FACTORES INVARIANTES DE UN ENDOMORFISMO

por

MIGUEL L. LAPLAZA

El objeto de este trabajo ha sido la exposición del tema en el Cursillo de la Escuela de Formación del Profesorado dedicado a Matemáticas (diciembre 1966). Este tema es ya clásico dentro del álgebra y puede desarrollarse fácilmente partiendo de la estructura de los módulos de tipo finito sobre dominios principales.

En el presente trabajo hemos partido de los conocimientos elementales de espacios vectoriales (homomorfismos, suma directa, base, dimensión de variedades, ...) y de la divisibilidad y teoría de ideales en anillos de polinomios de una indeterminada sobre un cuerpo.

Todos los espacios vectoriales que usemos tendrán dimensión finita. Indicaremos por V a un espacio vectorial sobre un cuerpo k y por φ a un endomorfismo de V. Si L es una variedad lineal de V, indicaremos por φ a la restricción de φ a L.

* * *

Definición 1.—Sea L una variedad lineal. Diremos que L es invariante si φ L $\subset$ L. Definiremos, $\mathbf{a}$ (L) $= \{f(X) \mid f(X) \in K[X], f(\varphi) L = 0\}$ $\mathbf{a}$ (L) es un ideal y designaremos por a (L) al polinomio de mayor grado con coeficiente la unidad que engendra el ideal $\mathbf{a}$ (L). Si $v \in V$, y kv es la variedad engendrada por v, llamaremos $\mathbf{a}(v) = \mathbf{a}(kv)$, y es inmediato comprobar que,

$$\mathbf{a}(v) = \mathbf{a}(kv) = \{ f(X) \mid f(X) \in k[X], f(\varphi) v = 0 \}$$

Proposición 1.—a (L) $\neq \{0\}$ para cualquier L, y si L $\subset$ L′, $\mathbf{a}$ (L) $\supset$ $\mathbf{a}$ (L′). En efecto:

Si $v \in$ L, los vectores $\{ \varphi^i v \}_{vi \in Z_+}$ (en que se toma $\varphi^0 = I$, homomorfismo unidad, siendo Z_+ el conjunto de los enteros positivos) no pueden ser independientes, por ser L de dimensión finita, lo que implica que existe una relación del tipo, $\Sigma\, l_i \varphi^i v = 0$, $l_i \neq 0$, $l_i \in k$, es decir, $\Sigma\, l_i X^i \in a(v)$, $\Sigma\, l_i X^i \neq 0$.

Si $\{ e_1, \ldots, e_r \}$ es una base de L, $a(e_1)\, a(e_2) \ldots a(e_r) \in \mathbf{a}(L)$, en que, $a(e_1)\, a(e_2) \ldots a(e_r) \neq 0$.

Proposición 2.—Si L es una variedad invariante, $f(X) = a(L)$, $f(X) = f_1(X)\, f_2(X)$, en que $f_1(X)$ y $f_2(X)$ son primos entre sí, con el primer coeficiente igual a la unidad, existe una descomposición, $L = L_1 \oplus L_2$, en que L_1 y L_2 son variedades lineales invariantes, tales que, $a(L_1) = f_1(X)$, $a(L_2) = f_2(X)$.

En efecto:

Sean $L_1 = \{ v \in L \mid f_1(\varphi)\, v = 0 \}$, $L_2 = \{ v \in L \mid f_2(\varphi)\, v = 0 \}$. Como $f_1(X)$ y $f_2(X)$ son primos entre sí, existe una expresión de la forma, $1 = a_1(X)\, f_1(X) + a_2(X)\, f_2(X)$, es decir, $I = a_1(\varphi)\, f_1(\varphi) + a_2(\varphi)\, f_2(\varphi)$, y si $v \in L$, $v = a_1(\varphi)\, f_1(\varphi)\, v + a_2(\varphi)\, f_2(\varphi)\, v$, en que, $a_1(\varphi)\, f_1(\varphi)\, v \in L_2$, $a_2(\varphi)\, f_2(\varphi)\, v \in L_1$, por lo que $L = L_1 + L_2$. Si $v \in L_1 \cap L_2$, $f_1(\varphi)\, v = f_2(\varphi)\, v = 0$, lo que implica que $v = a_1(\varphi)\, f_1(\varphi)\, v + a_2(\varphi)\, f_2(\varphi)\, v = 0$, es decir, $L_1 \cap L_2 = \{ 0 \}$, por lo que, $L = L_1 \oplus L_2$.

