Álgebras, Grupos y Representaciones

Ejercicios

Luis Antonio Ortega Andrés,
Guillermo Galindo Ortuño

April 2, 2020

Ejercicio 1. *Sea A un anillo. Diremos que A es trivial si $A = \{0\}$. Demostrar que A es trivial si, y sólo si,* $1 = 0$.

Supongamos que A es trivial, entonces como A es un anillo, $\exists 1 \in A \implies 0 = 1$. Sea ahora $1 = 0$, sea $a \in A$ se tiene que $a = a * 1 = a * 0 = 0 \implies A = \{0\}$.

Ejercicio 2. *Sea K un cuerpo y $M_n(K)$ el anillo de matrices cuadradas de orden n con entradas en K. Demostrar que $Z(M_n(K)) = \{kI_n \mid k \in K\}$, donde I_n es la matriz identidad de orden n.*

Es evidente que $\{kI_n \mid k \in K\} \subset Z(M_n(K))$. Tomemos $A \in Z(M_n(K))$, $E_{ij} \in M_n(K)$ la matriz de ceros salvo un 1 en la position (i, j). Se tiene que

$$E_{ij}A = AE_{ij} \ \forall i, j \in \{0, \dots, n-1\}$$

Pero es sencillo comprobar que $E_{ij}A$ es una matriz de ceros salvo por tener la fila j-ésima de A en la fila i-ésima. De igual forma AE_{ij} es una matriz de ceros salvo por tener la columna i-ésima de A en la columna j-ésima.
Luego estamos igualando una matriz con una sola fila no nula y una con una sola columna no nula, por ello A debe ser diagonal. Además, el valor i-ésimo y el valor j-ésimo de la diagonal deben coincidir. Con esto $A \in \{kI_n \mid k \in K\}$.

Ejercicio 3. *Sea V un espacio vectorial sobre un cuerpo K y el conjunto*

$$End_K(V) = \{f : V \to V \mid f \text{ es } K\text{-lineal}\}$$

comprobar que es un subanillo de $End(V)$. Consideremos la aplicación $h : K \to End_K(V)$ que asigna a cada $k \in K$ la homotecia $h(k) : V \to V$, definido por $h(k)(v) = kv \ \forall v \in V$. Comprobar que h está bien definida y que es un morfismo de anillos. Además si $T : V \to V$ es K-lineal y $k \in K$, comprobar que $T \circ h(k) = h(k) \circ T$, luego $Im(h) \subset Z(End_K(V))$. Con esto $End_K(V)$ es una K-álgebra.

Es claro que con las operaciones de $End(V)$, se converva la K-linealidad, luego $End_K(V)$ es un subanillo.
La aplicación h está bien definida por ser V un espacio vectorial sobre K. Veamos que es un morfismo de anillos.

- Sean $a, b \in K$ y $v \in V$, $h(a+b)(v) = (a+b)v = av+bv = h(a)(v)+h(b)(v) = (h(a)+h(b))(v)$
- Sean $a, b \in K$ y $v \in V$, $h(ab)(v) = (ab)v = a(bv) = ak(b)(v) = k(a) \circ k(b)(v)$
- Sea $v \in V$, $k(1)(v) = 1v = v = Id(v)$

Hagamos la última comprobación que se nos pide $T \circ h(k)(v) = T(kv) = kT(v) = h(k) \circ T(v)$.

Ejercicio 4. *Supongamos que A y B son K-álgebras con morfismos de estructura ρ_A y ρ_B. Sea $\phi : A \to B$ un morfismo de anillos. Demostrar que ϕ es un morfismo de K-álgebras si, y sólo si, $\phi \circ \rho_A = \rho_B$.*

Supongamos que $\phi \circ \rho_A = \rho_B$, sean $k \in K$ y $a \in A$

$$\phi(ka) = \phi(\rho_A(k) \star a) = \phi \circ \rho_A(k) \star \phi(a) = \rho_B(k) \star \phi(a) = k\phi(a)$$

Que es la única propiedad que necesita ϕ para ser un morfismo de K-espacios vectoriales.
Supongamos ahora que ϕ un morfismo de K-álgebras, veamos que $\phi \circ \rho_A = \rho_B$. Sea $k \in K, b \in B$

$$\phi \circ \rho_A(k) = \phi(k \star 1_A) = \phi(k) \star \phi(1_A) = k \star 1_B = k1_B = \rho_B(k)$$

Ejercicio 5. *Sea A un espacio vectorial sobre un cuerpo K. Demostrar que dar una estructura de K-álgebra asociativa unital sobre A es equivalente a dar una multiplicación asociativa K-bilineal $\star : A \times A \to A$ junto con una aplicación K-lineal $\tau : K \to A$ tal que $\tau(k) \star a = ka = a \star \tau(k)$ $\forall k \in K, a \in A$*

Supongamos que tenemos una estructura de K-álgebra sobre A. Denotamos $\star$ a la multiplicación de A como anillo y $\tau : K \to Z(A)$ al morfismo que dota de estructura de K-álgebra. Veamos que τ es K-lineal, sea $k \in K$:

$$\tau(k) = \tau(k) \star 1_A = k1_A = k\tau(1_K)$$

Comprobemos ahora que $\star$ es K-bilineal, la bilinealidad viene dada por la estructura de anillo. Sean $k \in K, a, b \in A$

$$k(a \star b) = \tau(k) \star (a \star b) = (\tau(k) \star a) \star b = (ka) \star b$$

$$k(a \star b) = \tau(k) \star (a \star b) = (\tau(k) \star a) \star b = (a \star \tau(k)) \star b = a \star (\tau(k) \star b) = a \star (kb)$$

Supongamos ahora que tenemos ambas aplicaciones definidas. Notamos que $\tau(1_K) \star a = 1_K a = a = a \star \tau(1_K)$. Luego $\tau(1_K) := 1_A$ actua como elemento neutro de A para la operación $\star$. Si comprobamos que A con $(\star, 1_A)$ es un anillo, entonces tendremos que A es una K-álgebra. Como la operación es asociativa por hipótesis y ya tenemos el elemento neutro, solo nos quedaría comprobar la distributividad que la tenemos por ser $\star$ una aplicación bilineal.

