Teorema de Artin–Wedderburn

Pablo Brianese

28 de octubre de 2021

Teorema 1 (Lema de Zorn)**.** *Si A es un conjunto parcialmente ordenado novacío tal que toda cadena en A tiene una cota superior en A, entonces A contiene un elemento maximal.*

Capítulo 1

Matrices

En el presente capítulo estudiaremos matrices. Matrices cuadradas con entradas en un anillo de división. Nuestro objetivo final será probar que el anillo formado por estas es artiniano y noetheriano. Para conocer las cadenas de ideales del anillo usaremos las llamadas series de composición. Por un lado, trabajaremos con series de composición concretas. Por el otro, estudiaremos la relación abstracta que existe entre las series de composición y las cadenas de ideales.

Sea D un anillo de división, escribimos $\mathrm{Mat}_n D$ para denotar al anillo formado por las matrices $n \times n$ con entradas en D. Nuestra principal herramienta a la hora de calcular dentro del anillo $\mathrm{Mat}_n D$ seran las matrices elementales E_{rs}, donde $r, s \in \{1, \ldots, n\}$, y E_{rs} tiene 1_D como entrada (r, s) y 0_D en las demás posiciones. Parte de su valor se explica en la siguiente proposición.

Proposición 1. *Sea D un anillo de división y $R = \mathrm{Mat}_n D$. Para toda matriz $A = (A_{ij})_{ij}$ en R*

$$E_{pr} A E_{sq} = A_{rs} E_{pq} \tag{1.1}$$

Demostración. Es un cálculo directo. □

Usamos esta proposición para entender algunos ideales cíclicos de $\mathrm{Mat}_n D$, con propiedades especiales.

Teorema 2. *Si D es un anillo de división y $R = \mathrm{Mat}_n D$, entonces*

$$R E_{j_0 j_0} = \sum_{i=1}^{n} D E_{i j_0} \qquad (\forall j_0 \in \{1, \ldots, n\}) \tag{1.2}$$

Demostración. Fijamos $j_0 \in \{1, \ldots, n\}$, y escribimos $I = R E_{j_0 j_0}$.

Afirmamos que $I' = \sum_{i=1}^{n} D E_{i j_0}$ es igual a I. Lo demostraremos usando que, por la proposición 1, toda matriz $a = (a_{ij})_{ij}$ en R verifica

$$a E_{j_0 j_0} = I_n a E_{j_0 j_0} = \sum_{i=1}^{n} E_{ii} a E_{j_0 j_0} = \sum_{i=1}^{n} a_{i j_0} E_{i j_0} \tag{1.3}$$

Si $A \in I$, entonces existe $a \in R$ con $A = aE_{j_0j_0}$. Luego $A = aE_{j_0j_0} = \sum_{i=1}^n a_{ij_0}E_{ij_0}$, también pertenece a I'. Recíprocamente, si $A = (A_{ij})_{ij}$ pertenece I', entonces $A = \sum_{i=1}^n A_{ij_0}E_{ij_0} = AE_{j_0j_0}$, y también es un elemento de I. □

Argumentos análogos demuestran que

Teorema 3. *Si D es un anillo de división y $R = \mathrm{Mat}_n D$, entonces*

$$E_{i_0i_0}R = \sum_{j=1}^n E_{i_0j}D \qquad (\forall i_0 \in \{1,\dots,n\}) \tag{1.4}$$

Demostración. Fijemos $i_0 \in \{1,\dots,n\}$, y escribamos $I = E_{i_0i_0}R$.