$\varphi\, L_1 \subset L_1$, puesto que, $f_1(\varphi)\, v = 0 \Longrightarrow f_1(\varphi)\, \varphi\, v = \varphi\, f_1(\varphi)\, v = 0$. Y por lo tanto, L_1 y L_2 son invariantes.

De acuerdo con la definición, $f_1(X) \in \mathbf{a}(L_1)$; si $g(X) \in \mathbf{a}(L_1)$, $f_2(X)\, g(X) \in \mathbf{a}(L_1 + L_2)$, luego $f_2(X)\, g(X) = f_1(X)\, r(X)$, lo que implica, por ser $f_1(X)$ y $f_2(X)$ primos entre sí, que $g(X) = f_1(X)\, s(X)$ y, por consiguiente, a $(L_1) = f_1(X)$.

Proposición 3.—Si $f(X) = a(L)$, L variedad invariante, $f(X) = \Pi\, p_i^{\,n_i}(X)$, en que $p_i(X)$ es un polinomio primo con el mayor coeficiente igual a la unidad, existe una descomposición, $L = \oplus L_i$, en que L_i es una variedad invariante, tal que, $p_i^{\,n_i}(X) = a(L_i)$.

Para demostrar esta proposición basta aplicar de manera recurrente los resultados de la proposición anterior.

Proposición 4.—Si $f(X) = a(L)$, L variedad lineal invariante, $f(X) = p^r(X)$, en que $p(X)$ es un polinomio primo, cuyo primer coeficiente es la unidad, existe un $v \in L$, tal que $a(v) = f(X)$.

En efecto:

Sea $\{ e_1, \ldots, e_r \}$ una base de L; como $\mathbf{a}(e_i) \supset \mathbf{a}(L)$, $a(e_i) = p^{r_i}(X)$, $r_i \leq r$; si para todo i, $r_i \neq r$, $p^{r-1}(\varphi)\, e_i = 0$, para todo i, lo que implicaría que, $p^{r-1}(X) \in \mathbf{a}(L)$, lo que está en contradicción con que, $a(L) = p^r(X)$.

Proposición 5.—Si $f(X) = a(L)$, L variedad lineal invariante, existe un $v \in L$, tal que, $a(v) = f(X)$.

En efecto:

De acuerdo con la proposición 3, si $f(X) = \Pi\, p_i^{\,r_i}(X)$ es la descomposición de $f(X)$ en potencias de polinomios primos, $L = \oplus L_i$, en que L_i son variedades invariantes, y $a(L_i) = p_i^{\,r_i}(X)$. De acuerdo con la proposición 4, existe un $v_i \in L_i$, tal que $a(v) = p_i^{\,r_i}(X)$. El elemento, $v = \Sigma\, v_i$, es tal que si $g(\varphi)\, v = 0$, como $g(\varphi)\, v_i \in L_i$, y $L = \oplus L_i$, se deduce de ahí que, $g(\varphi)\, v_i = 0$, para todo i, lo que implica que, $g(X)$ es múltiplo de $p_i{}^{r_i}(X)$, para todo i, de donde se deduce que g (X) es múltiplo de $f(X)$, y como $f(X) \in \mathbf{a}(v)$, $a(v) = f(X)$.