Ejercicio 6. * Sin Terminar. *Sea K un cuerpo. Comprobar que el anillo de polinomios es una $K[X]$-álgebra. Si ahora tomamos un ideal no nulo I de $K[X]$, comprobar que $A = K[X]/I$ tiene estructura de K-álgebra. Sabemos que existe un único polinómio $p(X) \in K[X]$ tal que $I = \langle p(X) \rangle$.*

Llamamos n al grado de $p(X)$, y suponemos $n > 0$. Comprobar que $\mathcal{B} = \{1+I, x+I, \ldots, x^{n-1}+I\}$ es una base de A como K-espacio vectorial y, por tanto $dim_K A = n$. Sea

$$p(X) = p_0 + p_1X + p_2X^2 \cdots + X^n$$

Comprobar que la matriz de $M_n(K)$ que representa al endomorfismo $\lambda(x+I)$ con respecto a la base $\mathcal{B}$ es

$$\tilde{N}(p) = \begin{bmatrix} 0 & \ldots & 0 & -p_0 \\ 1 & \ldots & 0 & -p_1 \\ \vdots & & \vdots & \vdots \\ 0 & \ldots & 1 & -p_{n-1} \end{bmatrix}$$

y que A es isomorfa a la subálgebra $\{a_0I + a_1\tilde{N}(p) + \cdots + a_{n-1}\tilde{N}(p)^{n-1} : a_0, a_1, \ldots, a_{n-1} \in K\} \subset M_n(K)$

El anillo de polinomios $K[X]$ es una K-álgebra utilizando el morfismo de anillos

$$\begin{aligned} \rho : K &\to K[X] \\ k &\mapsto k \end{aligned}$$

El morfismo de anillos que da a $A = K[X]/I$ estructura de K-álgebra es el siguiente:

$$\begin{aligned} \rho : K &\to K[X]/I \\ k &\mapsto k + I \end{aligned}$$

La comprobación de que se tratan de morfismos de anillos es rutinaria. El algoritmo de división nos asegura que todos los polinomios de A tienen grado a lo sumo $n-1$, por tanto $\mathcal{B}$ es un sistema de generadores de A y forman una base por ser linealmente independientes.
Sea el endomorfismo $\lambda(x+I)(a) = (x+I)a$, es claro que las primeras $n-1$ columnas de la matriz $\tilde{N}(p)$ corresponden a multiplicar $x+I$ por los elementos $1+I, \ldots, x^{n-2}+I$. Ahora,

$$(x+I)(x^{n-1}+I) = x^n + I = -p(X) + I$$

De ahí la última columna de la matriz.
Dado $a \in A$ con $a = (a_0, \ldots, a_{n-1})$ en $\mathcal{B}$ el morfismo de K-álgebras lleva $(a_0, \ldots, a_{n-1}) \to a_0I + a_1\tilde{N}(p) + \cdots + a_{n-1}\tilde{N}(p)^{n-1}$

Ejercicio 7. * Sin terminar *Sea K un cuerpo. Dar la lista, salvo isomorfismos, de todas las K-álgebras asociativas unitales de dimensión 2.*

Sea A una K-álgebra con morfismo de estructura ρ. Sea $\{1, a\}$ la base de A como espacio vectorial. Consideramos

$$\begin{aligned} f : K[X] &\to A \\ \alpha &\mapsto \rho(\alpha) \\ x &\mapsto a \end{aligned}$$

Es un morfismo de álgebras por ser $\rho = f \circ \rho_K$ con ρ_K el morfismo de estructura de $K[X]$.

Notamos que la imagen de f tiene dimensión 2 como espacio vectorial, luego es sobreyectivo (?). Esto nos dice que existe I ideal de $K[X]$ tal que $K[X]/I \cong A$. Por ello, buscar álgebras de dimensión 2 es equivalente a buscar ideales del anillo de polinomios $K[X]$.
Tenemos entonces 3 opciones

- $K[X]/\langle x^2 - 1\rangle$
- $K[X]/\langle x^2 + 1\rangle$
- $K[X]/\langle x^2\rangle$

Ejercicio 8. *Expresar el cuerpo* $\mathbb{Q}(\sqrt{2}$ *como una* $\mathbb{Q}$*-álgebra de un álgebra de matrices sobre* $\mathbb{Q}$*.*

Tomamos la base $\mathcal{B} = \{1, \sqrt{2}\}$, el morfismo inyectivo de $\mathbb{Q}$-álgebras $m = M_{\mathcal{B}} \circ \lambda : \mathbb{Q} \to M_{,,}(\mathbb{Q})$ verificando:

