Notas sintéticas para un curso de Algebra Lineal y Geometría-II

Felipe Cano, Beatriz Molina y Fernando Sanz

2017-18 Universidad de Valladolid

October 4, 2018

CHAPTER 1

Clasificación de endomorfismos de espacios vectoriales

En este capítulo abordaremos el teorema de Jordan de clasificación de endomorfismos de espacios vectoriales de dimensión finita, desde la óptica de los módulos de tipo finito sobre dominios de ideales principales.

1. Dominios de ideales principales. Repaso

Recordamos que un *anillo conmutativo con unidad* $\mathcal{A}$ es una terna $\mathcal{A} = (A, s, p)$ donde A es un conjunto, que denominaremos el *conjunto soporte* o *conjunto subyacente de* $\mathcal{A}$; los símbolos s y p denotan las operaciones suma y producto respectivamente

$$s : A \times A \to A; \quad p : A \times A \to A,$$

para las cuales utilizaremos la notación habitual: $s(a, b) = a + b$ y $p(a, b) = ab$. Además, deben cumplirse las siguientes propiedades:

(1) (A, s) es un grupo abeliano. Es decir, la suma es conmutativa, asociativa, existe elemento neutro, que denotamos 0 y todo elemento tiene su opuesto.
(2) El producto $p : (a, b) \mapsto ab$ es conmutativo, asociativo, existe unidad, que denotamos 1, con $1 \neq 0$ y, finalmente, hay distributividad respecto de la suma:
$$a(b + c) = ab + ac.$$

En particular, se tiene que $a0 = 0$ y que $(-1)a = -a$ para todo $a \in A$.

Diremos que un anillo $\mathcal{A}$ es un *dominio de integridad*, o simplemente un *dominio*, si se tiene:

"Para todos $a, b \in A$; si $ab = 0$ y $a \neq 0$, entonces $b = 0$".

Si $\mathcal{A}$ es un dominio entonces se tiene la ley de cancelación:

"Para todos $a, b, c \in A$; si $a \neq 0$ y $ab = ac$, entonces $b = c$".

Diremos que un subconjunto $I \subset A$ es un *ideal de* $\mathcal{A}$, si se cumplen las siguientes propiedades:

(1) $s(I \times I) \subset I$ y la aplicación $\bar{s} : I \times I \to I$, obtenida por restricción de s, hace de $(I, \bar{s})$ un grupo abeliano.
(2) $p(A \times I) \subset I$.

Dos ejemplos de ideales (llamados *ideales triviales*) son el ideal cero $\{0\}$ y el ideal unidad o total A.

La intersección de cualquier familia de ideales es un ideal. Dado un subconjunto $S \subset A$, el *ideal generado por* S, que denotaremos habitualmente por (S), es por definición la intersección de todos los ideales que contienen S. Cuando el conjunto S es unipuntual, $S = \{s\}$, denotaremos para simplificar $(s) = (\{s\})$; en particular, el ideal cero será denotado por (0).

PROPOSICIÓN 1. *Dado $S \subset A$, el ideal (S) generado por S es el conjunto de las combinaciones lineales finitas con coeficientes en A de elementos de S, es decir, los elementos $b \in A$ de la forma:*

$$b = a_1 s_1 + a_2 s_2 + \cdots + a_n s_n,$$

donde $n \in \mathbb{Z}_{\geq 0}$, $a_i \in A$, $s_i \in S$, para $i = 1, 2, \ldots, n$.

Demostración: Las combinaciones lineales finitas consideradas están necesariamente en cualquier ideal que contenga S, por tanto en la intersección de todos ellos. Por otro lado, el conjunto de todas las combinaciones lineales finitas de elementos de S, constituye un ideal (dejamos la comprobación al lector). CQD.

Decimos que un ideal I de $\mathcal{A}$ es *principal*, si existe un elemento $s \in A$ tal que $I = (s)$; es decir, si está generado por uno de sus elementos. Nótese que:

$$(s) = As = \{as; a \in A\}.$$

Diremos que un anillo $\mathcal{A}$ es un *dominio de ideales principales*, si es un dominio y todos sus ideales son principales. Frecuentemente nos referiremos a ellos con las siglas DIP.

Dos ejemplos importantes de DIP son el anillo $\mathbb{Z}$ de los números enteros y el anillo $k[X]$ de polinomios en una variable X con coeficientes en un cuerpo k dado.

2. Divisibilidad en dominios de ideales principales

Sea $\mathcal{A} = (A, s, p)$ un anillo conmutativo con unidad y $\mathfrak{p} \subset A$ un ideal, con $\mathfrak{p} \neq A$. Decimos que $\mathfrak{p}$ es un *ideal primo* si y sólo si se cumple la siguiente propiedad:

"Dados $f, g \in A$ con $fg \in \mathfrak{p}$ y $f \notin \mathfrak{p}$, se tiene que $g \in \mathfrak{p}$."

Nótese que $\mathcal{A}$ es un dominio si y sólo si el ideal (0) es un ideal primo.

Dados dos elementos $f, g \in A$, decimos que f *divide* g si y sólo si existe $h \in A$ tal que $g = hf$. Esto equivale a decir que $g \in (f)$.

PROPOSICIÓN 2. *Si $\mathfrak{p} = (p)$ es un ideal principal de $\mathcal{A}$, con $\mathfrak{p} \neq A$, son equivalentes:*

1. *El ideal $\mathfrak{p}$ es primo.*
2. *Dados dos elementos $f, g \in A$; si p divide fg y no f, entonces divide g.*

Demostración: Basta observar que, dado $h \in A$, se tiene que $h \in (p)$ si y sólo si p divide h. CQD.

Se dice que $p \in A$ es un *elemento primo* si y sólo si $p \neq 0$ y el ideal (p) es primo.

Se dice que $u \in A$ es una *unidad de* $\mathcal{A}$ si y sólo si $(u) = A$. Esto es equivalente a decir que $1 \in (u)$, o equivalentemente que existe $u' \in A$ tal que $u'u = 1$. Nótese que las unidades no son elementos primos.

Dos elementos $f, g \in A$ *están asociados* si y sólo si existe una unidad u con $g = uf$.

Dados dos elementos $f, g \in A$, un *máximo común divisor* de f, g es cualquier elemento $d \in A$ que divide f y g y tal que si $d' \in A$ divide f y g, entonces d' divide d. Si $\mathcal{A}$ es un dominio, dos máximos comunes divisores de f, g están siempre asociados.

Si $\mathcal{A}$ es un DIP y $f, g \in A$, cualquier generador del ideal $(\{f, g\})$ es un máximo común divisor de f, g. En particular, tenemos la *identidad de Bézout*: si d es un máximo común divisor de f, g, existen $a, b \in A$ tales que

$$d = af + bg.$$

La identidad de Bézout no es necesariamente cierta para un dominio que no sea un DIP.

Dos elementos $f, g \in A$ son *primos entre sí* si no existe ningún divisor común $d \in A$ de f y g que no sea una unidad. Equivalentemente, si 1 es un máximo común divisor de f, g.

Se dice que $f \in A$ es *irreducible* si y sólo si f no es una unidad y para toda descomposición $f = gh$ donde g no es una unidad, se tiene que h es una unidad.

PROPOSICIÓN 3. *Todo elemento primo de un dominio es irreducible.*

Demostración: Sea $p \in A$ un elemento primo y supongamos que $p = gh$. Hay que probar que o bien g es una unidad, o bien h es una unidad. Nótese que p divide gh; por tanto, como p es primo, tenemos que p divide g o p divide h. Si p divide g, existe $u \in A$ tal que $g = up$ y por consiguiente $p = uhp$, en particular $(1-uh)p = 0$. Como $\mathcal{A}$ es un dominio y $p \neq 0$, se tiene que $1 = uh$ y por tanto h es una unidad. Del mismo modo, si p divide h se concluye que g es una unidad.

CQD.

Se dice que el anillo $\mathcal{A}$ es un *dominio de factorización única*, para lo que utilizaremos las siglas DFU, si y sólo si es un dominio y para cada elemento $f \in A$, con $f \neq 0$, se tienen las siguientes dos propiedades:

- Existe una *descomposición de f en factores irreducibles* de la forma
$$f = u_0 f_1 f_2 \cdots f_n,$$
donde $n \in \mathbb{Z}_{\geq 0}$, el elemento $u_0 \in A$ es una unidad y los elementos $f_1, f_2, \ldots, f_n \in A$ son irreducibles.
- Dadas dos descomposiciones en factores irreducibles
$$f = u_0 f_1 f_2 \cdots f_n, \quad f = u'_0 f'_1 f'_2 \cdots f'_{n'},$$
se tiene que $n = n'$ y existe una permutación $\sigma \in S_n$ tal que $f_{\sigma(i)}$ y f'_i están asociados, para todo $i = 1, 2, \ldots, n$.

Si $\mathcal{A}$ es un DFU todo elemento $f \neq 0$ se puede descomponer de la forma

$$f = u p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n},$$

donde $u \in A$ es una unidad, cada p_i es irreducible y p_i no está asociado con p_j si $i \neq j$. Basta agrupar los elementos asociados en la descomposición de f en factores irreducibles.

PROPOSICIÓN 4. *En un DFU todo elemento irreducible es primo.*

Demostración: Sea $\mathcal{A}$ un DFU y consideremos un elemento irreducible $p \in A$. Queremos probar que el ideal (p) es primo. Como p no es una unidad, tenemos que $(p) \neq A$. Supongamos que p divide fg y no divide g. Esto quiere decir que p aparece en la descomposición en factores irreducibles de fg, pero no en la de g, por consiguiente aparece en la de f y así divide f. CQD.

Ejemplo 1. Un DFU no necesariamente es DIP. Por ejemplo, el anillo de polinomios en dos variables $k[X,Y]$ con coeficientes en un cuerpo k es un DFU, que no es un DIP. De hecho, se sabe que todo anillo de polinomios en una variable con coeficientes en un DFU, es un DFU. A continuación veremos que, sin embargo, todo DIP es un DFU.

Proposición 5. *Sea $\mathcal{A}$ un DIP y $f \in A \setminus \{0\}$. Existe una descomposición de f en factores irreducibles del tipo*

$$f = u_0 f_1 f_2 \cdots f_n, \quad n \in \mathbb{Z}_{\geq 0},$$

donde u_0 es una unidad y cada f_i es irreducible para $1 \leq i \leq n$.

Demostración: Razonemos por reducción al absurdo, suponiendo que existe $f \neq 0$ que no admite una descomposición en factores irreducibles. Entonces f no es irreducible, pues si lo fuera tendríamos $f = 1 \cdot f$ y sería una descomposición en factores irreducibles. Se concluye que hay una descomposición $f = g_1 h_1$, donde ni g_1 ni h_1 son unidades. Tampoco puede ocurrir que g_1 y h_1 admitan una descomposición en factores irreducibles ambos, pues generaríamos una de f. Uno de ellos, digamos g_1, no admite una descomposición en factores irreducibles. Repitiendo el razonamiento, encontramos que $g_1 = g_2 h_2$ donde h_2 no es una unidad y g_2 no admite una descomposición en factores irreducibles.

De este modo tenemos una sucesión de parejas $\{(g_n, h_n)\}_{n\geq 1}$, con $g_n \neq 0$, $h_n \neq 0$, de modo que cada h_n no es una unidad y se tiene

$$g_n = g_{n+1} h_{n+1}, \quad \text{para todo } n \geq 1.$$

En particular, tenemos inclusiones estrictas de ideales

$$(g_n) \subsetneq (g_{n+1})$$

para cada $n \geq 1$. En efecto, la inclusión $(g_n) \subset (g_{n+1})$ está dada por el hecho de que $g_n = g_{n+1} h_{n+1}$ y por consiguiente $g_n \in (g_{n+1})$. Por otro lado, $(g_n) \neq (g_{n+1})$, en efecto, si $g_{n+1} \in (g_n)$ tendríamos que $g_{n+1} = a g_n$ y por tanto $g_{n+1} = a h_{n+1} g_{n+1}$, es decir $(1 - a h_{n+1}) g_{n+1} = 0$, como $\mathcal{A}$ es un dominio, se tendría que $1 - a h_{n+1} = 0$ dado que $g_{n+1} \neq 0$, es decir que $1 = a h_{n+1}$ y por tanto h_{n+1} sería una unidad, que suponemos no ocurre. Así pues $g_{n+1} \notin (g_n)$, lo que prueba que $(g_n) \neq (g_{n+1})$.

Consideremos ahora el ideal $I \subset A$ generado por el conjunto de los elementos g_n, con $n \geq 1$. Como cada $g_n \neq 0$ se tiene que $I \neq (0)$. La hipótesis de que $\mathcal{A}$ es un DIP, nos dice que $I = (s)$, con $s \neq 0$. Por un lado $s \in I$, esto quiere decir que existe una combinación lineal finita

$$s = a_1 g_1 + a_2 g_2 + \cdots + a_N g_N.$$

Por otro lado $g_{N+1} \in (s)$ y entonces $g_{N+1} = bs$. Recordemos que para cada $1 \leq n \leq N$ se tiene $g_n \in (g_N)$, esto es, $g_n = b_n g_N$ para algún $b_n \in A$. Finalmente obtenemos que

$$g_{N+1} = bs = b(a_1 b_1 + a_2 b_2 + \cdots + a_N b_n) g_N.$$

Esta igualdad implica que $g_{N+1} \in (g_N)$. Es la contradicción buscada. CQD.

Proposición 6. *Sean $\mathcal{A}$ un DIP y dos elementos no nulos $f, g \in A$. Son equivalentes:*

1. *Los elementos f y g son primos entre sí.*
2. *No existe ningún divisor común irreducible de f y g.*

(3) *El ideal generado por* $\{f, g\}$ *es el total.*
(4) *Existen* $a, b \in A$ *tales que* $af + bg = 1$. (Identidad de Bézout).