Proposición 6.—Sea L una variedad invariante, tal que $\varphi L = L$. Existe una descomposición, $L = L_1 \oplus L_2 \dots L_r$, unos polinomios, $f_1(X), f_2(X), \dots, f_r(X)$, y unos elementos, $v_i \in L_i$, tales que,

a) $L_1, L_2 \dots, L_r$ son variedades invariantes.

b) $a(v_i) = a(L_i) = f_i(X)$.

c) $\{v_i, \varphi v_i, \dots, \varphi^{n_i-1}v_i\}$ es una base de L_i, siendo n_i el grado de $f_i(X)$.

d) $f_1(X) = a(L)$.

e) $f_i(X)$ es múltiplo de $f_{i+1}(X)$.

En efecto:

Observemos primeramente que *d)* es consecuencia de *a)*, *b)* y *c)*, pero lo hemos puesto en la forma anterior por ser más cómodo de esta manera para la demostración por inducción. Vamos a demostrarlo por inducción sobre la dimensión de L. Para $\dim L = 1$, es inmediato, puesto que $L = L_1$ en la descomposición y basta tomar un vector $v \in L$, $v \neq 0$, para que se verifiquen las condiciones de la proposición. Tomemos $f_1(X) = a(L)$, y $L_1 = \{v_1 \varphi v_1, \dots, \varphi^{n_1-1}v_1\}$, en que, $a(v_1) = f_1(X)$, elemento que existe, de acuerdo con la proposición 5. L_1 es invariante, puesto que, $\varphi \varphi^{n_1-1}v_1 = \varphi^{n_1}v_1 = -a_{10} - a_{11}\varphi v_1 - \dots - a_{1n_1-1}\varphi^{n_1-1}v$, siendo, $f_1(X) = a_{10} + a_{11}X + \dots + a_{1n_1-1}X^{n_1-1} + X^{n_1}$. Por otra parte, $\varphi L_1 = L_1$, puesto que $\varphi L = L$, implica que φ es un isomorfismo.

Sea $\overline{\varphi} : L/L_1 \to L/L_1$ la correspondencia definida por, $\overline{\varphi}(v + L_1) = \varphi v + L_1$. Se comprueba fácilmente que es un homomorfismo; veamos que es inyectivo: $\overline{\varphi}(v + L_1) = 0 \Rightarrow \varphi v \in L_1 = \varphi L_1$, por lo que, $\varphi v = \varphi v'$, $v' \in L_1$, $v = v'$, $v + L_1 = 0$, y $\overline{\varphi}$ es por lo tanto un homomorfismo que cumple las hipótesis de inducción (pues $\dim L/L_1 < \dim L$), por lo que existe una descomposición $L/L_1 = \overline{L}_2 \oplus \overline{L}_3 \dots \overline{L}_r$, unos polinomios $f_2(X), \dots, f_r(X)$ y unos elementos $v_i + L_1 \in \overline{L}_i$, tales que,

i) $\overline{L}_2, \dots, \overline{L}_r$ son variedades invariantes en

ii) $a(v_i + L_1) = a(\overline{L}_i) = f_i(X)$.

iii) $\{v_i + L_1, \varphi v_i + L_1, \dots, \varphi^{n_i-1}v_i + L_1\}$ es una base de L_i, siendo n_i el grado de $f_i(X)$.

iv) $f_2(X) = a(L/L_1)$.

v) $f_i(X)$ es múltiplo de $f_{i+1}(X)$, para $i = 2, 3, \dots, r-1$.

Veamos que se puede tomar v_i de modo que además de las hipótesis anteriores verifique que $a(v_i) = f_i(X)$. De acuerdo con *ii)*, $f_i(\varphi)v_i = g(\varphi)v_i$; sea $f(X) = a(v_i)$; $f_i(X)$ divide a $f(X)$, pues $g(\varphi)v_i = 0 \Rightarrow g(X) \in \mathbf{a}(v_i + L_1)$; de aquí se deduce que $[f/f_i(\varphi)]f_i(\varphi)v_i = 0 = [f/f_i(\varphi)]g(\varphi)v_1$, lo que implica que, $f(X)g(X)/f_i(X) = f_1(X)r(X)$, es decir, $g(X) = f_1(X)f_i(X)r(X)/f(X)$, y como $f_1(X)$ es múltiplo de $f(X)$, $g(X)$ multiplica a $f_i(X)$. Por lo tanto, $f_i(\varphi)v_i = f_i(\varphi)g_1(\varphi)v_1$; el elemento $v_i - g_1(\varphi)v_1$ cumple las condiciones *a)*, *b)*, *c)*, *d)* y *e)*, y además, $f_i(\varphi)[v_i - g_1(\varphi)v_1] = 0$, lo que implica que, $a(v_i) = f_i(X)$, puesto que en cualquier caso, $a(v_i)$ ha de ser múltiplo de $f_i(X)$.