- $\lambda(a + b\sqrt{2})(1) = a + b\sqrt{2} \implies (a, b)$ en $\mathbb{B}$
- $\lambda(a + b\sqrt{2})(\sqrt{2}) = a\sqrt{2} + 2b \implies (2b, a)$ en $\mathbb{B}$

Luego

$$\mathbb{Q}(\sqrt{2}) \cong \{m(a + b\sqrt{2}), a, b \in \mathbb{Q}\} \cong \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}, a, b \in \mathbb{Q} \right\}$$

Ejercicio 9. *Sea*

$$\mathbb{H} = \left\{ \begin{bmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{bmatrix} \ : \ \alpha, \beta \in \mathbb{C} \right\}$$

1. Demostrar que $\mathbb{H}$ *es una subálgebra real de* $M_2(\mathbb{C})$ *y que* $Z(\mathbb{H}) = \mathbb{R}$
2. Demostrar que todo elemento no nulo de $\mathbb{H}$ *es una unidad*
3. Demostrar que las matrices

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \mathbf{i} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \mathbf{j} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

forman una base de $\mathbb{H}$ *como espacio vectorial real.*
4. Comprobar las identidades

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1},\ \mathbf{ij} = \mathbf{k},\ \mathbf{jk} = \mathbf{i},\ \mathbf{ki} = \mathbf{j}$$

Para ver que es una subálgebra, vemos que $\mathbb{H}$ es un subespacio vectorial de $M_2(\mathbb{C})$, vemos que es cerrado para la suma de matrices

$$\begin{bmatrix} \alpha_1 & -\bar{\beta_1} \\ \beta_1 & \bar{\alpha_1} \end{bmatrix} \begin{bmatrix} \alpha_2 & -\bar{\beta_2} \\ \beta_2 & \bar{\alpha_2} \end{bmatrix} = \begin{bmatrix} \alpha_1 + \alpha_2 & -\bar{\beta_1} + \bar{\beta_2} \\ \beta_1 + \beta_2 & \bar{\alpha_1} + \bar{\alpha_2} \end{bmatrix}$$

y para la multiplicación

$$\begin{bmatrix} \alpha_1 & -\bar{\beta_1} \\ \beta_1 & \bar{\alpha_1} \end{bmatrix} \begin{bmatrix} \alpha_2 & -\bar{\beta_2} \\ \beta_2 & \bar{\alpha_2} \end{bmatrix} = \begin{bmatrix} \alpha_1\alpha_2 - \bar{\beta_1}\beta_2 & -\alpha_1\bar{\beta_2} - \bar{\beta_1}\bar{\alpha_2} \\ \beta_1\alpha_2 + \bar{\alpha_1}\beta_2 & -\beta_1\bar{\beta_2} + \bar{\alpha_1}\bar{\alpha_2} \end{bmatrix}$$

además $1 \in \mathbb{H}$
Para que un elemento esté en el centro deben coincidir

$$\begin{bmatrix} \alpha_1 & -\bar{\beta_1} \\ \beta_1 & \bar{\alpha_1} \end{bmatrix} \begin{bmatrix} \alpha_2 & -\bar{\beta_2} \\ \beta_2 & \bar{\alpha_2} \end{bmatrix} = \begin{bmatrix} \alpha_1\alpha_2 - \bar{\beta_1}\beta_2 & -\alpha_1\bar{\beta_2} - \bar{\beta_1}\bar{\alpha_2} \\ \beta_1\alpha_2 + \bar{\alpha_1}\beta_2 & -\beta_1\bar{\beta_2} + \bar{\alpha_1}\bar{\alpha_2} \end{bmatrix}$$

$$\begin{bmatrix} \alpha_2 & -\bar{\beta_2} \\ \beta_2 & \bar{\alpha_2} \end{bmatrix} \begin{bmatrix} \alpha_1 & -\bar{\beta_1} \\ \beta_1 & \bar{\alpha_1} \end{bmatrix} = \begin{bmatrix} \alpha_2\alpha_1 - \bar{\beta_2}\beta_1 & -\alpha_2\bar{\beta_1} - \bar{\beta_2}\bar{\alpha_1} \\ \beta_2\alpha_1 + \bar{\alpha_2}\beta_1 & -\beta_2\bar{\beta_1} + \bar{\alpha_2}\bar{\alpha_1} \end{bmatrix}$$

Para tener esto necesitamos $\beta_1\alpha_2 + \bar{\alpha_1}\beta_2 = \beta_2\alpha_1 + \bar{\alpha_2}\beta_1 \implies \beta_1 = 0$ y $\alpha_1 = \bar{\alpha_1}$. Luego $\alpha \in \mathbb{R}$

$$Z(\mathbb{H}) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : \ a \in \mathbb{R} \right\} \cong \mathbb{R}$$

2. Para ver que todo elemento es una unidad basta tomar

$$\begin{bmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{bmatrix}^{-1} = \begin{bmatrix} \bar{\alpha}/\|\alpha\| & \bar{\beta}/\|\beta\| \\ -\beta/\|\beta\| & \alpha/\|\alpha\| \end{bmatrix}$$

3. Veamos ahora que dichas matrices son una base, es sencillo ver que son linealmente independientes, luego comprobemos que son un sistema de generadores

$$\begin{bmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{bmatrix} = Re(\alpha)\mathbf{1} + Re(\beta)\mathbf{i} + Im(\alpha)\mathbf{j} + Im(\beta)\mathbf{k}$$

4. Para comprobar dichas identidades basta con realizar las cuentas correspondientes.

Ejercicio 10. *Dado un A-módulo V no nulo, demostrar que*

$$Ann_A(V) = \{a \in A : av = 0 \ \forall v \in V\}$$

es un ideal de A. Dotar a V de estructura de $A/Ann_A(V)$-módulo fiel (es decir, la representación correspondiente es fiel).