Demostración: Los enunciados (3) y (4) son equivalentes por definición. Veamos la equivalencia de los demás mediante una lista circular de implicaciones:

(1) $\Rightarrow$ (2) Evidente, ya que un irreducible no es una unidad por definición.
(2) $\Rightarrow$ (3) Escribamos $(\{f, g\}) = (a)$, si a es una unidad entonces $(a) = (1)$. Si a no es una unidad, cualquier irreducible de una descomposición en factores irreducibles de a es un divisor común irreducible de f y de g.
(3) $\Rightarrow$ (1) Si f y g no son primos entre sí, existe una no unidad h tal que $f, g \in (h)$. Entonces $(\{f, g\}) \subset (h) \subsetneq (1)$ y por tanto $(\{f, g\}) \neq (1)$.

CQD.

Corolario 1. *En un DIP todo elemento irreducible es primo.*

Demostración: Sea $\mathcal{A}$ un DIP y consideremos un elemento irreducible $p \in A$. Queremos probar que el ideal (p) es primo. Supongamos que p divide fg y no divide g. Como p no divide g y los únicos divisores de p son los irreducibles asociados con p, se sigue que p y g son primos entre sí. Así pues existen $a, b \in A$ tales que $1 = ap + bg$. Escribamos $fg = hp$, tenemos

$$f = (ap + bg)f = apf + bfg = afp + bhp = (af + bh)p.$$

Se sigue que p divide f. CQD.

Corolario 2. *Todo DIP es un DFU.*

Demostración: Solo falta comprobar la unicidad de las descomposiciones en factores irreducibles de elementos no nulos. Sea $\mathcal{A}$ un DIP y consideremos dos descomposiciones de un elemento $f \neq 0$ en factores irreducibles

$$f = u_0 f_1 f_2 \cdots f_n = u'_0 f'_1 f'_2 \cdots f'_{n'}, \quad n \leq n'.$$

Si $n = 0$ entonces $f = u_0$ es una unidad y por tanto $n' = 0$. Supongamos que $n \geq 1$. Como f_1 es irreducible, es primo y entonces divide alguno de los f'_j. Salvo reordenación, podemos suponer que f_1 divide f'_1 y por consiguiente están asociados, ya que f'_1 es irreducible. Salvo multiplicar por una unidad, podemos suponer que $f_1 = f'_1$. Escribiendo $f = f_1 g$, tenemos que

$$g = u_0 f_2 f_3 \cdots f_n = u'_0 f'_2 f'_3 \cdots f'_{n'}$$

y procedemos por inducción finita sobre n. CQD.

3. Módulos sobre un anillo

Sea $\mathcal{A} = (A, s, p)$ un anillo conmutativo con unidad. Un *módulo* $\mathcal{M}$ *sobre* $\mathcal{A}$ es una terna $\mathcal{M} = (M, \sigma, \pi)$ donde M es un conjunto no vacío y σ, π son aplicaciones

$$\sigma : M \times M \to M, \quad \pi : A \times M \to M$$

que denotaremos $\sigma(m, n) = m + n$ y $\pi(a, m) = am$ si no hay confusión. Pedimos que (M, σ) sea un grupo abeliano, que el producto $(a, m) \mapsto am$ sea distributivo respecto de la suma en $\mathcal{A}$ y en $\mathcal{M}$, es decir:

(a) para todos $a, b \in A$, $m \in M$, se tiene $(a + b)m = am + bm$,

(b) para todos $a \in A$, $m, n \in M$, se tiene $a(m+n) = am + an$;

que sea asociativo respecto del producto en $\mathcal{A}$:

(c) para todos $a, b \in A$, $m \in M$, se tiene $(ab)m = a(bm)$

y además se tenga:

(d) para todo $m \in M$, se tiene $1m = m$ y $0m = 0$,

(e) para todo $a \in A$, se tiene $a0 = 0$.

El conjunto M se llama *conjunto soporte* o *conjunto subyacente* al módulo $\mathcal{M}$. También se dice que $\mathcal{M}$ es una *estructura de $\mathcal{A}$-módulo sobre M*.

Tenemos los siguientes ejemplos básicos:

- Todo grupo abeliano es un $\mathbb{Z}$-módulo de forma natural.
- Todo ideal I de $\mathcal{A}$ admite una estructura natural de $\mathcal{A}$-módulo.
- En el caso de que $\mathcal{A}$ sea un cuerpo k, un k-módulo es lo mismo que un k-espacio vectorial.

Dado un $\mathcal{A}$-módulo $\mathcal{M} = (M, \sigma, \pi)$, decimos que un subconjunto $N \subset M$ *soporta un submódulo de $\mathcal{M}$* si soporta un subgrupo abeliano y es invariante para el producto, es decir $\pi(A \times N) \subset N$. En este caso tenemos un $\mathcal{A}$-módulo $\mathcal{N} = (N, \bar{\sigma}, \bar{\pi})$ dado por:

$$\bar{\sigma}(m, n) = \sigma(m, n),\ \bar{\pi}(a, m) = \pi(a, m),$$

que llamaremos *el submódulo de $\mathcal{M}$ soportado por N*. En adelante, si no hay confusión, identificaremos cada submódulo de $\mathcal{M}$ con su conjunto soporte, dado que la estructura inducida de $\mathcal{A}$-módulo sobre un subconjunto de M que soporte un submódulo es única.

La intersección de cualquier familia de submódulos es también un submódulo. Así, dado un subconjunto cualquiera B de M definiremos el *submódulo $< B >$ generado por B* como la intersección de todos los submódulos que contienen B.

Proposición 7. *Dado $B \subset M$, el submódulo $< B >$ de $\mathcal{M}$ generado por B es el conjunto de combinaciones lineales finitas*

$$a_1 m_1 + a_2 m_2 + \cdots + a_n m_n,$$

donde $n \in \mathbb{Z}_{\geq 0}$ los $a_i \in A$ y los $m_i \in B$, para $i = 1, 2, \ldots, n$.

Demostración: Es la misma "mutatis mutandis" que la del caso de ideales en la proposición 1. CQD.

Sean N_1 y N_2 dos subconjuntos de M. Definimos el conjunto $N_1 + N_2$ como

$$N_1 + N_2 = \{n \in M;\ n = n_1 + n_2,\ n_1 \in N_1,\ n_2 \in N_2\}.$$

Proposición 8. *Si N_1 y N_2 son submódulos de $\mathcal{M}$, se tiene*

$$< N_1 \cup N_2 >= N_1 + N_2.$$

Demostración: Basta observar que $N_1 + N_2$ es un submódulo que contiene N_1 y N_2 y además está contenido en cualquier submódulo que contenga N_1 y N_2. CQD.

Proposición 9. *Dados N_1 y N_2 submódulos de $\mathcal{M}$, se tiene que $N_1 \cap N_2 = \{0\}$ si y sólo si, dados $n_1, n_1' \in N_1$, $n_2, n_2' \in N_2$ con*

$$n_1 + n_2 = n_1' + n_2',$$

entonces $n_1 = n_1'$ y $n_2 = n_2'$.

Demostración: Basta observar que $n_1 - n_1' = n_2' - n_2 \in N_1 \cap N_2$. CQD.

Se dice que $N_1 + N_2$ es *suma directa interna* de los sumódulos N_1 y N_2 si y sólo si $N_1 \cap N_2 = \{0\}$. Lo escribimos $N_1 + N_2 = N_1 \oplus N_2$.

De manera más general, si tenemos una lista finita $N_1, N_2, \ldots, N_n$ de submódulos de $\mathcal{M}$, vemos que

$$< N_1 \cup N_2 \cup \cdots \cup N_n >= N_1 + N_2 + \cdots + N_n.$$

Por inducción diremos que $N_1 + N_2 + \cdots + N_n$ es suma directa interna de la lista anterior y lo escribiremos:

$$N_1 + N_2 + \cdots + N_n = N_1 \oplus N_2 \oplus \cdots \oplus N_n,$$

si se tiene $N_1 + N_2 + \cdots + N_{n-1} = N_1 \oplus N_2 \oplus \cdots \oplus N_{n-1}$ y además:

$$(N_1 + N_2 + \cdots + N_{n-1}) + N_n = (N_1 \oplus N_2 \oplus \cdots \oplus N_{n-1}) \oplus N_n.$$

Un caso particularmente interesante se da cuando tenemos

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_n,$$

en este caso todo $m \in M$ admite una expresión única

$$m = m_1 + m_2 + \cdots + m_n; \quad m_i \in N_i,\ i = 1, 2, \ldots, n.$$

3.1. Homomorfismos de módulos sobre un anillo. Dados dos módulos $\mathcal{M}_1 = (M_1, \sigma_1, \pi_1)$ y $\mathcal{M}_2 = (M_2, \sigma_2, \pi_2)$ sobre un anillo $\mathcal{A}$, llamamos *homomorfismo de $\mathcal{A}$-módulos de $\mathcal{M}_1$ en $\mathcal{M}_2$* a toda aplicación de conjuntos $\phi : M_1 \to M_2$ que es un homomorfismo de grupos abelianos y además cumple

$$\phi(am) = a\phi(m), \quad m \in M_1,\ a \in A.$$

Nótese que am denota el producto π_1 en $\mathcal{M}_1$ y $a\phi(m)$ se refiere al producto π_2 en $\mathcal{M}_2$.

Denotaremos por $\mathrm{Hom}_{\mathcal{A}}(\mathcal{M}_1, \mathcal{M}_2)$ el conjunto de los homomorfismos de $\mathcal{A}$-módulos de $\mathcal{M}_1$ en $\mathcal{M}_2$. El primer ejemplo es la identidad $\mathrm{id}_M \in \mathrm{Hom}_{\mathcal{A}}(\mathcal{M}, \mathcal{M})$. Dados tres $\mathcal{A}$-módulos $\mathcal{M}_1$, $\mathcal{M}_2$ y $\mathcal{M}_3$ la composición de aplicaciones permite construir una aplicación bien definida

$$\mathrm{Hom}_{\mathcal{A}}(\mathcal{M}_1, \mathcal{M}_2) \times \mathrm{Hom}_{\mathcal{A}}(\mathcal{M}_2, \mathcal{M}_3) \to \mathrm{Hom}_{\mathcal{A}}(\mathcal{M}_1, \mathcal{M}_3)$$

dada por $(\phi, \psi) \mapsto \psi \circ \phi$.

Diremos que $\phi \in \mathrm{Hom}_{\mathcal{A}}(\mathcal{M}_1, \mathcal{M}_2)$ es un *isomorfismo de $\mathcal{A}$-módulos* si existe $\psi \in \mathrm{Hom}_{\mathcal{A}}(\mathcal{M}_2, \mathcal{M}_1)$ tal que $\psi \circ \phi = \mathrm{id}_{M_1}$ y $\phi \circ \psi = \mathrm{id}_{M_2}$. Denotaremos por $\mathrm{Isom}_{\mathcal{A}}(\mathcal{M}_1, \mathcal{M}_2)$ el conjunto de isomorfismos de $\mathcal{M}_1$ en $\mathcal{M}_2$.

Ejercicio 1. Todo homomorfismo biyectivo entre $\mathcal{A}$-módulos es un isomorfismo y recíprocamente, todo isomorfismo de $\mathcal{A}$-módulos es biyectivo.

Ejercicio 2. Dados dos $\mathcal{A}$-módulos $\mathcal{M}_1$ y $\mathcal{M}_2$ con el mismo conjunto subyacente M, la aplicación identidad $id_M : M \to M$ no necesariamente es un homomorfismo de $\mathcal{M}_1$ en $\mathcal{M}_2$. Por ejemplo, consideremos $M = \{m_1, m_2, m_3, m_4\}$ un conjunto de cuatro elementos y dos biyecciones

$$\varphi_1 : M \to \mathbb{Z}/(2) \times \mathbb{Z}/(2), \quad \varphi_2 : M \to \mathbb{Z}/(4).$$

Dotamos ahora M de dos estructuras distintas $\mathcal{M}_1$ y $\mathcal{M}_2$ de grupo abeliano (o $\mathbb{Z}$-módulo) a través de las biyecciones φ_1 y φ_2, es decir

$$\sigma_i(m_j, m_k) = \varphi_i^{-1}(\varphi_i(m_j) + \varphi_i(m_k)), \quad i = 1, 2.$$

En este ejemplo, la identidad $id_M \notin \mathrm{Hom}_{\mathbb{Z}}(\mathcal{M}_1, \mathcal{M}_2)$.

El *núcleo* $\mathrm{Ker}\phi$ *de un homomorfismo* $\phi : M \to M'$ entre dos $\mathcal{A}$-módulos $\mathcal{M}$ y $\mathcal{M}'$ se define por

$$\mathrm{Ker}\phi = \{m \in M;\ \phi(m) = 0\}.$$

Es un submódulo de $\mathcal{M}$ y se cumple que $\mathrm{Ker}\ \phi = \{0\}$ si y sólo si ϕ es inyectivo.

Más generalmente, si $N' \subset M'$ es un submódulo de $\mathcal{M}'$, entonces $\phi^{-1}(N')$ es un submódulo de $\mathcal{M}$.

Asimismo, la *imagen* $\mathrm{Im}\phi$ de ϕ se define por

$$\mathrm{Im}\phi = \{m' \in M';\ \text{ existe } m \in M \text{ tal que } \phi(m) = m'\}.$$

Es un submódulo de $\mathcal{M}'$ y se cumple que $\mathrm{Im}\ \phi = M'$ si y sólo si ϕ es suprayectivo.

Los elementos de $\mathrm{Hom}_{\mathcal{A}}(\mathcal{M}, \mathcal{M})$ reciben el nombre de *endomorfismos* de $\mathcal{M}$. Denotaremos por $\mathrm{End}_{\mathcal{A}}(\mathcal{M})$ el conjunto de endomorfismos de $\mathcal{M}$, esto es

$$\mathrm{End}_{\mathcal{A}}(\mathcal{M}) = \mathrm{Hom}_{\mathcal{A}}(\mathcal{M}, \mathcal{M}).$$

Aquellos que son isomorfismos se llaman *automorfismos* de $\mathcal{M}$. Asimismo denotaremos por $\mathrm{Aut}_{\mathcal{A}}(\mathcal{M})$ los automorfismos de $\mathcal{M}$.