Afirmamos que $I' = \sum_{j=1}^n E_{i_0j}D$ es igual a I. Lo demostraremos usando que, por la proposición 1, toda matriz $a = (a_{ij})_{ij}$ en R verifica

$$E_{i_0i_0}a = E_{i_0i_0}aI_n = \sum_{j=1}^n E_{i_0i_0}aE_{jj} = \sum_{j=1}^n a_{i_0j}E_{i_0j} \tag{1.5}$$

Si $A \in I$ entonces existe $a \in R$ con $A = E_{i_0i_0}a$. Luego $A = E_{i_0i_0}a = \sum_{j=1}^n a_{i_0j}E_{i_0j}$, también pertenece a I'. Recíprocamente, si $A = (A_{ij})_{ij}$ pertenece a I', entonces $A = \sum_{j=1}^n A_{i_0j}E_{i_0j} = E_{i_0i_0}A$, y también es un elemento de I. □

Ahora probaremos propiedades importantes de estos módulos cíclicos.

Teorema 4. *Si D es un anillo de división y $R = \mathrm{Mat}_n D$, entonces los R-submódulos izquierdos de R*

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

no tienen submódulos propios.

Demostración. Fijemos $j_0 \in \{1,\dots,n\}$, y escribamos $E = E_{j_0j_0}$, $I = RE$.

Supongamos que J es un submódulo nonulo de I. Probaremos $J = I$. Entonces existe $a \in J \setminus 0$. Porque $a \in I$ se sigue del teorema 2 que $a = \sum_{i=1}^n a_{ij_0}E_{ij_0}$. Notemos que $a \neq 0$ implica $a_{i_0j_0} \neq 0$ 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 $a_{i_0j_0}^{-1} \in D$. Entonces $Ma = E_{i_0j_0} + \sum_{i\neq i_0} a_{ij_0}E_{ij_0}$. 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 $-a_{ij_0}$ con la fila i_0-ésima. Entonces $A_1 \cdots A_n Ma = E_{i_0j_0}$ (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 $P_iA_1 \cdots A_n Ma = E_{ij_0}$. Por lo tanto $E_{ij_0} \in J$ para todo $i \in \{1,\dots,n\}$. Eso implica que $I = \sum_{i=1}^n DE_{ij_0} \subseteq J$ (recordar el teorema 2). En conclusión $J = I$. □

Argumentos similares demuestran que

Teorema 5. *Si D es un anillo de división y $R = \mathrm{Mat}_n D$, entonces los R-submódulos derechos de R*

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

no tienen submódulos propios.

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

Supongamos que J es un submódulo nonulo de I. Entonces existe $a \in J \setminus 0$. Porque $a \in I$ se sigue del teorema 3 que $a = \sum_{j=1}^{n} a_{i_0 j} E_{i_0 j}$. Notemos que $a \neq 0$ implica $a_{i_0 j_0} \neq 0$ 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 $j \in \{1, \dots, n\}$. Eso implica que $I = \sum_{j=1}^{n} E_{i_0 j} D \subseteq J$ (recordar el teorema 3). En conclusión $J = I$. □

Estos módulos cíclicos que hemos estudiado aparecen como cocientes en cadenas formadas por otros módulos cíclicos, que pasamos a investigar.

Teorema 6. *Sea D un anillo de división y $R = \mathrm{Mat}_n D$. Definimos $M_0 = 0$ y para $j \in \{1, \dots, n\}$ definimos $M_j = R(E_{11} + \cdots + E_{jj})$. Entonces la secuencia $R = M_n \supseteq M_{n-1} \supseteq \cdots \supseteq M_1 \supseteq M_0 = 0$, formada por R-submódulos izquierdos de R, satisface $M_j / M_{j-1} \simeq RE_{jj}$.*

Demostración. Primera observación. Sea $j \in \{1, \dots, n\}$ arbitrario. Notar que $M_j \subseteq RE_{11} + \cdots + RE_{jj}$. Usando el teorema 2, se sigue que, para toda $A \in M_j$, son nulas las columnas $j+1, \dots, n$ de A.

Fijemos $j_0 \in \{1, \dots, n\}$, y simplifiquemos la notación escribiendo $E = E_{j_0 j_0}$, $M = M_{j_0}$, $N = M_{j_0 - 1}$.