Sean $a, b \in Ann_A(V)$, tenemos que $(a+b)(v) = av + bv = 0 \implies a + b \in Ann_A(V)$. Sea ahora $a \in Ann_A(V), b \in A$, $(ab)v = a(bv) = 0 \implies ab \in Ann_A(V)$ luego tenemos un ideal.
Una representación es fiel si y solo si su núcleo es trivial. Sea ρ el morfismo de estructura de V, tenemos que $Ker(\rho) = Ann_A(V)$ que hemos visto es un ideal, luego para dotar a V de estructura de $A/Ann_A(V)$-módulo fiel definimos el morfismo de estructura

$$\begin{gathered} \tau : A/Ann_A(V) \to End(V) \\ a + Ann_A(V) \mapsto \rho(a) \end{gathered}$$

Ejercicio 11. *Sea M un A-módulo*

1. *Dados submódulos $N_1, \ldots, N_m$ de M, tenemos que*

$$N_1 + \cdots + N_m = \{n_1 + \cdots + n_m : n_i \in Ni\}.$$

2. *Dado* $X = \{m_1, \dots, m_n\} \subset M$*, tenemos que* $RX = Rm_1 + \cdots + Rm_n$*.*

1. Por $N_1, \dots, N_m$ submódulos es claro que $N_1 \cup \cdots \cup N_m \subset \{n_1 + \cdots + n_m : n_i \in Ni\}$ y que $\{n_1 + \cdots + n_m : n_i \in Ni\}$ es también un submódulos de M.
Supongamos ahora que existe N submódulo de M con $\cup_i N_i \subset N$ submódulo de M. Para cualesquiera $n_1, \dots, n_m$ en $N_1, \dots, N_m$ respectivamente, por contener N a la unión de todos los N_i,

$$n_i \in N \forall i = 1, \dots, m.$$

Y por N submódulo,

$$\sum_i n_i \in N \implies \{n_1 + \cdots + n_m : n_i \in Ni\} \subset N.$$

2. La inclusión de izquierda a derecha es inmediata pues $Rm_1 + \cdots + Rm_n$ es un submódulo que contiene X. Para la otra inclusión, claramente $Rm_1, \dots, Rm_n \subset Rx$. Ahora, usando el apartado anterior, y que Rx es un submódulo de M, tenemos $Rm_1 + \cdots + Rm_n \subset Rx$

Ejercicio 12. *Demostrar que un conjunto de generadores* $m_i : i \in I$ *de un módulo* ${}_AM$ *es una base si, y solo si, la igualdad* $\sum_i r_i m_i = 0$ *para* $r_i \in A$ *implica* $r_i = 0$ *para todo* $\forall i \in I$*. Dar un ejemplo de módulo no nulo finitamente generado que no sea libre.*

Razonemos por contradicción para la primera implicación. Supongamos que $m_1, \dots, m_n$ es base de ${}_AM$ y que existen $r_1, \dots, r_n$, con $r_k \neq 0$ tal que $\sum_i r_i m_i = 0$. Sea $m \in M$ con $m = \sum_i a_i m_i$. Entonces

$$m = \sum_i a_i m_i = \sum_i a_i m_i + \sum_i r_i m_i = \sum_i (a_i + r_i) m_i$$

con $a_k + r_k \neq a_k$. Por tanto $m_1, \dots, m_n$ no sería base.
Para la otra implicación, supongamos que existen $a_1, \dots, a_n, a'_1, \dots a'_n \in A$ tales que $\sum_i a_i m_i = \sum_i a'_i m_i$. Entonces,

$$\sum_i a_i m_i - \sum_i a'_i m_i = 0 \implies \sum_i (a_i - a'_i) m_i = 0 \implies a_i = a'_i \quad \forall i \in I.$$

Un ejemplo de módulo no nulo finitamente generado que no sea libre es $\mathbb{Z}_2$ visto como $\mathbb{Z}$-módulo. Claramente es finitamente generado pues solo tiene 2 elementos, y la única posible base sería 1, pero no lo es por $2 \cdot 1 = 0$

Ejercicio 13. *Para cada* A*-módulo* M*, demostrar que el conjunto* $End_A(M)$ *es un subanillo de* $End(M)$*. Demostrar que si, además,* M *es libre con base* $m_1, \dots, m_n$*, entonces* $End_A(M)^{op}$ *es isomorfo, como anillo, a* $M_n(A)$*. Discutir qué ocurre cuando* A *es un álgebra sobre un cuerpo* K*.*

Veamos que $End_A(M)$ es un subanillo. Sean $f, g \in End_A(M)$. Entonces

- $(f + g)(am) = f(am) + g(am) = a(f(m) + g(m)) = a(f + g)(m)$
- $(fg)(am) = f(g(am)) = a(f(g(m))) = a(fg)(m)$
- $id(am) = am = a(id)(m)$