La composición de aplicaciones es una operación interna en $\mathrm{End}_{\mathcal{A}}(\mathcal{M})$ y con esta operación $\mathrm{Aut}_{\mathcal{A}}(\mathcal{M})$ es un grupo.

Ejercicio 3. El grupo $\mathrm{Aut}_{\mathcal{A}}(\mathcal{M})$ no es necesariamente abeliano.

Un ejemplo interesante de endomorfismo de un módulo $\mathcal{M}$ es el endomorfismo $\phi_a^{\mathcal{M}} : M \to M$ obtenido de la multiplicación por un elemento fijo $a \in A$ del anillo:

$$\phi_a^{\mathcal{M}}(m) = am.$$

Observemos que $\phi_1^{\mathcal{M}} = \mathrm{id}_M$, $\phi_a^{\mathcal{M}} \circ \phi_b^{\mathcal{M}} = \phi_{ab}^{\mathcal{M}} = \phi_b^{\mathcal{M}} \circ \phi_a^{\mathcal{M}}$. En particular, si a es una unidad entonces $\phi_a^{\mathcal{M}}$ es un automorfismo. Nos resultará interesante considerar los submódulos de la forma

$$\mathrm{Ker}(\phi_a^{\mathcal{M}}) = \{m \in M;\ am = 0\}.$$

4. Módulos de torsión sobre un DIP

Sea $\mathcal{M} = (M, \sigma, \pi)$ un módulo sobre un anillo $\mathcal{A}$ conmutativo con unidad. Dado un elemento $m \in M$, definimos el *anulador* $\mathrm{Ann}_{\mathcal{M}}(m)$ por

$$\mathrm{Ann}_{\mathcal{M}}(m) = \{a \in A;\ am = 0\}.$$

El anulador $\mathrm{Ann}_{\mathcal{M}}(m)$ es un ideal de $\mathcal{A}$. Diremos que el elemento $m \in M$ es *de torsión en* $\mathcal{M}$ si $\mathrm{Ann}_{\mathcal{M}}(m) \neq (0)$, es decir, si existe un elemento $a \neq 0$ del anillo $\mathcal{A}$ tal que $am = 0$. Si no hay lugar a confusión, omitiremos el subíndice, denotando simplemente $\mathrm{Ann}_{\mathcal{M}}(m) = \mathrm{Ann}(m)$.

Ejemplos 1. Si el anillo $\mathcal{A}$ es un cuerpo, y por consiguiente $\mathcal{M}$ es un espacio vectorial, el único elemento de torsión es el cero.

Si por ejemplo consideramos el $\mathbb{Z}$-módulo $\mathcal{M}$ dado por

$$M = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$$

con la suma definida por $(m, n) + (m', n') = (m + m', n + n')$, entonces todos sus elementos son de torsión y más concretamente tenemos

$$\mathrm{Ann}(1, 0) = (2);\ \mathrm{Ann}(0, 1) = (3);\ \mathrm{Ann}(1, 1) = (6).$$

PROPOSICIÓN 10. *Sea $\mathcal{A}$ un dominio de integridad y $\mathcal{M}$ un $\mathcal{A}$-módulo. El conjunto $\tau(\mathcal{M}) \subset M$ de los elementos de torsión de $\mathcal{M}$ es un submódulo de $\mathcal{M}$.*

Demostración: Tenemos que ver que dados dos elementos $m_1, m_2 \in \tau(\mathcal{M})$, se tiene que $m_1 - m_2 \in \tau(\mathcal{M})$ y también que dados $m \in \tau(\mathcal{M})$ y $b \in A$ se tiene que $bm \in \tau(\mathcal{M})$. Sabemos que existen $a_1, a_2 \in A$ no nulos tales que $a_1 m_1 = a_2 m_2 = 0$, como $\mathcal{A}$ es un dominio tenemos que $a_1 a_2 \neq 0$ y entonces la ecuación

$$a_1 a_2 (m_1 - m_2) = a_2(a_1 m_1) - a_1(a_2 m_2) = 0,$$

nos dice que $m_1 - m_2 \in \tau(\mathcal{M})$. Por otro lado, si tomamos $a \neq 0$ con $am = 0$ tenemos que $a(bm) = b(am) = 0$ y así $bm \in \tau(\mathcal{M})$. CQD.

Diremos que $\mathcal{M}$ es un *módulo de torsión* si $\tau(\mathcal{M}) = M$. El *anulador* $\mathrm{Ann}(\mathcal{M})$ del módulo $\mathcal{M}$ se define por

$$\mathrm{Ann}(\mathcal{M}) = \{a \in A;\ am = 0,\ \text{para todo } m \in M\}.$$

Se trata también de un ideal de $\mathcal{A}$.

Diremos que un $\mathcal{A}$-módulo $\mathcal{M}$ es *de tipo finito*, o también *finitamente generado*, si existe un subconjunto finito B del soporte M tal que $< B >= M$.

PROPOSICIÓN 11. *Supongamos que $\mathcal{A}$ es un dominio y que $\mathcal{M}$ es un $\mathcal{A}$-módulo de tipo finito. Son equivalentes*

1. *El módulo $\mathcal{M}$ es de torsión, esto es $\tau(\mathcal{M}) = M$.*
2. $\mathrm{Ann}(\mathcal{M}) \neq (0)$.

Demostración: Supongamos que $\mathcal{M}$ es de torsión y seleccionemos una lista finita $m_1, m_2, \ldots, m_n$ de generadores de $\mathcal{M}$. Para cada $i = 1, 2, \ldots, n$ tomemos $a_i \neq 0$ con $a_i m_i = 0$. Sea $a = a_1 a_2 \cdots a_n$. Como $\mathcal{A}$ es un dominio, tenemos que $a \neq 0$. Además $am = 0$ para todo $m \in M$, entonces $0 \neq a \in \mathrm{Ann}(\mathcal{M})$. Recíprocamente, con caracter general se tiene que $\mathrm{Ann}(\mathcal{M}) \subset \mathrm{Ann}(m)$ para todo $m \in M$ y por tanto todo elemento de $\mathcal{M}$ es de torsión cuando $\mathrm{Ann}(\mathcal{M}) \neq (0)$.
CQD.

Consideremos ahora el caso de DIP. El siguiente resultado se conoce como "segundo teorema de estructura para módulos de tipo finito sobre DIP".

TEOREMA 1. *Sea $\mathcal{A}$ un dominio de ideales principales y $\mathcal{M}$ un $\mathcal{A}$-módulo de tipo finito y de torsión. Supongamos que*

$$Ann\ (\mathcal{M}) = (fg),$$

donde f y g son primos entre sí y no son unidades. Entonces existen dos submódulos únicos N_g y N_f de $\mathcal{M}$ con las siguientes propiedades

1. *El módulo $\mathcal{M}$ es suma directa interna de N_g y N_f, esto es $M = N_g \oplus N_f$.*
2. *Ann $(N_g) = (g)$ y Ann $(N_f) = (f)$.*

Además, se tiene que $N_f = \mathrm{Ker}\phi_f^{\mathcal{M}}$ y $N_g = \mathrm{Ker}\phi_g^{\mathcal{M}}$.

Demostración: Nótese que $fg \neq 0$ dado que ni f ni g son unidades y son primos entre sí. Definamos

$$\begin{aligned} N_g &= \mathrm{Im}\ (\phi_f^{\mathcal{M}}) = \{n \in M;\ \text{ existe } m \in M \text{ con } n = fm\}, \\ N_f &= \mathrm{Im}\ (\phi_g^{\mathcal{M}}) = \{n \in M;\ \text{ existe } m \in M \text{ con } n = gm\}. \end{aligned}$$

Como f y g son primos entre sí y $\mathcal{A}$ es un DIP, se cumple la identidad de Bézout y se tienen $a, b \in A$ con $af + bg = 1$. En particular todo elemento $m \in M$ se escribe

$$m = 1m = (af + bg) = a(fm) + b(gm).$$

Esto prueba que $M = N_g + N_f$.

Veamos ahora que $N_g \cap N_g = \{0\}$ y por consiguiente se tiene la suma directa interna $M = N_g \oplus N_f$. Si $n \in N_g \cap N_f$ tenemos

$$n = fm_1 = gm_2.$$

Por tanto $n = 1n = (af + bg)n = afgm_2 + bgfm_1 = fg(am_2 + bm_1) = 0$, ya que Ann $(\mathcal{M}) = (fg)$.

De la definición de N_f y N_g y dado que $(fg) =$ Ann $(\mathcal{M})$ se concluye que $f \in$ Ann (N_f) y $g \in$ Ann (N_g). Sean $f', g' \in A$ tales que Ann $(N_f) = (f')$ y Ann $(N_g) = (g')$; obsérvese que $f'g' \neq 0$. Queremos ver que $f' \in (f)$ y $g' \in (g)$ con lo cual se tendrá que $(f) = (f')$ y $(g) = (g')$.

Escribamos $f = h_1 f'$ y $g = h_2 g'$. Por otro lado $f'g' \in$ Ann $(\mathcal{M})$, dado que $M = N_g + N_f$. Se sigue que $f'g' = hfg = hh_1h_2f'g'$ y por tanto h_1 y h_2 son unidades. Es decir $(f') = (f)$ y $(g') = (g)$.

Comprobemos la unicidad de N_f y N_g. Supongamos que se tienen N'_f y N'_g con las propiedades requeridas. Dado $m \in N'_f$, tenemos que $fm = 0$ y entonces

$$m = 1m = (af + bg)m = bgm \in \mathrm{Im}(\phi_g^{\mathcal{M}}) = N_f.$$

Por consiguiente $N'_f \subset N_f$ y también $N'_g \subset N_g$. Recíprocamente, todo elemento $m \in N_f$, se expresa en $M = N_g \oplus N_f = N'_g \oplus N'_f$ de forma única como

$$m = 0 + m = m'_g + m'_f.$$

Se concluye que $m'_g = m - m'_f \in N_f$, como $m'_g \in N'_g \subset N_g$ se tiene que

$$m'_g \in N_f \cap N_g = \{0\}$$

y por consiguiente $m'_g = 0$. Es decir $m = m'_f$ y por tanto $N_f = N'_f$. Del mismo modo $N'_g = N_g$.

Finalmente, probemos que $N_f = \mathrm{Ker}(\phi_f^{\mathcal{M}})$. Recordemos que

$$\mathrm{Ker}(\phi_f^{\mathcal{M}}) = \{m \in M; fm = 0\}.$$

Sabemos que $\mathrm{Ann}(N_f) = (f)$ y por tanto $N_f \subset \mathrm{Ker}(\phi_f^{\mathcal{M}})$. Recíprocamente, tomemos $m \in M$ tal que $fm = 0$. Escribamos $m = fm_1 + gm_2$ según la descomposición $M = N_g + N_f$ obtenida. Queremos probar que $fm_1 = 0$ y entonces $m = gm_2 \in N_f$. Como $fm = 0$, se tiene $f(fm_1 + gm_2) = 0$ y por tanto $f^2m_1 = 0$. Si $fm_1 \neq 0$, tenemos que $\mathrm{Ann}(fm_1) = (h)$ con h no unidad y además $f = h'h$, $g = h''h$, se concluye que h divide f y g, absurdo. Del mismo modo se tiene que $N_g = \mathrm{Ker}(\phi_g^{\mathcal{M}})$. CQD.

Corolario 3. *Sea $\mathcal{A}$ un dominio de ideales principales y $\mathcal{M}$ un $\mathcal{A}$-módulo de tipo finito y de torsión. Supongamos que*

$$Ann\ (\mathcal{M}) = (f_1 f_2 \dots f_t),$$

donde los f_i son dos a dos primos entre sí y no son unidades. Entonces existen submódulos únicos N_{f_i} de $\mathcal{M}$ con las siguientes propiedades

(1) *El módulo $\mathcal{M}$ es suma directa interna de los N_{f_i}, esto es*
$$M = N_{f_1} \oplus N_{f_2} \oplus \cdots \oplus N_{f_t}.$$
(2) *Ann $(N_{f_i}) = (f_i)$, para $i = 1, 2, \ldots, t$.*

Además, se tiene que $N_{f_i} = \mathrm{Ker}\phi_{f_i}^{\mathcal{M}}$, para $i = 1, 2, \ldots, t$.

Demostración: Si $t = 2$ es el teorema anterior. Hagamos inducción sobre t. Sabemos que
$$M = N_{f_1} \oplus N_{f_2 f_3 \cdots f_t}.$$
concluimos aplicando inducción a $N_{f_2 f_3 \cdots f_t}$. Se dejan los detalles como ejercicio para el lector, la observación clave es que la restricción de $\phi_{f_i}^{\mathcal{M}}$ a N_{f_1} es inyectiva, para $i = 2, 3, \ldots, t$. CQD.

5. Forma normal de Smith de una matriz en un DIP

En esta sección daremos un resultado clásico que será clave para determinar la estructura de los módulos de tipo finito sobre un DIP.

Partimos de un dominio de ideales principales $\mathcal{A}$. Recordemos que sobre el producto cartesiano
$$A^n = A \times A \times \overset{n)}{\cdots} \times A$$
hay una estructura estándar de $\mathcal{A}$-módulo. Todo homomorfismo de $\mathcal{A}$-módulos $\phi : A^n \to A^m$ determina una matriz $T_\phi = (t_{ij})$ con n filas y m columnas y cuyos coeficientes t_{ij} están en A, donde
$$\phi(\mathbf{e}_i^n) = (t_{i1}, t_{i2}, \ldots, t_{im}),$$
siendo $\mathbf{e}_i^n = (0, 0, \ldots, 0, 1, 0, \ldots, 0) \in A^n$, con el coeficiente 1 en el lugar i. Recíprocamente, toda matriz T de dimension $n \times m$ con coeficientes en A determina un homomorfismo de $\mathcal{A}$-módulos $\phi_T : A^n \to A^m$ cuya matriz es T.