Definamos, $L_i = \{v_i, \varphi v_i, \dots, \varphi^{n_i-1}v_i\}$, $i = 2, 3, \dots, r$. Se deduce de esta definición que, $\{v_i, \varphi v_i, \dots, \varphi^{n_i-1}v_i\}$ es una base de L_i, por ser $\{v_i + L_1, \varphi v_i + L_1, \dots, \varphi^{n_i-1}v_i + L_1\}$ una base de $\overline{L}_i$.

Los elementos $\{ v_1, \varphi v_1, \ldots, \varphi^{n_1-1} v_1, v_2, \varphi v_2, \ldots, \varphi^{n_r-1} v_r \}$ constituyen un sistema de generadores de L (por ser unión de un sistema de generadores del núcleo con un conjunto cuya imagen es un sistema de generadores del espacio imagen), y como $\dim L = \dim L_1 + \dim \overline{L}_2 + \ldots + \dim \overline{L}_r = \Sigma n_i$, los elementos considerados son independientes y constituyen una base y L se descompone en la forma $L = L_1 \oplus L_2 \oplus \ldots L_r$. Veamos que se cumplen las condiciones de la proposición.

b) $a(v_1) = f_1(X) = a(L_1)$, de acuerdo con la definición de v_1 y de L_1. Para $i \neq 1$, $a(v_i) = f_i(X)$, de acuerdo con la elección que hemos hecho de v_i. Esto implica que $a(v_i)$ divide a $a(L_i)$ y como $f_i(\varphi)\, \varphi / v_i = \varphi\, / f_i(\varphi)\, v_i = 0$, $f_i(X)$ divide a $a(L_i)$, lo que implica que $a(v_i) = f_i(X) = a(L_i)$.

a) De acuerdo con el resultado anterior, $L_2, \ldots L_r$, han de ser invariantes, puesto que $\varphi^{n_i} v + a_{in_i-1} \varphi^{n_i-1} v_i + \ldots + a_{i_0} = 0$, y ya hemos demostrado anteriormente que L_1 es invariante.

c), d) y *e)* se deducen inmediatamente de las definiciones.

Proposición 7.—Sea L una variedad lineal invariante. Se puede encontrar una descomposición de la forma, $L = \ker \oplus L'$, en que $\varphi L' = L'$.

En efecto:

Sea $\overline{\varphi} : L/\ker \varphi \rightarrow L/\ker \varphi$ la correspondencia definida por $\overline{\varphi}(a + \ker) = \varphi a + \ker \varphi$. Se comprueba de modo inmediato que $\overline{\varphi}$ es un homomorfismo. La existencia de variedades complementarias con el núcleo de φ en L demuestra que $\overline{\varphi}$ es un endomorfismo suprayectivo y por lo tanto un isomorfismo. De acuerdo con la proposición anterior, $L/\ker \varphi = \overline{L}_1 \oplus \overline{L}_2 \ldots \overline{L}_r$, en que $\overline{L}_i = \{v_i + \ker \varphi, \varphi v_i + \ker \varphi, \ldots, \varphi^{n_i-1} v_i + \ker \varphi\}$, $a(v_i + \ker \varphi) = a(\overline{L}_i) = f_i(X)$, en que los polinomios $f_i(X)$ no son múltiplos de X, pues $\overline{\varphi}$ es un isomorfismo. Veamos que se puede tomar v_i, de modo que $a(v_i) = f_i(X)$; $f_i(\varphi)(v_i + \ker \varphi) = 0$, lo que implica que $f_i(\varphi)\, v_i \in \ker \varphi$, es decir, $\varphi f_i(\varphi)\, v_i = f_i(\varphi)\, \varphi v_i = 0$, y entonces, $\{\varphi v_i + \ker \varphi, \ldots, \varphi^{r_i} v_i + \ker \varphi\}$ es una base de L_i, puesto que $\overline{\varphi}$ es un isomorfismo y que L_i es invariante y bastará tomar φv_i en lugar de v_i. En estas condiciones, si tomamos, $L' = \{v_1, \varphi v_1, \ldots, \varphi^{n_1} v_1, v_2 \ldots, \varphi^{n_r} v_r\}$, y $\{n_1, \ldots, n_s\}$ es una base de $\ker \varphi$, $\{n_1, \ldots, n_s, v_1, \varphi v_1, \ldots, \varphi^{n_1} v_1, \ldots, \varphi^{n_1-1} v_1, v_2, \ldots, \varphi^{n_r} v_r\}$ es un sistema de generadores de L y como, $\dim L = \dim = \ker \varphi + \Sigma \dim L_i = s + \Sigma n_i$, el conjunto anterior es una base y $L = \ker \oplus L'$, en que L' es invariante, de acuerdo con la elección de v_i.

Proposición 8.—Si $\varphi : V \rightarrow V$ es un endomorfismo, se puede encontrar una descomposición del tipo, $V = L_1 \oplus L_2 \ldots L_r \oplus \ker \varphi$, unos polinomios, $f_i(X)$ y unos elementos, $v_i \in L_i$, tales que,

i) L_i es una variedad invariante.

ii) $a(v_i) = a(L_i) = f_i(X)$.

iii) $\{ v_i, \varphi v_i, \ldots, \varphi^{n_i-1} v_i\}$ es una base de L_i, siendo n_i el grado de $f_i(X)$.

iv) $f_i(X)$ es múltiplo de $f_{i+1}(X)$.

En efecto:

Esta proposición es consecuencia inmediata de las proposiciones 6 y 7.

Proposición 9.—Los polinomios f_i (X) a que hace referencia la proposición anterior son únicos.

En efecto:

Para ello demostraremos que si A es la matriz que determina las ecuaciones de un automorfismo respecto a una base, y llamamos Δ_i al máximo común divisor de los menores de orden i de la matriz A — IX (siendo I la matriz unidad), $f_i = \Delta_{n-i}/\Delta_{n-i-1}$, siendo n la dimensión de V. Como el cambio de base no altera este máximo común divisor, puesto que, $TAT^{-1} = T(A - IX)T^{-1}$, lo que implica que los menores de orden i de una de las dos matrices son combinaciones lineales de los menores de la otra matriz, vamos a calcular estos Δ_i en un caso concreto. Si tomamos como base de V la indicada en el apartado *iii)* de la proposición 8, es inmediato comprobar que la matriz que determina el homomorfismo es la matriz.

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_1 & & & \\ & \mathbf{A}_2 & & \\ & & \cdot & \\ & & & \cdot \\ & & & & \mathbf{A}_r \end{pmatrix}$$

siendo,

$$\mathbf{A}_i = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & 1 \\ -a_{i0} & -a_{i1} & -a_{i2} & \cdots & -a_{in_i-1} \end{pmatrix}$$

En este caso la matriz A — IX toma la forma

$$\mathbf{A} - \mathrm{IX} = \begin{pmatrix} \mathbf{A}_1 - \mathrm{IX} & & & \\ & \mathbf{A}_2 - \mathrm{IX} & & \\ & & \cdot & \\ & & & \mathbf{A}_r - \mathrm{IX} \end{pmatrix}$$

Mediante cambios que no influyen más que en el signo de los menores (cambio de filas o de columnas, o sumar a una fila o columna una combinación lineal de las otras) vamos a transformar las matrices $\mathbf{A}_i$ — IX; sustituyendo la primera columna por el resultado de sumarle la segunda multiplicada por X, la tercera por X^2, etc., obtenemos una matriz de la forma