.
Ahora, por $m_1, \dots, m_n$ base de M, dado $f \in End_A(M)$, podemos realizar el procedimiento similar al que utilzamos para aplicaciones lineales en espacios vectoriales, definiendo el morfismo $\varphi : End_A(M)^{op} \to M_n(A) con$:

$$\varphi(f) = (a_{ij})^t =: \Lambda_f$$

donde a_{ij} viene dado por $f(m_j) = \sum_i a_{ij} m_i$. La inversa sería, dada una matriz, el endomorfismo asociado a su transpuesta (de manera análoga a como se hace para aplicaciones lineales de espacios vectoriales). Para ver que son morfismo de anillos únicamente probaremos que respetan el producto, pues el resto de propiedades son inmediatas. Sean $f, g \in End_A(M)^{op}$,

$$\varphi(f * g) = \varphi(g \circ f) = (\Lambda_g * \Lambda_f)^t = (\Lambda_f)^t * (\Lambda_g)^t = \varphi(f) * \varphi(g).$$

Ejercicio 14. *Sea M un módulo sobre una álgebra finito-dimensional A. Demostrar que si M admite bases $\{m_1, \dots, m_r\}$ y $\{n_1, \dots, n_t\}$, entonces $r = t$.*

Supongamos $r \neq t$, entonces $M \cong A^r$ y $M \cong A^t \implies A^r \cong A^t$, pero como A es finito-dimensional, sabemos que eso no puede pasar si $r \neq t$.

Ejercicio 15 . *Sea θ y $T_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ el endomorfismo que gira los vectores un ángulo θ en sentido contrario de las agujas del reloj. Consideremos la correspondiente estructura de $R[X]$-módulo definida por T_θ sobre $\mathbb{R}^2$. Llamamos a este módulo V_θ. Discutir para que valores de θ es V_θ simple.*

Claramente, si $\theta = k\pi$ para algún $k \in \mathbb{N}$, el submódulo generado por cualquier vector es la recta vetorial con ese vector director, y por tanto V_θ no es simple.
Por otro lado, si $\theta \neq k\pi \forall k \in \mathbb{N}$, tomando un vector v cualquiera, y $T_\theta(v)$ forman una base de $\mathbb{R}^2$, y por tanto cualquier submódulo distinto del vacío es el total y V_θ es simple

Ejercicio 16 *Siguiendo la notación del Ejercicio 15, ¿para qué valores θ, θ' son los $\mathbb{R}[X]$-módulos $V_\theta, V_{\theta'}$ isomorfos?*

Idea: Si es $q \cdot \pi$ siendo q racional únicamente si $\theta y \theta'$ son el mismo ángulo u opuestos. Si son el mismo el morfismo es la identidad, y si son opuestos, fijas un vector, y el morfismo es el que lleva cada vector en el simétrico respecto del eje dado por dicho vector. En caso contrario, tras aplicar un número de veces el giro sobre V_θ volvemos al vector original, y sin embargo eso no ocurre en el nuevo. (No está formalizado y es muy probable que esté mal.)

Ejercicio 17 *Sea M un A-módulo. Demostrar que M es simple si, y solo si, $M = Am$ paa todo $0 \neq m \in M$.*

Claramente, si M es simple, por Am submódulo tiene que ser M o $\{0\}$, y por $m \neq 0$ tenemos que $Am = M$.
La otra implicación es también casi inmediata. Supongamos que existe $N \subset M$ submódulo distinto de $\{0\}$. Entonces, sea $n \in N$ distinto de 0, tenemos que $An \subset N$, pero como $An = M$, $N = M$.

Ejercicio 18 *Sea A un anillo. Demostrar que A es un anillo de división si, y solo si, A es un A-módulo simple.*

Supongamos que A es un anillo de división. Entonces, para todo $0 \neq m \in A$ tenemos que $1 \in Am$ y por tanto $Am = A$, y usando el ejercicio anterior tenemos que A es un A-módulo simple.
Supongamos ahora que A es un A-módulo simple. Entonces para todo $0 \neq m \in A$ tenemos que $Am = A$, y por tanto, $1 \in Am$, y como la acción de A es el producto, existe un elemento $a^{-1} \in A$ tal que $a^{-1}a = 1$.

Ejercicio 20. * *Consideramos $T : \mathbb{R}^3 \to \mathbb{R}^3$ una aplicación lineal, y la estructura de $\mathbb{R}[X]$-módulo correspondiente sobre $\mathbb{R}^3$. Discutir los posibles valores de la longitud de $\mathbb{R}^3$ como $\mathbb{R}[X]$-módulo, dependiendo de como sea T. Poner un ejemplo de T para que se alcance cada longitud.*

Sabemos que un submódulo de nuestro $\mathbb{R}[x]$-módulo sobre $\mathbb{R}^3$ tiene que ser un subespacio de este, por tanto las posibles longitudes son $1, 2$ o 3.

Veamos que, para cualquier espacio real de dimensión n, y cualquier operador lineal T, debe existir un subespacio invariante por T ya sea de dimensión 1 o dimensión 2, donde un subespacio invariante es equivalente a ser un submódulo, esto nos permitirá descartar el caso en el que no exista ningún submódulo y la longitud sea 1.

Si tomamos un vector no nulo $v \in \mathbb{R}^n$, sabemos que existen unos coeficientes reales $a_0, \dots, a_n$ tal que
$$0 = a_0 v + \cdots + a_n T^n(v) = (a_0 I + \cdots + a_n T^n)(v)$$
Factoriamos este polinomio en T en factores irreducibles de grado 1 y 2. Como el polinomio no es inyectivo, alguno de dichos factores debe no serlo.