Exactamente como ya sabemos hacer para espacios vectoriales, si tenemos dos homomorfismos de $\mathcal{A}$-módulos
$$A^n \overset{\phi}{\to} A^m \overset{\psi}{\to} A^s$$
se cumple que $T_{\psi \circ \phi} = T_\phi T_\psi$. En particular, si $\alpha : A^n \to A^m$ es un isomorfismo, la matriz T_α es invertible, más concretamente
$$T_\alpha T_{\alpha^{-1}} = I_m; \quad T_{\alpha^{-1}} T_\alpha = I_n.$$

Proposición 12. *Si A^n y A^m son isomorfos, se tiene que $n = m$.*

Demostración: Basta ver que si tenemos dos matrices P y Q con coeficientes en A, de dimensiones $n \times m$ y $m \times n$ respectivamente y tales que $PQ = I_n$ y $QP = I_m$ entonces $n = m$. Como $\mathcal{A}$ es un dominio, existe un cuerpo K con $A \subset K$ y el problema se plantea para matrices con coeficientes en un cuerpo, por tanto $n = m$. (La existencia de K se deriva de la construcción usual del cuerpo de fracciones de un dominio, que no difiere esencialmente de la construcción de los números racionales a partir de $\mathbb{Z}$.) CQD.

Cualquier matriz cuadrada invertible da lugar a un isomorfismo. Nótese que, aunque se trate de un DIP y no un cuerpo las fórmulas para obtener la inversa de una matriz cuadrada son las mismas, en particular una matriz cuadrada T con coeficientes en A es invertible si y sólo si su determinante es una unidad.

Diremos que dos homomorfismos $\phi, \psi : A^n \to A^m$ son *homomorfismos equivalentes de $\mathcal{A}$-módulos* si y sólo si existen isomorfismos $\alpha : A^n \to A^n$ y $\beta : A^m \to A^m$ tales que

$$\psi = \beta \circ \phi \circ \alpha^{-1}.$$

Esto es equivalente a decir que existen matrices invertibles P y Q con coeficientes en A, tales que

$$T_\psi = PT_\phi Q.$$

TEOREMA 2 (Teorema de Smith). *Dada una matriz T de dimensión $n \times m$ con coeficientes en un dominio de ideales principales $\mathcal{A}$, existen dos matrices invertibles P y Q tales que el producto PTQ tiene una de las siguientes formas diagonales*

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 \cdots 0 \\ 0 & d_2 & \cdots & 0 & 0 \cdots 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d_s & 0 \cdots 0 \end{pmatrix}, \quad \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d_s \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix};$$

donde $(d_1) \supset (d_2) \supset \cdots \supset (d_s)$, siendo $r = \min(n, m)$.

El teorema de Smith se sigue de los siguientes lemas:

LEMA 1. *Dada una matriz $T = (t_{ij})$ de dimensión $n \times m$ con coeficientes en un dominio de ideales principales $\mathcal{A}$ y matrices invertibles P y Q de dimensiones respectivas $n \times n$ y $m \times m$. Consideremos la matriz $T' = PTQ = (t'_{ij})$. El máximo común divisor (d) de los coeficientes t_{ij} es igual al máximo común divisor (d') de los coeficientes t'_{ij}.*

Demostración: Veamos primero el caso en el que $Q = I_m$. Los coeficientes t'_{ij} se obtienen como combinaciones lineales de coeficientes t_{ij}, se sigue que d divide todos los t'_{ij} y en particular $(d) \supset (d')$. Argumentando que $T = P^{-1}(PT)$ concluimos asimismo que $(d') \supset (d)$. Por consiguiente $(d) = (d')$. Argumento similar para el caso $P = I_n$. Finalizamos observando que podemos obtener T' a partir de T en dos pasos del tipo anterior: $T \rightsquigarrow PT \rightsquigarrow (PT)Q = T'$. CQD.

LEMA 2. *Dada una matriz $T = (t_{ij})$ de dimensión $n \times m$ con coeficientes en un dominio de ideales principales $\mathcal{A}$, existen dos matrices invertibles P y Q tales que el producto PTQ tiene la forma*

$$PTQ = \left(\begin{array}{c|c} d & 0 \\ \hline 0 & H \end{array}\right)$$

donde H es una matriz $(n-1) \times (m-1)$ y d divide todos los coeficientes de H.

Demostración: Dado un elemento $a \in A$, consideremos la descomposición en producto de elementos irreducibles primos entre sí dos a dos $a = up_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$. Llamemos *longitud* $\ell(a)$ a la suma $\ell(a) = n_1 + n_2 + \cdots + n_t$. Por convención, escribimos $\ell(0) = \infty$.

Sea d un máximo común divisor de los coeficientes de T. Haremos inducción sobre el valor $\ell(T)$ definido por $\ell(T) = \ell(t_{11}) - l(d)$. Obsérvese que $\ell(T) \geq 0$.

Si $\ell(T) = 0$, como d divide t_{11}, tenemos que $t_{11} = ud$, donde u es una unidad. En particular t_{11} divide todos los coeficientes de T. En este caso podemos conseguir una matriz de la forma deseada, substituyendo la columna c_1 por $u^{-1}c_1$ y para cada $j \geq 2$, la columna c_j por $c_j - \lambda_j c_1$, donde $t_{1j} = \lambda_j t_{11}$. Así obtenemos una matriz de la forma

$$PTQ = \left(\begin{array}{c|c} d & 0 \\ \hline * & H \end{array}\right).$$

Ahora realizamos una operación similar con las filas: Dejamos fija la primera y para cada $i \geq 2$ substituimos la fila f_i por $f_i - \mu_i f_1$ donde $t_{i1} = \mu_i t_{11}$. Las operaciones realizadas corresponden al producto a la izquierda, caso de las filas, y a la derecha, caso de las columnas, por matrices invertibles sencillas, cuya descripción dejamos al lector.

Supongamos que $\ell(T) > 0$ y que el resultado es cierto para todas las matrices T' con $\ell(T') < \ell(T)$. Distinguimos varios casos:

A_1) En la primera fila existe un coeficiente no divisible por t_{11}. Después de un cambio de orden en las columnas, podemos suponer que este coeficiente es t_{12}. Sea d' el máximo común divisor de t_{11} y de t_{12}, nótese que $\ell(d') < \ell(t_{11})$. Sabemos que existen $\alpha, \beta, \gamma, \delta \in A$ tales que

$$\alpha t_{11} + \beta t_{12} = d',\ \gamma\alpha + \delta\beta = 1.$$

Consideramos ahora la matriz T' obtenida multiplicando T a la derecha por la siguiente matriz invertible:

$$\left(\begin{array}{cc|c} \alpha & -\gamma & \\ \beta & \delta & 0 \\ \hline \multicolumn{2}{c|}{0} & I_{m-2} \end{array}\right)$$

En la nueva matriz T' el coeficiente t'_{11} es igual a d'. Teniendo en cuenta el lema anterior,

$$\ell(T') = l(d') - \ell(d) < \ell(t_{11}) - \ell(d) = \ell(T)$$

y aplicamos la hipótesis de inducción a T'.

A_2) En la primera columna existe un coeficiente no divisible por t_{11} actuamos como en el caso A_1).

B) Supongamos que todos los coeficientes de la primera fila y la primera columna son divisibles por t_{11}. Podemos poner ceros en la primera fila y la primera columna, para reducirnos al caso en el que T tiene la forma

$$T = \left(\begin{array}{c|c} t_{11} & 0 \\ \hline 0 & H \end{array}\right),$$

donde hay un coeficiente t_{ij} con $i, j \geq 2$ no divisible por t_{11}. Sumamos la fila i a la primera fila, este coeficiente pasa a la primera fila y recaemos necesariamente en el caso A_1). CQD.

NOTA 1. Los ideales de la descomposición de Smith son únicos, aunque no detallaremos esta prueba. No obstante, podemos dar una idea de cómo hacerla. El ideal (d_1) es el máximo común divisor de los menores de tamaño uno (los coeficientes) de la matriz PTQ, que sabemos coincide con el máximo común divisor de los coeficientes de la matriz T. Para un índice $1 \leq k \leq r$, el ideal $(d_1 d_2 \cdots d_k)$ es el máximo común divisor de los menores de tamaño k de la matriz PTQ. Se puede demostrar que coincide con el máximo común divisor de los menores de tamaño k de la matriz T, aunque es un poco tedioso. Para verlo, si denotamos por $\Lambda^k(T)$ la matriz formada por los menores de orden k de T,

adecuadamente colocados, se puede demostrar que $\Lambda^k(PTQ) = \Lambda^k(P)\Lambda^k(T)\Lambda^k(Q)$, y así reducimos el problema al caso inicial de los coeficientes.

Sea l el entero tal que $(1) = (d_l) \supsetneq (d_{l+1})$. Se tiene que:

$$(1) = (d_1) = (d_2) = \cdots = (d_l) \supsetneq (d_{l+1}) \supset (d_{l+2}) \supset \cdots \supset (d_r).$$

Escribamos $s = r - l$ y $e_j = d_{l+j}$ para $j = 1, 2, \ldots, s$. La lista de ideales

$$(e_1) \supset (e_2) \supset \cdots (e_s),$$

recibe el nombre de *lista de factores invariantes de la matriz* T.

6. Submódulos de un módulo finitamente generado

Sea $\mathcal{A}$ un dominio de ideales principales. Decimos que un módulo $\mathcal{M}$ es *libre de rango n sobre* $\mathcal{A}$ si y sólo si $\mathcal{M}$ es isomorfo a un módulo de tipo A^n. Obsérvese que los módulos libres no tienen elementos de torsión, esto es $\tau(\mathcal{M}) = \{0\}$.

PROPOSICIÓN 13. *Todo submódulo $N \subset A^m$ de un módulo libre de rango m es libre de rango n con $n \leq m$.*

Demostración: Trabajamos por inducción sobre m. Si $m = 1$, un submódulo N de A es exactamente un ideal de A y como se trata de un DIP, tenemos que $N = aA$. Si $a = 0$, tenemos que $N = (0)$ es libre de rango 0. Si $a \neq 0$, es libre de rango 1, ya que la aplicación

$$A \to aA; \quad b \mapsto ab$$

da un isomorfismo de $\mathcal{A}$-módulos entre A y aA.

Supongamos ahora que $m > 1$ y consideremos la aplicación de proyección sobre la última coordenada

$$\pi : A^m \to A; \quad (a_1, a_2, \ldots, a_m) \mapsto a_m.$$

La imagen $\pi(N) \subset A$ es un módulo libre de rango uno, o bien es $\pi(N) = \{0\}$. Si $\pi(N) = \{0\}$, entonces

$$N \subset A^{m-1} \times \{0\} \leftrightarrow A^{m-1}$$

y podemos aplicar la inducción. En caso contrario, tenemos $\pi(N) = aA$, con $a \neq 0$. Nótese que Ker $(\pi) = A^{m-1} \times \{0\}$ es libre de rango $m - 1$. Seleccionemos un elemento $s_0 \in N$ tal que $\pi(s_0) = a$. Tenemos que $< s_0 > \subset N$ es isomorfo a aA y por tanto a A. Por otro lado veamos que

$$N = (N \cap \text{Ker } (\pi)) \oplus < s_0 > .$$

En efecto, dado $s \in N$, sabemos que $\pi(s) = ba$ y tenemos una expresión

$$s = (s - bs_0) + bs_0 \in (N \cap \text{Ker } (\pi)) + < s_0 > .$$

Se sigue que $N = (N \cap \text{Ker } (\pi)) + < s_0 >$. Veamos que la suma es directa: si $\pi(bs_0) = 0$, entonces $ba = 0$ y $b = 0$. Con esto terminamos, ya que, por inducción, sabemos que $N \cap \text{Ker } (\pi) \subset \text{Ker } (\pi)$ es libre de rango menor o igual que $m - 1$.

CQD.

COROLARIO 4. *Supongamos que $\mathcal{M}$ es un $\mathcal{A}$-módulo generado por m elementos y que $N \subset M$ es un submódulo, entonces N puede generarse por n elementos con $n \leq m$.*

Demostración: Consideremos un sistema de generadores $v_1, v_2, \ldots, v_m$ de M. Existe un homomorfismo suprayectivo de $\mathcal{A}$-módulos

$$\phi : A^m \to M$$

tal que $\phi(\mathbf{e}_i^m) = v_i$; donde recordamos que $\mathbf{e}_i^m \in A^m$ es el elemento cuyos coeficientes son 0 excepto el que ocupa el lugar i, que es igual a 1. Sabemos que $\phi^{-1}(N)$ es libre de rango $n \leq m$ por la proposición anterior. Como ϕ induce un homomorfismo suprayectivo

$$\phi^{-1}(N) \to N,$$

concluimos que N puede generarse por n elementos. CQD.

7. Decomposición en módulos cíclicos

Consideremos un dominio de ideales principales $\mathcal{A}$ y un $\mathcal{A}$-módulo $\mathcal{M}$. Diremos que $\mathcal{M}$ es *cíclico* si está generado por un sólo elemento, es decir, existe $m \in M$ tal que

$$M =< m >= \{am;\ a \in A\}.$$

Nótese que si $\mathcal{M}$ es cíclico, su anulador coincide con el del generador m, es decir,

$$\text{Ann } (\mathcal{M}) = \text{Ann } (m).$$

Sabemos que $\mathcal{M}$ es de torsión si y solamente si Ann $(\mathcal{M}) =$ Ann $(m) \neq (0)$. Cuando $\mathcal{M}$ no es de torsión, la aplicación $A \to M$ dada por $a \mapsto am$ define un isomorfismo de $\mathcal{A}$-módulos.

Dado un A-módulo $\mathcal{M}$ de tipo finito, denotaremos por $\mu(\mathcal{M})$ el mínimo número de generadores de $\mathcal{M}$. Es decir, este número está determinado por el hecho de que existe un sistema finito de generadores de $\mathcal{M}$ con $\mu(\mathcal{M})$ elementos y no existe ninguno con menos elementos. Por convención diremos que $\mu(\mathcal{M}) = 0$ es equivalente a decir que $M = \{0\}$.