Segunda observación. Notar que si $A \in M$ con $A = r(E_{11} + \cdots + E_{j_0 j_0})$ para un $r \in R$, entonces $AE = rE$. En efecto

$$\begin{aligned} AE &= r(E_{11} + \cdots + E_{j_0 j_0})E && (1.8)\\ &= r(E_{11}E + \cdots + E_{j_0 - 1, j_0 - 1}E + E^2) && (1.9)\\ &= r(0 + \cdots + 0 + E) && (1.10)\\ &= rE && (1.11) \end{aligned}$$

Por este motivo $A + N = AE + N$. Para verlo, calculamos

$$A + N = r(E_{11} + \cdots + E_{j_0 j_0}) + N \tag{1.12}$$
$$= r(E_{11} + \cdots + E_{j_0-1,j_0-1}) + rE + N \tag{1.13}$$
$$= rE + N \tag{1.14}$$
$$= AE + N \tag{1.15}$$

Tercera observación. Supongamos que $A + N = B + N$ para unas matrices $A, B \in M$ arbitrarias. Entonces $AE + N = BE + N$ por nuestra segunda observación. Escribamos $C = (A - B)E$. Por un lado, la ecuación $AE + N = BE + N$ implica $C \in N$, y por el otro $C \in RE$. El primer dato, mediante nuestra primera observación, implica $\mathrm{Col}_j C = 0$ para $j \in \{j_0, \ldots, n\}$. El segundo dato, mediante el teorema 2, implica $\mathrm{Col}_j C = 0$ para $j \in \{1, \ldots, n\} \setminus j_0$. Luego $C = 0$. Es decir $AE = BE$.

Esta última observación nos permite definir una función $\phi : M/N \to RE$ dada por $A+N \mapsto AE$. Resulta ser un homomorfismo de R-módulos. Es además un monomorfismo. Si $\phi(A + N) = 0$ entonces $AE = 0$ y $\mathrm{Col}_{j_0} A = 0$. Además, $A \in M$ implica $\mathrm{Col}_j A = 0$ $(\forall j \in \{j_0 + 1, \ldots, n\})$. Luego $\mathrm{Col}_j A = 0$ $(\forall j \in \{j_0, \ldots, n\})$, y $A \in N$. Entonces $A + N = 0 + N$, el elemento nulo del cociente. También es un epimorfismo. Dado $aE \in RE$, tenemos $aE \in M$ por el teorema 2. Calculamos $\phi(aE + N) = (aE)E = aE^2 = aE$. Por lo tanto $aE \in \mathrm{Im}\,\phi$. Concluímos que $\phi : M/N \to RE$ es un isomorfismo. □

Argumentos análogos demuestran el siguiente teorema

Teorema 7. *Sea D un anillo de división y $R = \mathrm{Mat}_n D$. Definimos $M_0 = 0$ y para $i \in \{1, \ldots, n\}$ definimos $M_i = (E_{11} + \cdots + E_{ii})R$. Entonces la secuencia $R = M_n \supseteq M_{n-1} \supseteq \cdots \supseteq M_1 \supseteq M_0 = 0$, formada por R-módulos derechos, satisface $M_i/M_{i-1} \simeq E_{ii}R$.*

Demostración. Primera observación. Sea $i \in \{1, \ldots, n\}$ arbitrario. Notar que $M_i \subseteq E_{11}R + \cdots + E_{ii}R$. Usando el teorema 3, se sigue que, para toda $A \in M_i$, son nulas las filas $i + 1, \ldots, n$ de A.

Fijemos $i_0 \in \{1, \ldots, n\}$, y simplifiquemos la notación escribiendo $E = E_{i_0 i_0}$, $M = M_{i_0}$, $N = M_{i_0-1}$.