- **Caso 1.** Un factor de grado 1 no es inyectivo, sea este factor de la forma $T - \lambda I$, $\exists u \in \mathbb{R}^3$ tal que $(T - \lambda I)(u) = 0 \implies T(u) = \lambda u \implies \langle u \rangle$ es un submódulo. Notamos además que u es un vector propio.

- **Caso 2.** Un factor de grado 2 no es inyectivo, sea ese factor $T^2 + \alpha T + \beta I$, $\exists u \in \mathbb{R}^3$ tal que $(T^2 + \alpha T + \beta I)(u) = 0$. Sea entonces $U =< u, T(u) >$, como $T^2(u) = -\alpha T(u) - \beta u$, U es un submódulo.

Además es facil comprobar que todos los submódulos se generan de esta forma, pues sea $\langle u \rangle = U$ un submódulo, se tiene que $T(u) \in U \implies \exists a \in \mathbb{R}$ tal que $T(u) = au$, luego u es un vector propio. En caso de ser $U = \langle u, v \rangle$, si alguno de ellos no es un vector propio, digamos por ejemplo u, entonces $T(u)$ y u son linealmente independientes y $T(u) \in U \implies U = \langle u, T(u) \rangle$.

Como estamos en $\mathbb{R}^3$, la descomposición en irreducibles del polinomio característico de T contiene un polinomio de grado 1, luego siempre existe un vector propio.

Nos limitamos a tres casos en el estudio de la longitud (los casos anteriores no son excluyentes), a saber

- Existe un único valor propio, y para el vector propio asociado u no existe ningún espacio de la forma $\langle v, T(v)\rangle$ que contenga a u, invariante por T. Entonces tenemos la serie de composición

  $$0 \subset \langle u\rangle \subset \mathbb{R}^3$$

  luego la longitud es 2.

- Existe un único valor propio, y el vector propio asociado u se encuentra dentro de un submódulo de dimensión 2 $\langle v, T(v)\rangle$, tenemos entonces

  $$0 \subset \langle u\rangle \subset \langle v, T(v)\rangle \subset \mathbb{R}^3$$

  luego la longitud es 3.

- Existen 3 valores propios, en cuyo caso, tomando dos vectores propios u, v, tenemos que

  $$0 \subset \langle u\rangle \subset \langle u, v\rangle \subset \mathbb{R}^3$$

  luego la longitud es 3.

A continuación mostramos un ejemplo de aplicación lineal $T : \mathbb{R}^3 \to \mathbb{R}^3$ que genere un módulo de cada una de las posibles longitudes. Para dar la aplicación lineal únicamente tendremos que definir la imagen de una base de nuestro espacio, y por tanto utilizaremos la base usual $\{(1,0,0),(0,1,0),(0,0,1)$ por comodidad.

Longitud 2

$$\begin{aligned} T : \mathbb{R}^3 &\to \mathbb{R}^3 \\ (1,0,0) &\mapsto (0,1,0) \\ (0,1,0) &\mapsto (0,0,1) \\ (0,0,1) &\mapsto (1,0,0) \end{aligned}$$

En este caso tenemos un único valor propio, luego hay un único vector propio $u = (1,1,1)$, luego tenemos un submódulo de dimensión 1 generado por el mismo. Veamos que no se encuentra incluido dentro de ningún submódulo de dimensión 2. Supongamos que $\exists \alpha$ linealmente independiente con u, tal que $\langle u, \alpha\rangle$ es un submódulo de dimensión 2. Consideremos entondes

$$T(\alpha) = (\alpha_3, \alpha_1, \alpha_2) \notin \langle u, \alpha\rangle$$

Con esto tenemos que la serie de composición sería

$$0 \subset \langle (1,1,1)\rangle \subset \mathbb{R}^3$$

Longitud 3

$$\begin{aligned} T : \mathbb{R}^3 &\to \mathbb{R}^3 \\ x &\mapsto x \end{aligned}$$

En este caso, todos los vectores son vectores propios luego es sencillo comprobar que cualquier subespacio de $\mathbb{R}^3$ es un $\mathbb{R}[X]$-submódulo, la siguiente serie de composición nos da la longitud buscada.

$$0 \subset \langle (1,0,0)\rangle \subset \langle (1,0,0),(0,1,0)\rangle \subset \mathbb{R}^3$$

Ejercicio 21. *Sea $\mathbb{P}_n$ el espacio vectorial real de las funcione polinómicas en una variable de grado menor o igual que n. Sea $T : \mathbb{P}_n \to \mathbb{P}_n$ la aplicación lineal que asigna a cada polinomio su derivada. Calcular una serie de composición de $\mathbb{P}_n$ visto como $\mathbb{R}[X]$-módulo via T.*

Consideremos los espacios vectoriales $\mathbb{P}_{n-1}, \dots, \mathbb{P}_0$, es claro que $\mathbb{P}_i \subset \mathbb{P}_{i+1}$ $\forall i = 0, \dots, n-1$ y además son cerrados bajo derivación, luego son un submódulos. Consideramos entonces la siguiente cadena de submódulos.

$$0 \subset \mathbb{P}_0 \subset \cdots \subset \mathbb{P}_n$$

Solo nos queda comprobar que cada eslabón este formado por un submódulo maximal, tomamos $\mathbb{P}_i \subset \mathbb{P}_{i+1}$, y añadamos un polinomio p de grado $i+1$ a $\mathbb{P}_i$, entonces es claro que con las operaciones del espacio vectorial podemos construir cualquier polinomio de grado $i+1$, luego $\langle (p, \mathbb{P}_i) \rangle = \mathbb{P}_{i+1}$. Por lo tanto, los eslabones son maximales y tenemos una serie de composición.