Deseamos probar el siguiente resultado:

TEOREMA 3. *Sea $\mathcal{A}$ un dominio de ideales principales y $\mathcal{M} \neq 0$ un $\mathcal{A}$-módulo de tipo finito. Escribamos $m = \mu(\mathcal{M})$. Existe una descomposición de $\mathcal{M}$ en suma directa interna de submódulos cíclicos*

$$M =< v_1 > \oplus < v_2 > \oplus \cdots \oplus < v_m >; \quad \text{Ann}(< v_i >) = (e_i),\ i = 1, 2, \ldots, m,$$

tal que $(1) \neq (e_1) \supset (e_2) \supset \cdots \supset (e_m)$. En particular $\text{Ann}(\mathcal{M}) = (e_m)$.

Demostración: Si $m = 0$, entonces $M = \{0\}$ y no hay nada que demostrar. Si $m = 1$, entonces $\mathcal{M}$ ya es un módulo cíclico $M =< v >$ con $v \neq 0$, en este caso

$$\text{Ann}(v) = \text{Ann}(\mathcal{M}) = (e),$$

donde $(e) \neq (1)$, ya que $v \neq 0$. Veamos ahora el caso general $m \geq 1$. Como $\mathcal{M}$ puede generarse por m elementos, existe un morfismo suprayectivo

$$\phi : A^m \to M.$$

El núcleo Kerϕ es un submódulo de A^m y por tanto es un módulo libre de A^m de rango $r \leq m$. Así, existe un homomorfismo inyectivo $\psi' : A^r \to A^m$ tal que $\text{Im}(\psi') = \text{Ker}\phi$. Consideremos la primera proyección $\pi : A^r \times A^{m-r} \to A^r$ y sea $\psi = \psi' \circ \pi$. Como π es suprayectivo, tenemos que $\text{Im}(\psi) = \text{Im}(\psi')$. Así pues, tenemos un morfismo

$$\psi : A^m \to A^m,$$

tal que $\mathrm{Im}(\psi) = \mathrm{Ker}\phi$.

Apliquemos el teorema de Smith al morfismo ψ. Entonces existen dos isomorfismos $\alpha : A^m \to A^m$ y $\beta : A^m \to A^m$ tales que el homomorfismo $\bar{\psi}$ dado por

$$\bar{\psi} = \beta \circ \psi \circ \alpha^{-1} : A^m \to A^m$$

cumple que $\bar{\psi}(\mathbf{e}_i^r) = d_i \mathbf{e}_i^m$ para $i = 1, 2, \ldots, m$, donde cada d_i divide el siguiente. Definamos φ por:

$$\varphi = \phi \circ \beta^{-1} : A^m \to M.$$

Como ϕ es suprayectivo y β es una biyección, tenemos que φ es suprayectivo. Además $\bar{\psi}(A^r) = \mathrm{Ker}\varphi$, en efecto

$$\bar{\psi}(A^r) = \beta \circ \psi \circ \alpha^{-1}(A^r) = \beta \circ \psi(A^r) = \beta(\mathrm{Ker}\phi) = \mathrm{Ker}(\phi \circ \beta^{-1}) = \mathrm{Ker}\varphi.$$

Observemos que

$$\mathrm{Ker}\varphi = \bar{\psi}(A^r) = \{(a_1 d_1, a_2 d_2, \ldots, a_m d_m) \in A^m;\ a_i \in A, 1 \leq i \leq m\}.$$

Denotemos $v_i = \varphi(\mathbf{e}_i^m)$, para $i = 1, 2, \ldots, m$. Sabemos que

$$M =< v_1, v_2, \ldots, v_m > .$$

Veamos que,

$$\mathrm{Ann}(w_i) = (d_i), \quad i = 1, 2, \ldots, m.$$

Se tiene que $d_i w_i = \varphi(d_i \mathbf{e}_i^m)$. Dada la descripción de $\mathrm{Ker}\varphi = \bar{\psi}(A^n)$, vemos que $d_i \mathbf{e}_i^m \in \mathrm{Ker}\varphi$ y por tanto, $d_i w_i = 0$, luego $d_i \in \mathrm{Ann}(w_i)$; recíprocamente, si $q \in \mathrm{Ann}(w_i)$, entonces $q\mathbf{e}_i^m \in \mathrm{Ker}\varphi$. Esto implica que

$$q\mathbf{e}_i^m = a_1 d_1 \mathbf{e}_1^m + a_2 d_2 \mathbf{e}_2^m + \cdots + a_n d_n \mathbf{e}_n^m$$

y por consiguiente $q = a_i d_i \in (d_i)$.

Falta ver que la suma

$$M =< v_1 > + < v_2 > + \cdots + < v_m >$$

es directa. Para ello, es suficiente probar que si

$$0 = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m,$$

entonces $\lambda_i v_i = 0$ para todo $i = 1, 2, \ldots, m$. Tenemos que

$$0 = \varphi(\lambda_1 \boldsymbol{e}_1^m + \lambda_2 \boldsymbol{e}_2^m + \cdots + \lambda_m \boldsymbol{e}_m^m).$$

Dada la descripción de $\mathrm{Ker}(\varphi)$, existen $a_i \in A$ tales que

$$\lambda_1 \boldsymbol{e}_1^m + \lambda_2 \boldsymbol{e}_2^m + \cdots + \lambda_m \boldsymbol{e}_m^m = a_1 e_1 \boldsymbol{e}_1^m + a_2 e_2 \boldsymbol{e}_2^m + \cdots + a_m e_m \boldsymbol{e}_m^m,$$

por tanto $\lambda_i v_i = a_i e_i \phi(\boldsymbol{e}_i^m) = a_i e_i v_i = 0$, pues $e_i v_i = 0$, para todo $i = 1, 2, \ldots, m$. CQD.

Observación 1. La descomposición de $\mathcal{M}$ que acabamos de ver, nos permite observar que el anulador de $\mathcal{M}$ es el ideal (0) si y sólo si $e_s = 0$. Más generalmente, supongamos que $e_{k+1} = e_{k+2} = \cdots = e_s = 0$ y que $e_k \neq 0$, entonces podemos descomponer $\mathcal{M}$ como suma directa interna

$$M = T \oplus L, \quad T =< v_1 > \oplus < v_2 > \oplus \cdots \oplus < v_k >,$$

donde $L = Av_{k+1} \oplus Av_{k+2} \oplus \cdots \oplus Av_s$ es un $\mathcal{A}$-módulo libre de rango $s - k$ y T es un $\mathcal{A}$-módulo de torsión cuyo anulador es el ideal (e_k). Además, podemos ver que $T = \tau(\mathcal{M})$. En efecto, si $t + l$ es un elemento de torsión con $t \in T$ y $l \in L$, existe

un elemento del anillo $a \neq 0$ tal que $0 = a(t+l) = at + al$; en particular, se tiene que $al = 0$ y por tanto, $l = 0$, de donde $t + l \in T$.

NOTA 2. La observación anterior permitiría demostrar que el rango de la parte libre L de $\mathcal{M}$ está intrínsicamente definido, pues L se obtiene como el cociente de M por T. No insistiremos en esta construcción, que corresponde al "primer teorema de descomposición" de módulos de tipo finito sobre DIP.

NOTA 3. La cadena de ideales $(e_1) \supset (e_2) \supset \cdots \supset (e_s)$ es única. No haremos la demostración completa de esta propiedad para el caso de módulos de tipo finito sobre DIP, sin embargo sí la probaremos para un tipo especial de módulos de tipo finito sobre el anillo de polinomios con coeficientes en un cuerpo: los asociados a endomorfismos de espacios vectoriales.

La lista de ideales $(e_1) \supset (e_2) \supset \cdots \supset (e_s)$ recibe el nombre de *lista de factores invariantes del módulo* $\mathcal{M}$.

8. Homotecias y submódulos cíclicos

Sea $\mathcal{M}$ un módulo de tipo finito sobre un dominio de ideales principales $\mathcal{A}$. Dado $a \in A$, hemos visto que

$$\phi_a^{\mathcal{M}} : M \to M, \quad m \mapsto am,$$

es un endomorfismo de $\mathcal{M}$, que llamaremos *homotecia de razón* a. El núcleo de $\phi_a^{\mathcal{M}}$ es el submódulo de $\mathcal{M}$ definido por

$$\mathrm{Ker}(\phi_a^{\mathcal{M}}) = \{m \in M;\ am = 0\}.$$

Nos va a interesar describir la intersección de submódulos cíclicos de $\mathcal{M}$ con los del tipo $\mathrm{Ker}(\phi_a^{\mathcal{M}})$.

LEMA 3. *Sea $\mathcal{M}$ un $\mathcal{A}$-módulo finitamente generado, donde $\mathcal{A}$ es un dominio de ideales principales. Tomemos $v \in M$ con $\mathrm{Ann}(v) = (b)$. Consideremos un elemento $a \in A$ del anillo y d el máximo común divisor $(d) = (a, b)$. Escribamos $b = b'd$. La intersección*

$$N =< v > \cap \mathrm{Ker}(\phi_a^{\mathcal{M}})$$

es el submódulo cíclico $< b'v >$. Además $\mathrm{Ann}(b'v) = (d)$.

Demostración: Escribamos $a = a'd$. Observemos que $(a', b') = (1)$. Queremos probar que $N =< b'v >$. Sea $w = cv \in N$. Esto implica que $acv = 0$, en particular $ac \in (b)$, esto es $ac = be$ y por tanto $a'dc = b'de$, lo que implica que $a'c = b'e$. Como $(a', b') = (1)$, se sigue que $c \in (b')$, por lo tanto $c = fb'$ y entonces $w \in < b'v >$. Recíprocamente, consideremos un elemento de la forma $fb'v$, entonces $a(fb'v) = a'dfb'v = a'f(bv) = 0$.

Veamos que $\mathrm{Ann}(b'v) = (d)$. Ciertamente $\mathrm{Ann}(b'v) \supset (d)$ pues $db'v = bv = 0$. Recíprocamente, si $f(b'v) = 0$, entonces $fb' \in (b)$, es decir $fb' = gb = gb'd$, por tanto $f = gd \in (d)$. CQD.

COROLARIO 5. *Sea $\mathcal{M}$ un $\mathcal{A}$-módulo finitamente generado y consideremos una descomposición de $\mathcal{M}$ como suma directa interna de submódulos cíclicos*

$$M =< v_1 > \oplus < v_2 > \oplus \cdots \oplus < v_s >, \quad \mathrm{Ann}(< v_i >) = (d_i),$$

donde d_i divide d_{i+1} para $i = 1, 2, \ldots, s-1$. Dado $N = \mathrm{Ker}(\phi_a^{\mathcal{M}})$, donde $a \in A$, tenemos que N es suma directa interna de módulos cíclicos

$$N =< d_1'v_1 > \oplus < d_2'v_2 > \oplus \cdots \oplus < d_s'v_s >, \quad \mathrm{Ann}(< d_i'v_i >) = (e_i),$$

donde e_i divide e_{i+1}, para $i = 1, 2, \ldots, s-1$, con $(e_i) = (a, d_i)$ y $d_i = d_i'e_i$.

Demostración: Escribamos $N_i = N \cap < v_i >$. Por el lema anterior, sabemos que $N_i =< d_i'v_i >$. Además, la suma $N_1 + N_2 + \cdots + N_s$ es directa. Falta ver que

$$N = N_1 + N_2 + \cdots + N_s.$$

Tomemos $v \in N$. Lo podemos escribir $v = a_1v_1 + a_2v_2 + \cdots + a_sv_s$ y sabemos que $av = 0$. Así pues

$$0 = av = aa_1v_1 + aa_2v_2 + \cdots + aa_sv_s.$$

Como la suma es directa, se concluye que $aa_jv_j = 0$ y por consiguiente $a_jv_j \in N_j$, para todo $j = 1, 2, \ldots, s$. CQD.

Observación 2. La descomposición en suma directa de módulos cíclicos de $\mathcal{M}$ que aparece en el enunciado anterior, coincide con la descomposición en módulos cíclicos cuyos anuladores son los factores invariantes en el caso de que $(d_1) \neq (1)$ o, de manera equivalente, cuando $v_1 \neq 0$.

9. Módulos sobre $k[X]$ y endomorfismos de un espacio vectorial

Sea k un cuerpo, ya tenemos varios ejemplos de cuerpos, lo que hagamos en esta sección será válido para cualquiera de ellos. Recordemos que un espacio vectorial E sobre k es exactamente un k-módulo, es decir, es una terna

$$E = (V, \sigma, \pi); \quad \sigma : (v, w) \mapsto v + w; \quad \pi : (\lambda, v) \mapsto \lambda v,$$

que cumple los axiomas de k-módulo. Tenemos interés en dotar el conjunto subyacente V de varias estructuras diferentes.

Denotamos por $k[X]$ el anillo de polinomios en una variable X con coeficientes en k. Sabemos que es un DIP. En este caso, identificamos el anillo y su conjunto subyacente, ya que no habrá confusión posible, pues siempre utilizaremos la suma y producto habituales de polinomios.

Sea $E = (V, \sigma, \pi)$ un k-espacio vectorial. Consideremos un endomorfismo

$$f : V \to V$$

de E, esto es $f \in \mathrm{End}_k(E)$ o, lo que es lo mismo, la aplicación f es lineal. Dado un polinomio $P \in k[X]$, con

$$P = \lambda_0 + \lambda_1 X + \lambda_2 X^2 + \cdots + \lambda_n X^n \in k[X],$$

definimos el endomorfismo de k-espacios vectoriales $P(f) : V \to V$ por

$$P(f) = \lambda_0 \mathrm{id}_V + \lambda_1 f + \lambda_2 f^2 + \cdots + \lambda_n f^n.$$

donde f^k denota la composición k veces de f consigo mismo, y por convención $f^0 = \mathrm{id}_V$.

Podemos obtener un $k[X]$-módulo $M_f(E) = (V, \sigma, \pi_f)$, con el mismo conjunto subyacente V y la misma suma σ que E, definiendo el producto $\pi_f(P, v) = P \bullet_f v$ por

$$P \bullet_f v = P(f)(v), \quad P \in k[X], \ v \in V.$$

La comprobación de que $M_f(E)$ es un $k[X]$-módulo es inmediata. Nótese que:

(1) Si $\lambda \in k$, $v \in V$, entonces $\lambda \bullet_f v = \lambda v$.
(2) Dado $v \in V$, se tiene $X \bullet_f v = f(v)$.
(3) Dados $v \in V$, $P \in k[X]$, se tiene $P \bullet_f v = X \bullet_{P(f)} v = P(f)(v)$.

