplicidad. Por esto existe $t_i \in R$ tal que $t_i r_i u_i = v_i$. Sea $r = t_1 r_1 + t_2 r_2 + \dots + t_n r_n$. Recordar que $u_i \in V_j$ para $i \neq j$, luego $t_j r_j u_i \in t_j (r_j V_i) = t_j 0 = 0$. Consecuentemente $\alpha_r(u_i) = (t_1 r_1 + \dots + t_n r_n)u_i = r_i r_i u_i = v_i$. Por lo tanto $\text{Im } \alpha$ es un anillo denso de endomorfismos de D -espacio vectorial A . \square

Teorema 20. *Sea R un anillo denso de endomorfismos de un espacio vectorial V sobre un anillo de división D . Entonces R es artiniiano izquierdo [resp. derecho] si y solo si $\dim_D V$ es finita, en cuyo caso $R = \text{Hom}_D(V, V)$.*

Demostración. Si R es artiniiano izquierdo, y $\dim_D V$ es infinita, entonces existe un subconjunto de V linealmente independiente e infinito (numerable) $\{u_1, u_2, \dots\}$. Por el Ejercicio 14 V es un $\text{Hom}_D(V, V)$ -módulo izquierdo y por tanto un R -módulo izquierdo (recordar que $R \subseteq \text{Hom}_D(V, V)$). Para cada n sea I_n el aniquilador izquierdo en R del conjunto $\{u_1, \dots, u_n\}$. Por el Teorema 18 $I_1 \supseteq I_2 \supseteq \dots$ es una cadena descendente de ideales izquierdos de R . Sea w un elemento no nulo de V , no importa cual de ellos sea (podría ser u_1 , por ejemplo). Dado que $\{u_1, \dots, u_{n+1}\}$ es linealmente independiente (para cada n) y R es denso, existe $\theta \in R$ tal que $\theta u_i = 0$ ($\forall i \in \{1, \dots, n\}$) y $\theta u_{n+1} = w \neq 0$. Consecuentemente $\theta \in I_n$ pero $\theta \notin I_{n+1}$. Por lo tanto $I \supset I_2 \supset \dots$ es una cadena estrictamente descendente, su existencia lleva a una contradicción. Luego $\dim_D V$ es finita.

Recíprocamente, si $\dim_D V$ es finita, entonces V tiene una base finita $\{v_1, \dots, v_m\}$. Si f es un elemento de $\text{Hom}_D(V, V)$, entonces f está completamente determinado por su acción sobre v_1, \dots, v_m por los teoremas 12 y 13. Dado que R es denso, existe $\theta \in R$ tal que $\theta v_i = f v_i$ $\forall i \in \{1, \dots, m\}$. Luego $f = \theta \in R$. Por lo tanto $\text{Hom}_D(V, V) = R$. Pero $\text{Hom}_D(V, V)$ es artiniiano por el Teorema 15 y el corolario 1. \square

Teorema 21 (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 $\text{Hom}_R(A, A) = D$. Entonces R es isomorfo a un anillo denso de endomorfismos del D -espacio vectorial A .*

Demostración. Para cada $r \in R$ la aplicación $\alpha_r : A \rightarrow A$ dada por $\alpha_r(a) = ra$ es fácilmente identificada como un D -endomorfismo de A : esto es, $\alpha_r \in \text{Hom}_D(A, A)$. Además $\alpha_{(r+s)} = \alpha_r + \alpha_s$ y $\alpha_{rs} = \alpha_r \alpha_s$ para todo $r, s \in R$. Consecuentemente la aplicación $\alpha : R \rightarrow \text{Hom}_D(A, A)$ 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 $\text{Im } \alpha$ de $\text{Hom}_D(A, A)$.

Para completar la prueba debemos mostrar que $\text{Im } \alpha$ es un subanillo denso de $\text{Hom}_D(A, A)$. Sea $U = \{u_1, \dots, u_n\}$ un subconjunto D -linealmente independiente de A ; y sea $\{v_1, \dots, v_n\}$ un subconjunto arbitrario de A . Debemos encontrar $\alpha_r \in \text{Im } \alpha$ tal que $\alpha_r(u_i) = v_i$ ($\forall i \in \{1, \dots, n\}$). Para cada i sea V_i el D -subespacio de A generado por $\{u_j : j \neq i\}$. Dado que U es linealmente independiente, $u_i \notin V_i$. Consecuentemente, por el lema 1 existe $r_i \in R$ tal que $r_i u_i \neq 0$ y $r_i V_i = 0$. Después aplicamos el lema 1.11 al subespacio nulo y al elemento no nulo $r_i u_i$: existe $s_i \in R$ tal que $s_i r_i u_i \neq 0$ y $s_i 0 = 0$. Siendo $s_i r_i u_i \neq 0$, el R -submódulo $R(r_i u_i)$ de A es no nulo, luego $R(r_i u_i) = A$ por simplicidad. Por esto existe $t_i \in R$ tal que $t_i r_i u_i = v_i$. Sea $r = t_1 r_1 + t_2 r_2 + \dots + t_n r_n \in R$. Recordar que $u_i \in V_j$ para $i \neq j$, luego $t_j r_j u_i \in t_j (r_j V_i) = t_j 0 = 0$. Consecuentemente $\alpha_r(u_i) = (t_1 r_1 + \dots + t_n r_n) u_i = t_i r_i u_i = v_i$. Por lo tanto $\text{Im } \alpha$ es un anillo denso de endomorfismos del D -espacio vectorial A . \square

Teorema 22 (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 no nulo 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 no nulos 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 $S_0 \supseteq S_1 \supseteq S_2 \supseteq \dots$, 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 $J \supseteq J' \rightarrow J = J'$ 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 $u \in J$ no nulo. Consecuentemente, cada uno de estos u no nulos 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 21, 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, $R \simeq T = \text{Hom}_D(V, V)$ por el Teorema 20.

$3 \Leftrightarrow 4$ Teorema 15

$4 \Leftrightarrow 1$ Teorema 17

□