Ejercicio 22. ** *En las condiciones del ejercicio anterior, calcular todos los $\mathbb{R}[X]$-submódulos de $\mathbb{P}_n$.*

Comencemos viendo que los subespacios vectoriales $\mathbb{P}_i$ con $i \leq n$, son también $\mathbb{R}[X]$-submódulos. Esto es evidente pues la aplicación T consiste es la derivación. Luego estos espacios son cerrados ante T.

Comprobemos ahora que estos son los únicos submódulos que tenemos. Para ello tomemos un polinomio p cualquiera de grado $m < n$. Vamos a ver quien es el submódulo que genera $\langle p \rangle$.

Supongamos que

$$p = a_0 + a_1 x + \cdots + a_m x^m$$

Consideremos entonces $T^m(p) = m! a_m \in \mathbb{R}$, luego $1 \in \langle p \rangle$. De la misma forma,

$$T^{m-1}(p) = (m-1)! a_{m-1} + m! a_m x \implies \frac{T^{m-1}(p) - (m-1)! a_{m-1}}{m! a_m} = x \in \langle p \rangle$$

Siguiendo un proceso inductivo, podemos ver entonces que $x^i \in \langle p \rangle$ $\forall i = 0, \dots, n$. Luego $\langle p \rangle = \mathbb{P}_n$.

Por ello, concluimos que $\{\mathbb{P}_i\}_{i \leq n}$ son todos los $\mathbb{R}[X]$-submódulos de $\mathbb{P}_n$.

Ejercicio 25. ** *Supongamos $T : V \to V$ un endomorfismo K-lineal, donde V es un espacio vectorial de dimensión finita que consideramos, como de costumbre, como un $K[X]$-módulo. Supongamos que el polinomio mínimo $m(X)$ de T es irreducible en $K[X]$. Demostrar que existen $K[X]$-submódulos simples $V_1, \dots, V_t$ de V tales que $V = V_1 \oplus \cdots \oplus V_t$ como $K[X]$-módulo.*

Por $m(X)$ irreducible, tenemos que $K[X]/Ker\ e_T = K[X]/m(X)$ es un cuerpo. Entonces, podemos ver V como un $K[X]/Ker\ e_T$ espacio vectorial, utilizando la misma acción que utilizamos para la estructura de $K[X]$-módulo. Para ello, tenemos que comprobar que la acción está bien definida. En efecto, sean $p(X), q(X)$ pertencientes a una misma clase del cociente,

$$p(X) = q(X) + r(X)m(X),$$

y por tanto

$$p(T) = q(T) + r(T)m(T) = q(T)$$

por $m(X) \in Ker\ e_T$.

Ahora, sea $\{v_i : i \in I\} \subset V$ un conjunto de generadores de V, por el corolario 1.6.6 existe $J \in I$ tal que $V = \oplus_{j \in J}(K[X]/Ker\ e_T)v_j$, siendo cada uno de estos submódulos simples. Ahora, volviendo a ver V como $K[X]$-módulo, los submódulos $K[X]v_j$ para $j \in J$ son simples, pues en caso de tener un súbmodulo propio M, este sería también submódulo de $(K[X]/Ker\ e_T)v_j$.

Por tanto, tenemos que $V = \sum_{j \in J} K[X]v_j$, con $K[X]v_j$ simple para todo j en J. Al igual que hicimos en el corolario 1.6.6, aplicamos el teorema 1.6.5 para obtener un Γ, con cardinal digamos t, tal que $V = \oplus_{s \in \Gamma} K[X]v_s$.

Ejercicio 26. ** *En las condiciones del ejercicio anterior, demostrar que el polinomio característico de T es $m(X)^t$.*

Probemos la siguiente proposición
Proposición. Sean $f, g, h \in K[X]$ tales que $f = gh$, y g, h son coprimos, entonces

$$Ker(f(T)) = Ker(g(T)) \oplus Ker(h(T))$$

Demostración.
Comencemos notando que $Ker(g(T)), Ker(h(T)) \in Ker(f(T))$ y $Ker(g(T))+Ker(h(T)) \in Ker(f(T))$. Por ser coprimos, existen polinomios u, v tales que

$$1 = gu + hv \implies Id = u(T)g(T) + v(T)h(T)$$

Tomemos entonces $\alpha \in Ker(f(T))$, tenemos $\alpha = u(T)g(T)\alpha + v(T)h(T)\alpha$. Donde $u(T)g(T)\alpha \in Ker(h(T))$ y $v(T)h(T)\alpha \in Ker(g(T))$, luego concluimos que $Ker(f(T)) = Ker(g(T))+Ker(h(T))$. Supongamos que existe β tal que $g(T)\beta = h(T)\beta = 0$, luego tenemos que

$$0 = u(T)g(T)\beta + v(T)h(T)\beta = \beta$$

Proposición. Sea $T : V \to V$ un endomorfismo K-lineal, con V espacio vectorial de dimensión finita. Entonces, si el polinomio mínimo $m(X)$ de T es irreducible en $K[X]$, el polinomio característico $p(X)$ de T se escribe como $m(X)^t$ para algún $t \in \mathbb{N}$.