Dado un $k[X]$-módulo $\mathcal{M} = (M, \sigma, \tilde{\pi})$, se tiene un k-espacio vectorial

$$E_{\mathcal{M}} = (M, \sigma, \pi)$$

inducido, sin más que asimilar el producto por elementos de k al producto por polinomios constantes, a la vista de que $k \subset k[X]$. Es decir, para cada $\lambda \in k$ y $v \in M$, tenemos que $\pi(\lambda, v) = \tilde{\pi}(\lambda, v)$.

Fijado un espacio vectorial $E = (V, \sigma, \pi)$, denotemos por $\mathfrak{M}(E)$ el conjunto de $k[X]$-módulos que inducen E como k-espacio vectorial. Es decir

$$\mathfrak{M}(E) = \{\mathcal{M};\ \mathcal{M} \text{ es un } k[X]\text{-módulo y } E_{\mathcal{M}} = E\}.$$

PROPOSICIÓN 14. *Se tiene una biyección*

$$\Phi_E : \mathrm{End}_k(E) \to \mathfrak{M}(E),$$

dada por $\Phi_E(f) = M_f(E)$.

Demostración: Si $f \neq g$ son dos endomorfismos vectoriales diferentes, existe $v \in V$ tal que $f(v) \neq g(v)$. Esto implica que

$$\pi_f(X, v) = f(v) \neq g(v) = \pi_g(X, v),$$

así, los productos π_f y π_g son diferentes y por tanto $M_f(E) \neq M_g(E)$. Esto prueba la inyectividad de Φ_E. Recíprocamente, consideremos un $k[X]$-módulo

$$M = (V, \sigma, \tilde{\pi}) \in \mathfrak{M}(E).$$

Definamos $f : V \to V$ por $f(v) = \tilde{\pi}(X, v)$. Tenemos que $M = M_f(E)$ (ejercicio) y entonces la aplicación Φ_E es suprayectiva. CQD.

Dado $f \in \mathrm{End}_k(E)$ y un subespacio vectorial $W \subset V$ de E, decimos que W *es invariante por* f si se tiene que $f(W) \subset W$. Un ejemplo interesante de subespacio invariante es el conjunto $\mathrm{Prop}(E, f; \lambda)$ de los vectores propios de f con valor propio $\lambda \in k$.

PROPOSICIÓN 15. *Dados* $f \in \mathrm{End}_k(E)$ *y un subconjunto* $W \subset V$*, las siguientes propiedades son equivalentes:*

(1) W *es un subespacio vectorial de* E*, invariante por* f*.*
(2) W *es un* $k[X]$*-submódulo de* $M_f(E)$*.*

Demostración: Supongamos que se cumple (1). Sabemos que la suma en W es interna y se tiene un grupo abeliano. Para probar (2), falta ver que el producto en $M_f(E)$ por un polinomio es interno, para ello es suficiente ver que $X \bullet_f w \in W$ para cada $w \in W$, lo que es cierto ya que $X \bullet_f w = f(w) \in W$.

Recíprocamente, supongamos que se cumple (2). Por constucción W es un subespacio vectorial de E. Además, como el producto por X es interno en W, para cada $w \in W$ tenemos que $f(w) = X \bullet_f w \in W$, por tanto W es invariante por f. CQD.

10. Conjugación de endomorfismos vectoriales

Sean k un cuerpo y E un k-espacio vectorial de conjunto subyacente V. Decimos que dos endomorfismos $f, g \in \mathrm{End}_k(E)$ están *conjugados* si y sólo si existe un automorfismo $\phi \in \mathrm{Aut}_k(E)$ de manera que

$$\phi \circ f = g \circ \phi$$

Esto es equivalente a decir que $g = \phi \circ f \circ \phi^{-1}$ (recuérdese que ϕ es invertible, pues es un automorfismo).

Observación 3. En el caso de dimensión finita, sabemos que esto es equivalente a decir que f y g tienen la misma matriz si seleccionamos una base adecuada para f y otra para g; asimismo, si fijamos una base común, la matriz de g es *equivalente a la matriz de* f. Recordemos que dos matrices cuadradas A y B con coeficientes en un cuerpo k son equivalentes si existe una matriz invertible U tal que $B = UAU^{-1}$.

De una manera más general, dados $f, g \in \mathrm{End}_k(E)$, denotemos por $\mathrm{Conj}(E; f, g)$ el conjunto de endomorfismos $h \in \mathrm{End}_k(E)$ que cumplen la relación

$$h \circ f = g \circ h.$$

Denotemos asimismo por $\mathrm{Conj}^*(E; f, g)$ el conjunto de elementos de $\mathrm{Conj}(E; f, g)$ que son automorfismos, esto es

$$\mathrm{Conj}^*(E; f, g) = \mathrm{Conj}(E; f, g) \cap \mathrm{Aut}_k(E).$$

Los elementos de $\mathrm{Conj}^*(E; f, g)$ se llaman *conjugantes* para f y g.

Proposición 16. *Dados $f, g \in \mathrm{End}_k(E)$, se tienen las igualdades*

$$\begin{aligned} \mathrm{Conj}(E; f, g) &= \mathrm{Hom}_{k[X]}(M_f(E), M_g(E)), \\ \mathrm{Conj}^*(E; f, g) &= \mathrm{Isom}_{k[X]}(M_f(E), M_g(E)). \end{aligned}$$

Demostración: Tomemos $h \in \mathrm{Conj}(E; f, g)$. Para ver que h define un homomorfismo de $k[X]$-módulos de $M_f(E)$ en $M_g(E)$, falta solamente comprobar que

$$h\,(P \bullet_f v) = P \bullet_g h(v),$$

para cada $v \in V$ y $P \in k[X]$. Por compatibilidad con la suma y producto por escalares, es suficiente comprobar el caso $P = X^n$. Veamos por inducción que

$$h\,(X^n \bullet_f v) = X^n \bullet_g h(v), \quad n \geq 0.$$

Para $n = 0$ el resultado es inmmediato, pues $X^0 = 1$. Para $n = 1$, tenemos que

$$h\,(X \bullet_f v) = h(f(v)) = (h \circ f)(v) = (g \circ h)(v) = g(h(v)) = X \bullet_g h(v).$$

Usando la inducción, para cada $n \geq 1$ tenemos

$$\begin{aligned} h\,(X^n \bullet_f v) &= h(X \bullet_f (X^{n-1} \bullet_f v) = X \bullet_g h((X^{n-1} \bullet_f v) = \\ &= X \bullet_g (X^{n-1} \bullet_g h(v)) = X^n \bullet_g h(v). \end{aligned}$$

Recíprocamente, si tomamos $h \in \mathrm{Hom}_{k[X]}(M_f(E), M_g(E))$ sabemos que $h : V \to V$ es un endomorfismo del espacio vectorial E y que además, para todo $v \in V$ se tiene

$$(h \circ f)(v) = h(X \bullet_f v) = X \bullet_g h(v) = (g \circ h)(v),$$

por tanto $h \circ f = g \circ h$.

Finalmente sabemos que la condición necesaria y suficiente para que un endomorfismo de espacios vectoriales sea automorfismo es que sea biyectivo y lo mismo

ocurre para un homomorfismo de $k[X]$-módulos. Se concluye la segunda igualdad. CQD.

Un corolario muy importante es que dos endomorfismos f, g del k-espacio vectorial E están conjugados si y sólo si los $k[X]$-módulos $M_f(E)$ y $M_g(E)$ son isomorfos.

11. Primera descomposición de Jordan

Sean E un k-espacio vectorial de dimensión finita y $f \in \mathrm{End}_k(E)$ un endomorfismo de E.

PROPOSICIÓN 17. *El $k[X]$-módulo $M_f(E)$ está finitamente generado y es un módulo de torsión.*

Demostración: Consideremos una base $e_1, e_2, \ldots, e_n \in V$ del espacio vectorial E. Dado $v \in V$, sabemos que v es una combinación lineal con coeficientes en k de los elementos de la base

$$v = \mu_1 e_1 + \mu_2 e_2 + \cdots + \mu_n e_n.$$

Se trata, en particular, de una combinación lineal con coeficientes en $k[X]$ y por tanto $M_f(E)$ está finitamente generado. Para probar que $M_f(E)$ es de torsión, tenemos que ver que cada $v \in V$ es de torsión. Elijamos $v \in V$ y consideremos las sucesivas imágenes de v por f hasta, como máximo, la dimensión de V

$$v, f(v), f^2(v), \ldots, f^n(v).$$

Se trata de $n+1$ vectores en V que no pueden ser linealmente independientes, pues $n = \dim_k V$. Así pues existe una lista no nula $\lambda_0, \lambda_1, \lambda_2, \ldots, \lambda_n$ de elementos de k tal que

$$\lambda_0 v + \lambda_1 f(v) + \lambda_2 f^2(v) + \ldots + \lambda_n f^n(v) = 0.$$

Si consideramos el polinomio no nulo $P = \lambda_0 + \lambda_1 X + \lambda_2 X^2 + \ldots + \lambda_n X^n$, tenemos que $P \bullet_f v = P(f)(v) = 0$ y por consiguiente v es un elemento de torsión. CQD.

Obsérvese que, como $M_f(E)$ está finitamente generado y es de torsión, su anulador $\mathrm{Ann}(M_f(E))$ es un ideal principal no nulo. Sabemos que dado un polinomio $P \in k[X]$ existe un único polinomio mónico asociado a P, que está dado por $\lambda^{-1}P$, donde λ es el coeficiente del término de mayor grado de P. Esto da pie a la siguiente definición:

DEFINICIÓN 1. *El polinomio mínimo $P_f \in k[X]$ es el único generador mónico del anulador* $\mathrm{Ann}(M_f(E))$. *Es decir P_f es mónico y se tiene*

$$\mathrm{Ann}(M_f(E)) = (P_f) \subset k[X].$$

Si $\dim_k V \geq 1$, tenemos que P_f no es una unidad de $k[X]$, lo que equivale a decir que tiene grado mayor o igual que 1.

EJERCICIO 4. Si P_f tiene grado 1, es decir $P_f = X - \mu$, todos los vectores no nulos son vectores propios asociados al mismo valor propio.

Dado que $k[X]$ es un dominio de ideales principales y que dos polinomios mónicos están asociados si y sólo si son iguales, sabemos que existe una descomposición única salvo cambio de orden

$$P_f = F_1^{m_1} F_2^{m_2} \cdots F_t^{m_t}, \quad m_i \geq 1,\ i = 1, 2, \ldots, t;$$

donde cada F_i es un polinomio mónico e irreducible, para $i = 1, 2, \ldots, t$ y además $F_i \neq F_j$, si $i \neq j$. Nótese que si $i \neq j$ los polinomios $F_i^{m_i}$ y $F_j^{m_j}$ son primos entre sí.

PROPOSICIÓN 18. *Dos endomorfismos conjugados f y g de E tienen el mismo polinomio mínimo.*

Demostración: Sabemos que $M_f(E)$ y $M_g(E)$ son isomorfos como $k[X]$-módulos y por consiguiente tienen el mismo anulador. CQD.

PROPOSICIÓN 19. *Consideremos un endomorfismo $f \in \mathrm{End}_k(E)$ y sea*

$$P_f = F_1^{m_1} F_2^{m_2} \cdots F_t^{m_t}$$

la descomposición del polinomio mínimo como producto de potencias de polinomios mónicos irreducibles F_i diferentes. Existe una descomposición única de $M_f(E)$ en suma directa interna de $k[X]$-submódulos

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_t$$

de manera que $\mathrm{Ann}(W_i) = (F_i^{m_i})$, para cada $i = 1, 2, \ldots, t$. Además, se tiene que $W_i = \mathrm{Ker} F_i^{m_i}(f)$, para cada $i = 1, 2, \ldots, t$.

Demostración: Es consecuencia directa del teorema de descomposición de módulos de torsión finitamente generados sobre un DIP. Véase el corolario 3. CQD.

La suma directa que aparece en el enunciado, también lo es como suma directa de subespacios vectoriales de V invariantes para f. Si elegimos una base β_i de cada W_i, la unión $\beta = \cup_{i=1}^t \beta_i$ da una base de V. La expresión matricial de f en β es diagonal por bloques, formados por las matrices correspondientes, en cada β_i, a los endomorfismos $f_i : W_i \to W_i$ obtenidos por restricción de f.

Recordemos que un endomorfismo $f \in \mathrm{End}_k(E)$ es *diagonalizable* si existe una base del espacio vectorial formada por vectores propios o, lo que es equivalente, una base en la cual la expresión matricial de f sea diagonal.

PROPOSICIÓN 20. *Consideremos un endomorfismo $f \in \mathrm{End}_k(E)$ y sea*

$$P_f = F_1^{m_1} F_2^{m_2} \cdots F_t^{m_t}$$

la descomposición del polinomio mínimo como producto de potencias de polinomios mónicos irreducibles F_i diferentes. Son equivalentes

1. *El endomorfismo f es diagonalizable.*
2. *El grado de cada $F_i^{m_i}$ es igual a 1, para $i = 1, 2, \ldots, t$.*
3. *El grado de F_i es igual a 1 y $m_i = 1$, para $i = 1, 2, \ldots, t$.*

Además, en este caso el número de valores propios diferentes es igual a t.

Demostración: Nótese que (2) y (3) son visiblemente equivalentes.