Segunda observación. Notar que si $A \in M$ con $A = (E_{11} + \cdots + E_{i_0 i_0})r$ para un $r \in R$, entonces $EA = Er$. En efecto

$$EA = E(E_{11} + \cdots + E_{i_0 i_0})r \tag{1.16}$$
$$= (EE_{11} + \cdots + EE_{i_0-1,i_0-1} + E^2)r \tag{1.17}$$
$$= (0 + \cdots + 0 + E)r \tag{1.18}$$
$$= Er \tag{1.19}$$

Por este motivo $A + N = AE + N$. Para verlo, calculamos

$$A + N = (E_{11} + \cdots + E_{i_0 i_0})r + N \tag{1.20}$$
$$= (E_{11} + \cdots + E_{i_0-1,i_0-1})r + Er + N \tag{1.21}$$
$$= Er + N \tag{1.22}$$
$$= EA + N \tag{1.23}$$

Tercera observación. Supongamos que $A+N = B+M_{i_0-1}$ para unas matrices $A, B \in M$ arbitrarias. Entonces $EA + N = EB + N$, por nuestra segunda observación. Escribamos $C = E(A - B)$. Por un lado, la ecuación $EA + N = EB+N$ implica $C \in N$, y por el otro $C \in ER$. El primer dato, mediante nuestra primera observación, implica $\text{Fila}_i C = 0$ para $i \in \{i_0, \ldots, n\}$. El segundo dato, mediante el teorema 3, implica $\text{Fila}_i C = 0$ para $i \in \{1, \ldots, n\} \setminus i_0$. Luego $C = 0$. Es decir $EA = EB$.

Esta última observación nos permite definir una función $\phi : M/N \to ER$ dada por $A+N \mapsto EA$. Resulta ser un homomorfismo de R-módulos. Es además un monomorfismo. Si $\phi(A + N) = 0$ entonces $EA = 0$ y $\text{Fila}_{i_0} A = 0$. Además, $A \in M$ implica $\text{Fila}_i A = 0$ $(\forall i \in \{i_0 + 1, \ldots, n\})$. Luego $\text{Fila}_i A = 0$ $(\forall i \in \{i_0, \ldots, n\})$, y $A \in N$. Entonces $A + N = 0 + N$, el elemento nulo del cociente. También es un epimorfismo. Dado $Ea \in ER$, tenemos $Ea \in M_i$ 3. Calculamos $\phi(Ea + N) = E(Ea) = E^2 a = Ea$. Por lo tanto $Ea \in \operatorname{Im} \phi$. Concluímos que $\phi : M/N \to ER$ es un isomorfismo. □

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 $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$ 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 $B_1 \supseteq B_2 \supseteq B_3 \supseteq \cdots$ 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 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 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 novacío 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. 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 descendente de la cadena.

Recíprocamente, supongamos que A satisface la condición de la cadena descendente, y S es un conjunto novacío de submódulos de A. Para empezar, 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 descendente que viola la condición descendente de la cadena. Por lo tanto, S debe tener un elemento minimal. Concluímos que A satisface la condición minimal sobre submódulos. □

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

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

Recíprocamente, supongamos que A satisface la condición de la cadena ascendente, y S es un conjunto novacío de submódulos de A. Entonces existe $B_0 \in S$. Si S no tiene elemento maximal, entonces para todo submódulo $B \in S$ existe al menos un submódulo $B' \in S$ tal que $B \subset B'$. Para cada $B \in S$, 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 ascendente que viola la condición ascendente de la cadena. Por lo tanto, S debe tener un elemento maximal. Concluimos que A satisface la condición maximal de la cadena. □

1.3. series subnormales

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 notriviales). 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 notriviales 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 nonulo 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. Esta teoría incluye análogos al lema de Zassenhaus, y a los teoremas de Schreier y Jordan-Hölder. Como consecuencia tenemos el siguiente teorema.