Demostración.
Razonando por contradicción, supongamos que el polinomio característico de T es mg, donde g es primo relativo con m. Entonces, usando la proposición anterior tenemos que $V = Ker(m(T)) \oplus Ker(g(T))$. Es facil comprobar que el polinomio mínimo de T es el mínimo común múltiplo del polinomio mínimo de $T \restriction_{Ker(m(T))}$ y el polinomio mínimo $T \restriction_{Ker(g(T))}$.

Ahora, como el polinomio mínimo de $T \restriction_{Ker(m(T))}$ es m también, y este es irreducible, tenemos que $g = 1$, lo que prueba nuestro resultado.

Con esto, solo necesitamos probar que, dado un v cualquiera, la dimensión como subespacio de $K[X]v$ es el grado del polinomio mínimo, ya que, utilizando el ejercicio anterior, tendríamos que la dimensión de nuestro espacio vectorial sería $deg(m) \cdot t$. Veámoslo.
Sea $w \in K[X]v$, tenemos que $w = g(T)(v)$. Ahora bien, diviendo nuestro polinomio g por el polinomi mínimo m, tenemos que $g = mh+r$, donde r es un polinomio de grado estrictamente menor que el del polinomio mínimo. Por tanto, para cualquier polinomio g existe un polinomio r de grado estrictamente menor que el grado del polinomio mínimo m, digamos n, tal que $g(T)(v) = r(T)(v)$. Por tanto, $\{v, T(v), \ldots, T^n(v)\}$ forman un sistema de generadores de $K[X]v$.

Ejercicio 27. ** *Sea R un álgebra sobre un cuerpo de característica distinta de 2, y $a, b, e \in R$ idempotentes. Demostrar que si $e = a+b$, entonces $ab = ba = 0$. Si la característica es 2, encontrar un contraejemplo con $b \neq a$.*

Por e, a, b idempotentes, tenemos que

$$a + b = e = e^2 = a^2 + b^2 + ab + ba = a + b + ab + ba \implies ab + ba = 0.$$

Luego

$$ab = -ba. \tag{1}$$

Multiplicando a izquierda y derecha por a, por ser este idempotente tenemos que $aba = -aba$. Ahora, usando que $char(R) \neq 2$, $aba = 0$. Por último, sustituyendo ab ó ba respectivamente usando (1), tenemos

$$0 = aba = -baa = -ba \implies ba = 0$$

$$0 = aba = -aab = -ab \implies ab = 0.$$

Veamos ahora el contraejemplo. Sea $\mathbb{F}_2$ el cuerpo de dos elementos (el más sencillo con característica 2), y $M_2(\mathbb{F}_2)$ la $\mathbb{F}_2-$álgebra usual de matrices de orden 2 sobre este cuerpo. Entonces, tomamos

$$a = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix},\ b = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ e = a + b = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}.$$

En efecto, es sencillo comprobar que a, b, y e son idempotentes, y que por $b = I_2$, efectivamente $ab = ba = a \neq 0$

Ejercicio 35. ** Sin Terminar. *Sea V un K-espacio vectorial de dimensión finita n y $T : V \to V$ una aplicación lineal. Diremos que un vector $v \in V$ es cíclico para T si $\{v, T(v), \ldots, T^{n-1}(v)\}$ es una base de V como K-espacio vectorial. Demostrar que V admite un vector cíclico si, y sólo si, el polinomio mínimo de T tiene grado n. ¿Cuál es entonces la longitud de V en tanto que $K[X]$-módulo.*

Comencemos viendo que si admite un vector cíclico entonces el polinomio mínimo tiene grado n. Sabemos que el polinomio mínimo satisface que $m(T) = 0$. Supongamos que el grado de m es $n' < n$, entonces $m(T) = 0 \implies T^{n'}$ es una combinación lineal de $\{Id, T, \ldots, T^{n'-1}\}$ por lo tanto $T^{n'}(v)$ se puede escribir como combinación lineal de $\{v, T(v), \ldots, T^{n'-1}(v)\}$, luego no puede existir un vector cíclico.

Supongamos ahora que el polinomio mínimo m tiene grado n. Sea

$$m = \prod_i m_i^{n_i}$$

la descomposición de m en factores irreducibles y consideremos

$$V_i = Ker(m_i(T)) = \{v \in V \mid m_i(T)(v) = 0\}$$

Utilizando un proceso inductivo en la proposición del ejercicio 26, podemos ver que $V = \oplus_i V_i$, además, es sencillo comprobar que son submódulos de V puesto que T y $m_i(T)$ conmutan, luego $m_i(T)(T(v)) = T(m_i(T)(v)) = 0$. Notemos que $m_i^{n_i-1} \neq 0$ en V_i $\forall i$, ya que en caso contrario, lo multiplicariamos por el resto de factores irreducibles y tendríamos un polinomio que anula todo V de grado menor n.

Entonces existe $v_i \notin Ker(m_i^{n_i-1}(T))$ $\forall i$.

Si alguno de estos v_i se anulara en un $m_j(T)$ con $i \neq j$, entonces el polinomio mínimo de $\langle v_i \rangle$ divide a m_j y $m_i^{n_i}$, que como son primos relativos resulta ser 1, luego $v_i = 0$.
Consideramos entonces $x = \oplus_i v_i$, tenemos que ningún divisor de m evaluado en T anula a x. Entonces x es un vector que solo se anula por m y multiplos suyos, luego polinomio de menor grado evaluado en T y en x no resulta 0. Es decir, $\{x, T(x), \ldots, T^{n-1}(x)\}$ son linealmente independientes.