Supongamos que se cumple (1), es decir, existe una base $\{\mathbf{e}_i\}_{i=1}^n$ de E formada por vectores propios, esto es $f(\mathbf{e}_i) = \lambda_i \mathbf{e}_i$, para cada $i = 1, 2, \ldots, n$. Agrupemos los valores propios λ_i en un conjunto de valores propios distintos. Esto es, consideremos una aplicación suprayectiva $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, t\}$ con la propiedad de que $\lambda_i = \lambda_j$ si y sólo si $p(i) = p(j)$. Escribamos $\mu_u = \lambda_i$ si $p(i) = u$, para cada $u = 1, 2, \ldots, t$. Veamos que el polinomio mínimo P_f es igual a Q, donde

$$Q = (X - \mu_1)(X - \mu_2) \cdots (X - \mu_t).$$

En efecto, para cada $\mathbf{e}_i$ tenemos $Q(f)(\mathbf{e}_i) = 0$ y por tanto $Q \in \mathrm{Ann}(M_f(E))$. Esto prueba que P_f divide Q. En particular P_f es producto de todos o algunos de los factores $X - \mu_u$. Recíprocamente, si uno de los factores $X - \mu_u$ no está presente en la descomposición de P_f, podemos tomar un vector propio $\mathbf{e}_i$ con $\lambda_i = \mu_u$ y tenemos que $P_f \bullet_f \mathbf{e}_i = P_f(f)(\mathbf{e}_i) \neq 0$, absurdo. Se sigue que $P_f = Q$ y por tanto se cumple (2) y que el número t de valores propios diferentes es igual al número de factores irreducibles distintos de P_f.

Supongamos que se cumple (2), por tanto P_f es de la forma

$$Q = (X - \mu_1)(X - \mu_2) \cdots (X - \mu_t),$$

con $\mu_i \neq \mu_j$, para $i \neq j$. Aplicando la proposición 19, tenemos una descomposición de V en suma directa de subespacios invariantes

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_t,$$

de modo que, si denotamos por f_u el endomorfismo de W_u inducido por f, se tiene que $\mathrm{Ann}(M_{f_u}(W_u)) = (X - \mu_u)$, para todo $u = 1, 2, \ldots, t$. Cada vector de W_u es un vector propio con valor propio μ_u. Así construimos una base de V formada por vectores propios, obtenida como unión de bases de los W_i y entonces se tiene (1). CQD.

12. Endomorfismos de tipo cíclico

Diremos que $f \in \mathrm{End}_k(E)$ es un endomorfismo de *tipo cíclico* si el $k[X]$-módulo $M_f(E)$ es cíclico, esto es, está generado por un único elemento $v \in V$.

Proposición 21. *Sea $f \in \mathrm{End}_k(E)$ y sea d el grado del polinomio mínimo P_f. Son equivalentes:*

(1) *El endomorfismo f es de tipo cíclico.*
(2) *Existe $v \in V$ tal que los vectores*

$$v, f(v), f^2(v), \ldots, f^{d-1}(v)$$

forman una base del k-espacio vectorial E.

Demostración: Supongamos que tiene (1) y por consiguiente, el $k[X]$-módulo $M_f(E)$ está generado por un solo elemento $v \in V$, es decir $M_f(E) =< v >$. Como $M_f(E)$ es cíclico, para cada elemento $w \in V$ existe $H \in k[X]$ tal que $w = H \bullet_f v$. Podemos hacer la división $H = QP_f + R$, con el grado de R menor estrictamente que d; es decir $R = \mu_0 + \mu_1 X + \cdots + \mu_{d-1} X^{d-1}$. Así tenemos:

$$w = H \bullet_f v = (QP_f + R) \bullet_f v = R \bullet_f v =$$
$$= R(f)(v) = \mu_0 v + \mu_1 f(v) + \cdots + \mu_{d-1} f^{d-1}(v).$$

Así pues, los vectores $v, f(v), \ldots, f^{d-1}(v)$, generan el espacio vectorial. Si no fueran independientes, argumentando como en la prueba de la proposición 17, existiría un polinomio S no nulo de grado estrictamente menor que d, tal que $S \bullet_f v = 0$ y entonces S debería ser divisible por el polinomio mínimo P_f, absurdo.

Recíprocamente, la hipótesis dice que todo elemento $w \in V$ es de la forma $w = S \bullet_f v$ y por tanto v genera el $k[X]$-módulo $M_f(E)$. CQD.

Corolario 6. *Dos endomorfismos $f, g \in \mathrm{End}_k(E)$ de tipo cíclico con el mismo polinomio mínimo son conjugados.*

Demostración: Sea $P = P_f = P_g$ el polinomio mínimo común, dado por

$$P = \lambda_0 + \lambda_1 X + \lambda_2 X^2 + \cdots + \lambda_{d-1} X^{d-1} + X^d.$$

Elijamos $v, w \in V$ tales que tenemos dos bases β_f, β_g de E dadas por

$$\begin{aligned} \beta_f &= \{v, f(v), f^2(v), \ldots, f^{d-1}(v)\} = \{v_1, v_2, \ldots, v_d\} \\ \beta_g &= \{w, g(w), g^2(w), \ldots, g^{d-1}(w)\} = \{w_1, w_2, \ldots, w_d\}. \end{aligned}$$

La matriz de f en la base β_f es igual a la matriz de g en la base β_g, dado que

$$\begin{aligned} f(v_1) = v_2 \quad &; \quad g(w_1) = w_2 \\ f(v_2) = v_3 \quad &; \quad g(w_2) = w_3 \\ \cdots \quad &; \quad \cdots \\ f(v_d) = -\sum_{i=1}^{d} \lambda_{i-1} v_i \quad &; \quad g(w_d) = -\sum_{i=1}^{d} \lambda_{i-1} w_i. \end{aligned}$$

En virtud de la observación 3, los endomorfismos f y g están conjugados. CQD.

Observación 4. Sea f endomorfismo de tipo cíclico con polinomio mínimo de grado d y $v \in V$ un generador del $k[X]$-módulo $M_f(E)$. Elijamos una sucesión cualquiera $P_i \in k[X]$ de polinomios tales que el grado de P_i sea exactamente i. Entonces los vectores

$$P_0(f)(v), P_1(f)(v), \ldots, P_{d-1}(f)(v)$$

forman una base del espacio vectorial E.

13. Polinomio mínimo con un sólo factor irreducible

En esta sección consideramos endomorfismos cuyo polinomio mínimo es potencia de un polinomio irreducible. A continuación describimos lo que es una descomposición de Jordan para este tipo de endomorfismos.

Definición 2. *Sea $f \in \mathrm{End}_k(E)$ un endomorfismo tal que $P_f = F^m$, donde F es un polinomio mónico e irreducible de $k[X]$. Una* descomposición de Jordan *de $M_f(E)$ es una expresión $\mathcal{D}$ de V como suma directa interna de $k[X]$-submódulos cíclicos*

$$\mathcal{D}: \quad V = V_1 \oplus V_2 \oplus \cdots \oplus V_s, \tag{1}$$

que cumple que $V_i =< v_i >$ con $v_i \neq 0$ y $\mathrm{Ann}(V_i) = (e_i)$, de manera que e_i divide e_{i+1} para cada $i = 1, 2, \ldots, s-1$.

Por el teorema 3, sabemos que existe al menos una descomposición de Jordan de $M_f(E)$. En esta sección veremos resultados de unicidad para las descomposiciones de Jordan, en particular, veremos que los ideales (e_i) están unívocamente determinados. La lista de ideales (e_i) se llama *lista de divisores elementales del endomorfismo f*.

Nótese que se tiene $\mathrm{Ann}(M_f(E)) = (e_s) = (F^m)$. Más aún, tomando cada e_i mónico, existe un entero n_i tal que $e_i = F^{n_i}$ y la sucesión $\mathbf{n}(\mathcal{D}) = (n_i)_{i=1}^s$ de los n_i es creciente con $n_s = m$, es decir

$$n_1 \leq n_2 \leq n_3 \leq \cdots \leq n_s = m.$$

LEMA 4. *Sea $f \in \mathrm{End}_k(E)$ un endomorfismo de E con $P_f = F^m$ donde F es irreducible de grado a. Consideremos una descomposición de Jordan $\mathcal{D}$ de $M_f(E)$ y escribamos*

$$\mathbf{n}(\mathcal{D}) = (n_1, n_2, \ldots, n_s), \quad n_1 \leq n_2 \leq \cdots \leq n_s = m.$$

Existe una base β del espacio vectorial V tal que la matriz T de f en β es una matriz diagonal por s bloques T_i de la forma:

$$T_i = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ & & & \cdots & & \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -\lambda_0^{(n_i)} & -\lambda_1^{(n_i)} & -\lambda_2^{(n_i)} & \cdots & -\lambda_{n_i a-2}^{(n_i)} & -\lambda_{n_i a-1}^{(n_i)} \end{pmatrix}$$

donde

$$F^{n_i} = \lambda_0^{(n_i)} + \lambda_1^{(n_i)} X + \lambda_2^{(n_i)} X^2 + \cdots + \lambda_{n_i a-2}^{(n_i)} X^{n_i a-2} + \lambda_{n_i a-1}^{(n_i)} X^{n_i a-1} + X^{n_i a},$$

para $i = 1, 2, \ldots, s$.

Demostración: Elijamos para cada V_i un vector v_i tal que $V_i =< v_i >$. Sea $f_i : V_i \to V_i$ el endomorfismo de V_i obtenido por restricción de f. Sabemos que f_i es de tipo cíclico y en virtud de la proposición 21 los vectores $X^n \bullet_f v_i$ con $n = 0, 1, 2, \ldots, an_i - 1$ son una base β_i de V_i en la que la matriz de f_i tiene la forma deseada. CQD.

Sea $f \in \mathrm{End}_k(E)$ un endomorfismo de E con $P_f = F^m$ donde F es irreducible de grado a. Consideremos las dimensiones

$$\ell_n = \dim_k \mathrm{Ker}(F(f)^n); \; n = 0, 1, 2, \ldots.$$

Obsérvese que las dimensiones ℓ_n solamente dependen del endomorfismo f y además forman una sucesión creciente $\boldsymbol{\ell}(f) = (\ell_n)_{n \geq 0}$

$$0 = \ell_0 \leq \ell_1 \leq \ell_2 \leq \ell_3 \leq \cdots \leq \dim_k V.$$

Además la sucesión es estricta hasta el momento anterior a estabilizarse definitivamente, dicho de otro modo, si $\ell_i = \ell_{i+1}$, entonces $\ell_{i+1} = \ell_{i+2}$ (ejercicio).

PROPOSICIÓN 22. *Sea $\mathcal{D}$ una descomposión de Jordan de f. La sucesión $\mathbf{n}(\mathcal{D}) = (n_1, n_2, \ldots, n_s)$ está determinada por la sucesión $\boldsymbol{\ell}(f)$.*

Demostración: En virtud del corolario 5, observamos que para cada entero n se tiene

$$\mathrm{Ker}(F(f)^n) =< F(f)^{n_1'} v_1 > \oplus < F(f)^{n_2'} v_2 > \oplus \cdots \oplus < F(f)^{n_s'} v_s >,$$

donde $n_i' = \max\{0, n_i - n\}$ y, por otro lado $\mathrm{Ann}(< F(f)^{n_i'} v_i >) = (F^{e_i(n)})$, donde $e_i(n) = \min\{n_i, n\}$. Recuérdese que la dimensión de cada $< F(f)^{n_i'} v_i >$ es el grado de su polinomio mínimo, es decir, es igual a $ae_i(n)$. Así pues tenemos que:

$$\ell_n = a(e_1(n) + e_2(n) + \cdots + e_s(n)), \quad n \geq 0. \tag{2}$$

Veamos que estas fórmulas determinan la sucesión de enteros n_i a partir de la sucesión ℓ_n. Denotemos por κ_j el número de submódulos cíclicos $< v_i >$ tales que

$n_i = j$. Nótese que $\kappa_j = 0$, para $j \geq m+1$. El conocimiento de los números κ_j permite recuperar la sucesión de enteros n_i. En efecto

$$(n_1, n_2, \ldots, n_s) = (1, 1, \overset{\kappa_1)}{\ldots}, 1, 2, 2, \overset{\kappa_2)}{\ldots}, 2, 3, 3, \ldots).$$

Por consiguiente, es suficiente determinar los números κ_j a partir de la sucesión $\boldsymbol{\ell}(f)$. La fórmula en la ecuación (2) puede escribirse

$$\begin{aligned}
\ell_1 &= a(\kappa_1 + \kappa_2 + \kappa_3 + \cdots + \kappa_m),\\
\ell_2 &= a(\kappa_1 + 2(\kappa_2 + \kappa_3 + \cdots + \kappa_m)),\\
\ell_3 &= a(\kappa_1 + 2\kappa_2 + 3(\kappa_3 + \cdots + \kappa_m)),\\
\cdots &\quad \cdots \quad \cdots\\
\ell_m &= a(\kappa_1 + 2\kappa_2 + 3\kappa_3 + \cdots + m\kappa_m).
\end{aligned}$$

con $\ell_j = \ell_m$ si $j \geq m$. Observemos que

$$\begin{aligned}
\ell_1/a &= \kappa_1 + \kappa_2 + \cdots + \kappa_m,\\
(\ell_2 - \ell_1)/a &= \kappa_2 + \kappa_3 + \cdots + \kappa_m,\\
(\ell_3 - \ell_2)/a &= \kappa_3 + \kappa_4 + \cdots + \kappa_m\\
&\cdots \quad \cdots \quad \cdots\\
(\ell_m - \ell_{m-1})/a &= \kappa_m,
\end{aligned}$$

Ahora, las fórmulas

$$\kappa_i = \frac{1}{a}\left(2\ell_i - \ell_{i-1} - \ell_{i+1}\right), \quad i \geq 1,\ (\ell_0 = 0)$$

permiten determinar los números $\kappa_1, \kappa_2, \ldots, \kappa_m$ a partir de la sucesión $\boldsymbol{\ell}(f)$. CQD.