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

Teorema 11. *Un módulo nonulo 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. Sin embargo 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 A satisface ambas condiciones de la cadena. Dado B, un submódulo nonulo 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, la condición de la cadena ascendente nos asegura que 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 $f : S \to S$ mediante $f(B) = B'$ (usando el Axioma de Elección). Por el Teorema de la Recursión, existe una función $\phi : \mathbb{N} \to S$ 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 descendente por construcción. Luego, por la condición de la cadena descendente, 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 por construcción un submódulo maximal de A_k. Consecuentemente, cada factor A_k/A_{k+1} es nonulo 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. □

1.4. Conclusión

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

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

Capítulo 2

Teorema de Artin-Wedderburn

2.1. Ideales del anillo de matrices

Teorema 12. *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

$$(ra)E = (ra)E^2 = (rE)(aE) \in J \tag{2.1}$$

$$(ar)E = (ar)E^2 = (aE)(rE) \in J \tag{2.2}$$

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 13. *El anillo* $\mathrm{Mat}_n D$ *formado por todas las matrices* $n \times n$ *con entradas en un anillo de división* D *no tiene ideales propios.*

Demostración. Si J es un ideal de S, entonces, por el teorema 12, 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 $J = S$. □

2.2. Anillos simples y primitivos

Definición 4. *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.*

Observación 1. *El teorema 13 dice que* $\mathrm{Mat}_n D$ *es simple si* D *es un anillo de división.*

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 $Ra = A$. □

Teorema 14. *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 5. *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.

Teorema 15. *Un anillo artiniano izquierdo es primitivo si es simple.*

Demostración. 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 bilaterales propios, por lo cual $I = R$ o $I = 0$. Siendo $RR \neq 0$, es imposible que $R = 0$, por lo cual $I = 0$.

Dado que R es artiniano izquierdo, el conjunto formado por todos sus ideales izquierdos nonulos contiene un ideal izquierdo minimal J (una consecuencia del teorema 9). Esta minimalidad hace que J, como R-módulo, 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. Primero que nada, $\mathcal{A}(J)$ es un ideal bilátero de R porque J es un ideal izquierdo. Luego, la simplicidad de R implica que $\mathcal{A}(J) = R$ o $\mathcal{A}(J) = 0$. Supongamos, para llegar a un absurdo, que $\mathcal{A}(J) = 0$. Entonces $\mathcal{A}(J) = R$ y $RJ = 0$. Pero existen elementos $u \in J$ distintos de 0. Cada uno de estos u nonulos pertenece al ideal I que estudiamos al inicio de la prueba. Siendo $I = 0$, llegamos a una contradicción. Por lo tanto $\mathcal{A}(J) = 0$ y $RJ \neq 0$. En conclusión, J es un R–módulo simple y fiel. El anillo R es primitivo. □

2.3. El Teorema de Densidad de Jacobson

Definición 6. *Sea V un espacio vectorial izquierdo sobre un anillo de división D. Un subanillo R del anillo de endomorfismos* $\mathrm{Hom}_D(V,V)$ *es un* anillo denso de endomorfismos *de V (o un* subanillo denso *de* $\mathrm{Hom}_D(V,V)$*) 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 $\theta(u_i) = v_i$ $(\forall i \in \{1, \ldots, n\})$.*

Teorema 16. *Sea R un anillo denso de endomorfismos de un espacio vectorial V sobre un anillo de división D. Entonces R es artiniano izquierdo [resp. derecho] si y solo si* $\dim_D V$ *es finita, en cuyo caso* $R = \mathrm{Hom}_D(V,V)$.

Demostración. Si R es artiniano izquierdo y $\dim_D V$ es infinita, entonces existe un subconjunto de V linealmente independiente e infinito (numerable) $\{u_1, u_2, \ldots\}$. Por el Ejercicio 21, V es un $\mathrm{Hom}_D(V,V)$-módulo izquierdo y por tanto un R-módulo izquierdo (recordar que $R \subseteq \mathrm{Hom}_D(V,V)$). Para cada n sea I_n el aniquilador izquierdo en R del conjunto $\{u_1, \ldots, u_n\}$. Por el Teorema 14 $I_1 \supseteq I_2 \supseteq \cdots$ es una cadena descendente de ideales izquierdos de R. Sea w un elemento nonulo de V, no importa cual de ellos sea (podría ser u_1, por ejemplo). Dado que $\{u_1, \ldots, u_{n+1}\}$ es linealmente independiente (para cada n) y R es denso, existe $\theta \in R$ tal que $\theta u_i = 0$ $(\forall i \in \{1, \ldots, n\})$ y $\theta u_{n+1} = w \neq 0$. Consecuentemente $\theta \in I_n$ pero $\theta \notin I_{n+1}$. Por lo tanto $I_1 \supset I_2 \supset \cdots$ es una cadena estrictamente descendente de R-módulos izquierdos. La existencia de esta cadena lleva a una contradicción. Luego $\dim_D V$ es finita.