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & -X & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & 1 \\ -f_i(X) & -a_{i1} & -a_{i2} & \cdots & -X-a_{in_i-1} \end{pmatrix}$$

aplicando un procedimiento recurrente de restar a todas las filas (excepto la última) la anterior multiplicada por — X obtenemos

$$\begin{pmatrix} 0 & 1 & 0 & . & . & . & 0 \\ 0 & 0 & 1 & . & . & . & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & 1 \\ -f_i(X) & -a_{i1} & -a_{i2} & . & . & . & -x-a_{in_i-1} \end{pmatrix}$$

y sumando a la última fila la primera multiplicada por a_{i1}, la segunda multiplicada por a_{i2}, etc..., llegamos a la matriz

$$\begin{pmatrix} 0 & 1 & 0 & . & . & . & 0 \\ 0 & 0 & 1 & . & . & . & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & 1 \\ -f_i(X) & 0 & 0 & . & . & . & 0 \end{pmatrix}$$

y cambiando entre sí las columnas llegamos a

$$\begin{pmatrix} 1 & 0 & 0 & . & . & . & 0 \\ 0 & 1 & 0 & . & . & . & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & 0 \\ 0 & 0 & 0 & . & . & . & fi(X) \end{pmatrix}$$

De aquí se deduce que mediante cambios de este tipo podemos pasar de la matriz A — IX a la matriz

$$\begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & \cdot & & & & & \\ & & & \cdot & & & & \\ & & & & f_1(X) & & & \\ & & & & & 1 & & \\ & & & & & & \cdot & \\ & & & & & & & f_r(X) \end{pmatrix}$$

en la que es inmediato comprobar que $f_i(X) = \Delta_{n-i}/\Delta_{n-i-1}$.

En el caso general en que φ es un homomorfismo, basta considerar que si $L = \ker \varphi \oplus L_1 \oplus L_2 \ldots L_r$, y llamamos $\overline{\varphi}$ al automorfismo definido en la demostración de la proposición 7, y f es la aplicación natural de L en L/ker φ, L/ker $\varphi = f(L_1) \oplus f(L_2) \ldots f(L_r)$, en que por la relación de las dimensiones de L y L/ker φ debe ser a $f(L_i) = f_i(X)$, y podemos aplicar los resultados anteriores.

Proposición 10.—Si $\varphi, \varphi' : V \to V$, son endomorfismo, la condición necesaria y suficiente para que exista un automorfismo, a, tal que, $\varphi' = a^{-1}\varphi\, a$, es que φ y φ' posean los mismos factores invariantes.

En efecto:

La condición es suficiente. Basta que tomemos unas bases, $\{\varphi^k v_i,\ n_i\}$

y $\{\varphi'\ {}^k v_i', n_i'\}$ de acuerdo con la proposición 8 y tomemos el automorfismo, a, definido por $a\ (\varphi'\ {}^k v_i') = \varphi\ {}^k v_i$, $a(n'_i) = n_i$.

La condición es necesaria. Pues si φ o φ' es un automorfismo, deben serlo ambos y respecto a las ecuaciones matriciales tomadas con referencia a una base, la relación $\varphi' = a^{-1}\ \varphi a$, implica una relación del tipo $A' = T^{-1}\ AT$, siendo A y A' las matrices que determinan los homomorfismos, lo que implica, de acuerdo con la demostración de la proposición 9, la igualdad de los polinomios f_i (X). En el caso de ser φ y φ' homomorfismos no inyectivos, ker φ = ker φ', y si V = ker $\varphi \oplus L'$, $\varphi'\ L' = L'$, tenemos que $\varphi\ aL' = a\ \varphi'\ L' = aL'$, lo que quiere decir que la descomposición de L' y de aL' son del mismo tipo [respecto a los polinomios f_i(X)], lo que implica su igualdad.

(R - 12 - XII - 66)