Recíprocamente, supongamos que $\dim_D V$ es finita. En este caso V tiene una base finita $\{v_1, \ldots, v_m\}$. Si f es un elemento de $\mathrm{Hom}_D(V,V)$, entonces f está completamente determinado por su acción sobre $v_1, \ldots, v_m$ por los teoremas 19

y 20. Dado que R es denso, existe $\theta \in R$ tal que $\theta v_i = f v_i \ \forall i \in \{1, \ldots, m\}$. Luego $f = \theta \in R$. Por lo tanto $\mathrm{Hom}_D(V, V) = R$. Pero $\mathrm{Hom}_D(V, V)$ es artiniano por el Teorema 22 y el corolario 1. □

Lema 1. *Sea A un módulo simple sobre un anillo R. Consideramos A como un espacio vectorial sobre el anillo de división $D = \mathrm{Hom}_R(A, A)$. 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 17 (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 $\mathrm{Hom}_R(A, A) = D$. Entonces R es isomorfo a un anillo denso de endomorfismos del D-espacio vectorial A.*

Demostración. Para cada $r \in R$ la aplicación $\alpha_r : A \to A$ 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 $\alpha_{(r+s)} = \alpha_r + \alpha_s$ y $\alpha_{rs} = \alpha_r\alpha_s$ para todo par $r, s \in R$. 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 $\mathrm{Hom}_D(A,A)$. Sea $U = \{u_1, \ldots, u_n\}$ un subconjunto D-linealmente independiente de A; y sea $\{v_1, \ldots, v_n\}$ un subconjunto arbitrario 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 es linealmente independiente, $u_i \notin V_i$. Consecuentemente, por el lema 1 existe $r_i \in R$ tal que $r_iu_i \neq 0$ y $r_iV_i = 0$. Después aplicamos el lema 1 al subespacio nulo y al 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 en 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 $r = t_1r_1 + t_2r_2 + \cdots + t_nr_n \in R$. 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 $\alpha_r(u_i) = (t_1r_1 + \cdots + t_nr_n)u_i = t_ir_iu_i = v_i$. Por lo tanto $\mathrm{Im}\,\alpha$ es un anillo denso de endomorfismos del D-espacio vectorial A. □

Corolario 2. *Un anillo R artiniano izquierdo y primitivo es isomorfo al anillo de endomorfismos de un espacio vectorial nonulo sobre un anillo de división D.*

Demostración. Por el Teorema de Densidad de Jacobson 17, 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, el Teorema 16 implica $R \simeq T = \mathrm{Hom}_D(V,V)$. □

Teorema 18 (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. $1 \Rightarrow 2$. Teorema 15
$2 \Rightarrow 3$ Corolario 2.
$3 \Leftrightarrow 4$ Teorema 22
$4 \Leftrightarrow 1$ Teorema 13 □

Teorema 19. *Sea R un anillo con identidad. Las siguientes condiciones sobre un R-módulo unitario F son equivalentes:*

1. *F tiene una base novacía;*
2. *F es la suma directa (interna) de una famile 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 novacío X y una función $\imath : X \to F$ con la siguiente propiedad: dado un R-módulo unitario A y una función $f : X \to A$, existe un único homomorfismo de R-módulos $\bar{f} : F \to A$ tal que $\bar{f}\imath = f$. 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 20. *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 21. *Sean A y B ambos R-módulos.*

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

Teorema 22. *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*

$$\mathrm{Hom}_R(E, E) \simeq \mathrm{Mat}_n(R^{\mathrm{op}}) \tag{2.3}$$

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