Como corolario de los resultados anteriores, tenemos el siguiente teorema de unicidad

TEOREMA 4. *Sean $f, g \in \mathrm{End}_k(E)$ con el mismo polinomio mínimo*

$$P_f = P_g = F^m,$$

donde $F \in k[X]$ es irreducible. Consideremos dos descomposiciones de Jordan $\mathcal{D}$ y $\mathcal{D}'$ de $M_f(E)$ y $M_g(E)$ respectivamente. Son equivalentes

1. $\mathbf{n}(\mathcal{D}) = \mathbf{n}(\mathcal{D}')$.
2. *Los endomorfismos f y g son conjugados (es decir, los módulos $M_f(E)$ y $M_g(E)$ son isomorfos).*

Demostración: Supongamos que $\mathbf{n}(\mathcal{D}) = \mathbf{n}(\mathcal{D}')$. Sabemos por el lema 4 que se puede dar una base para f, respectivamente para g, cuya matriz solo depende del conocimiento de F y la sucesión $\mathbf{n}(\mathcal{D})$, respectivamente $\mathbf{n}(\mathcal{D}')$. Dado que $\mathbf{n}(\mathcal{D}) = \mathbf{n}(\mathcal{D}')$, las matrices obtenidas para f y para g son las mismas y, por tanto f y g son conjugados, véase la observación 3.

Supongamos que $M_f(E)$ y $M_g(E)$ son $k[X]$-módulos isomorfos mediante un isomorfismo $\phi : V \to V$. El isomorfismo ϕ produce una descomposición

$$\mathcal{D}(\phi) : V = \phi(V_1) \oplus \phi(V_2) \oplus \cdots \oplus \phi(V_s)$$

que es una descomposición de Jordan de $M_g(E)$, potencialmente distinta de $\mathcal{D}'$, pero tal que $\mathbf{n}(\mathcal{D}(\phi)) = \mathbf{n}(\mathcal{D})$. Por otro lado, tenemos que $\mathbf{n}(\mathcal{D}(\phi)) = \mathbf{n}(\mathcal{D}')$, aplicando la proposición 22, pues ambas sucesiones están determinadas del mismo modo por la lista $\boldsymbol{\ell}(g)$. CQD.

14. Teorema de Jordan

Consideremos un endomorfismo $f \in \mathrm{End}_k(E)$ y sea

$$\mathrm{Ann}(M_f(E)) = (F_1^{m_1} F_2^{m_2} \cdots F_t^{m_t}),$$

donde cada F_i es mónico e irreducible, con $F_i \neq F_j$ si $i \neq j$ y cada $m_i \geq 1$ para $i = 1, 2, \ldots, t$. Por la proposición 19, tenemos una descomposición única en subespacios vectoriales invariantes

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_t$$

tal que si $f_i \in \mathrm{End}_k(W_i)$ está inducido por f, se tiene que $\mathrm{Ann}(M_{f_i}(W_i)) = (F_i^{m_i})$. Ahora sabemos que para cada $i = 1, 2, \ldots, t$, existe una descomposición de Jordan de W_i

$$W_i = V_{i1} \oplus V_{i2} \oplus \cdots \oplus V_{is_i},$$

donde cada $V_{ij} =< v_{ij} >$ y se tiene que

$$\mathrm{Ann}(v_{ij}) = (F_i^{n_{ij}}), \quad 1 \leq n_{i1} \leq n_{i2} \leq \cdots \leq n_{is_i} = m_i.$$

La familias de ideales $\{(F_i^{n_{ij}})\}_{i,j}$, para $i = 1, 2, \ldots, t$, $j = 1, 2, \ldots, s_i$, recibe el nombre de *familia de divisores elementales* del endomorfismo f; es decir, los divisores elementales de f se obtienen como reunión de los divisores elementales de cada restricción f_i de f a W_i. Así, el espacio vectorial E es suma directa interna de subespacios invariantes cíclicos.

$$V = \oplus_{ij} < v_{ij} >, \quad \mathrm{Ann}(v_{ij}) = (F_i^{n_{ij}}).$$

De los resultados anteriores, se sigue el teorema de clasificación de Jordan

Teorema 5 (Jordan). *Dos endomorfismos $f, g \in \mathrm{End}_k(E)$ son conjugados si y solamente si tienen el mismo polinomio mínimo y la misma familia de divisores elementales.*

Demostración: Si f y g están conjugados los $k[X]$-módulos $M_f(E)$ y $M_g(E)$ son isomorfos y por consiguiente tienen el mismo polinomio mínimo y los mismos divisores elementales.

Para probar el recíproco, basta recordar que el conocimiento de P_f y de los divisores elementales permite dar unívocamente una matriz que representa f en alguna base. Esta construcción es común para g, lo que termina la demostración.

CQD.

15. Factores invariantes de un endomorfismo

Sea $f \in \mathrm{End}_k(E)$ un endomorfismo. Por el teorema 3, existe una descomposición de $M_f(E)$ en suma directa interna de submódulos cíclicos

$$\mathcal{D}: \quad V =< v_1 > \oplus < v_2 > \oplus \cdots \oplus < v_s >; \quad \mathrm{Ann}(< v_j >) = (e_j),\ j = 1, 2, \ldots, s,$$

tal que $(1) \neq (e_1) \supset (e_2) \supset \cdots \supset (e_s)$. Diremos que $\mathcal{D}$ es una descomposición de Smith para f y que la familia de ideales $\{(e_j)\}_{j=1}^s$ es la *familia de factores invariantes de $\mathcal{D}$*.

Supongamos que $P_f = F_1^{m_1} F_2^{m_2} \cdots F_t^{m_t}$ donde cada F_i es mónico e irreducible y que $\mathcal{D}$ es una descomposición de Smith para f. Como los anuladores (e_j) contienen cada uno al siguiente, podemos tomar cada e_j mónico de la forma:

$$e_j = F_1^{m_{1j}} F_2^{m_{2j}} \cdots F_t^{m_{tj}},$$

donde $0 \leq m_{i1} \leq m_{i2} \leq \cdots \leq m_{is} = m_i$, para $i = 1, 2, \ldots, t$.

Tenemos el siguiente resultado de unicidad:

TEOREMA 6. *Sean $f, f' \in \mathrm{End}_k(E)$ dos endomorfismos de E y sean $\mathcal{D}$, $\mathcal{D}'$ descomposiciones de Smith respectivas para f y f'. Son equivalentes:*

(1) *f y f' son endomorfismos conjugados.*
(2) *Las familias de factores invariantes de $\mathcal{D}$ y $\mathcal{D}'$ son iguales.*

Demostración: Si se cumple la propiedad (2), tenemos que $s = s'$ y que cada $< v_j >$ asociado a $\mathcal{D}$ es isomorfo al correspondiente $< v'_j >$ asociado a $\mathcal{D}'$. Por consiguiente, los $k[X]$-módulos $M_f(E)$ y $M_{f'}(E)$ son isomorfos y por tanto f y f' son conjugados.

Recíprocamente, supongamos que se cumple la propiedad (1). Argumentando como en la prueba del Teorema 4, podemos reducirnos al caso en el que $f = f'$. Supongamos que $P_f = F_1^{m_1} F_2^{m_2} \cdots F_t^{m_t}$ donde cada F_i es mónico e irreducible. Por la proposición 19, sabemos que existe una descomposición

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_t,$$

donde cada W_i es el núcleo de la homotecia $\phi_i : V \to V$ de razón $F_i^{m_i}$.

Aplicando el Corolario 5, obtenemos a partir de $\mathcal{D}$ una descomposición:

$$W_i = W_i \cap V = (W_i \cap < v_1 >) \oplus (W_i \cap < v_2 >) \oplus \cdots \oplus (W_i \cap < v_s >),$$

para cada $1 \leq i \leq t$, de modo que para cada $1 \leq j \leq s$ se tiene que

$$W_i \cap < v_j > = < w_{ij} >,$$

donde el anulador de w_{ij} es el máximo común divisor de $F_i^{m_i}$ y el anulador e_j de v_j. Como tenemos que

$$e_j = F_1^{m_{1j}} F_2^{m_{2j}} \cdots F_t^{m_{tj}}, \quad m_{ij} \leq m_i,$$

se concluye que $\mathrm{Ann}(w_{ij}) = (F_i^{m_{ij}})$. En conclusión, tenemos que

$$W_i = < w_{i1} > \oplus < w_{i2} > \oplus \cdots \oplus < w_{is} >,$$

donde los anuladores contienen cada uno al siguiente y el anulador de W_i es $F_i^{m_i}$, con lo que podemos utilizar los resultados de la sección 13. Entonces una descomposición de Jordan de W_i está dada por

$$W_i = < w_{i,s-s_i+1} > \oplus < w_{i,s-s_i+2} > \oplus \cdots \oplus < w_{i,s} >, \quad w_{i,s} = w_{i,s-s_i+s_i},$$

donde el índice s_i está definido por la propiedad

$$0 = m_{i,1} = m_{i,2} = \cdots = m_{i,s-s_i} < m_{i,s-s_i+1}.$$

Ahora podemos repetir el mismo procedimiento a partir de $\mathcal{D}'$. Los resultados de unicidad de la sección 13 nos dicen que $s'_i = s_i$ y que para cada $1 \leq k \leq s_i$ tenemos que $m'_{i,s-s_i+k} = m_{i,s-s_i+k}$. En consecuencia $m'_{ij} = m_{ij}$, para todo i, j. CQD.

La *lista de factores invariantes del endomorfismo f* es, por definición, la lista de factores invariantes de cualquier descomposición de Smith para f.

16. El teorema de Cayley-Hamilton

Dada una matriz cuadrada T de dimensión $m \times m$ con coeficientes en un cuerpo k, el *polinomio característico* $P_T^{\mathfrak{c}}$ *de la matriz* T se define como el determinante

$$P_T^{\mathfrak{c}} = \det(XI_m - T) \in k[X].$$

Es un polinomio mónico de grado m. Si Q es una matriz invertible, tenemos que

$$P_{QTQ^{-1}}^{\mathfrak{c}} = \det(Q(XI_m - T)Q^{-1}) = \det(XI_m - T) = P_T^{\mathfrak{c}}.$$

Por consiguiente, el polinomio característico es el mismo para dos matrices cuadradas conjugadas, es decir que representan el mismo endomorfismo en distintas bases. Así pues, podemos hablar del *polinomio característico* $P_f^{\mathfrak{c}}$ de un endomorfismo dado $f \in \mathrm{End}_k(E)$, que será $P_f^{\mathfrak{c}} = P_T^{\mathfrak{c}}$, donde T es una matriz que representa f en alguna base.

Teorema 7 (Cayley-Hamilton). *Dado* $f \in \mathrm{End}_k(E)$ *se tiene que*

$$P_f^{\mathfrak{c}} \in \mathrm{Ann}(M_f(E)).$$

Es decir, el polinomio mínimo P_f *divide el polinomio característico* $P_f^{\mathfrak{c}}$*. Además todo factor irreducible del polinomio característico lo es también del polinomio mínimo.*

Para probar este resultado usaremos las descomposiciones que ya conocemos.

Lema 5. *Consideremos un endomorfismo* $f \in \mathrm{End}_k(E)$*. Supongamos que se tiene una suma directa interna* $V = V_1 \oplus V_2$ *donde* V_1 *y* V_2 *son subespacios vectoriales invariantes. Denotemos* $f_i : V_i \to V_i$ *los endomorfismos correspondientes obtenidos de* f *por restricción, para* $i = 1, 2$*. Entonces tenemos que*

$$P_f^{\mathfrak{c}} = P_{f_1}^{\mathfrak{c}} P_{f_2}^{\mathfrak{c}}.$$

Demostración: Consideremos una base β de V formada por la unión $\beta = \beta_1 \cup \beta_2$ de una base β_1 de V_1 y una base β_2 de V_2. La matriz T de f en la base β está formada por bloques T_1 y T_2, donde T_i es la matriz de f_i en la base β_i, para $i = 1, 2$. Se tiene

$$T = \left(\begin{array}{c|c} T_1 & 0 \\ \hline 0 & T_2 \end{array}\right), \quad XI_m - T = \left(\begin{array}{c|c} XI_{m_1} - T_1 & 0 \\ \hline 0 & XI_{m_2} - T_2 \end{array}\right).$$

En consecuencia $\det(XI_m - T) = \det(XI_{m_1} - T_1)\det(XI_{m_2} - T_2)$. CQD.

Supongamos ahora que la descomposición del polinomio mínimo como producto de potencias de polinomios mónicos irreducibles y distintos dos a dos se escribe

$$P_f = F_1^{m_1} F_2^{m_2} \cdots F_t^{m_t}.$$

Sabemos que se tiene una suma directa interna en subespacios invariantes

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_t; \quad f_i : W_i \to W_i,$$

de manera que $P_{f_i} = F_i^{m_i}$, para $i = 1, 2, \ldots, t$. Como consecuencia del lema anterior y a la vista de esta observación, es suficiente hacer la prueba del teorema en el caso en el que el polinomio mínimo tenga la forma F^m, donde F es un polinomio mónico irreducible.

Supongamos pues que el polinomio mínimo es una potencia de un polinomio mónico irreducible $P_f = F^m$. Tenemos una descomposición en submódulos cíclicos

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_s; \quad f_j : V_j \to V_j,$$

donde el polinomio mínimo de f_j es F^{n_j}, con $n_1 \leq n_2 \leq \cdots \leq n_s$ y además $n_s = m$. Si vemos que el polinomio característico de cada f_j es $P^{\mathbf{c}}_{f_j} = F^{n_j}$, hemos terminado, pues en ese caso se tiene

$$P^{\mathbf{c}}_f = \prod_{j=1}^{s} F^{n_j}; \quad P_f = F^m = F^{n_s}.$$

Así pues, para terminar es suficiente probar el siguiente resultado

PROPOSICIÓN 23. *Si $f \in \mathrm{End}_k(E)$ es de tipo cíclico, entonces $P_f = P^{\mathbf{c}}_f$.*

Demostración: Supongamos que $P = \lambda_0 + \lambda_1 X + \cdots + \lambda_{n-1}X^{n-1} + X^n$ es el polinomio mínimo. Existe un vector no nulo $v \in V$ de modo que se tiene una base de V dada por

$$v, f(v), f^2(v), \ldots, f^{n-1}(v).$$

En esta base, el endomorfismo f tiene una matriz T de la forma

$$T = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ & & & \cdots & & \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -\lambda_0 & -\lambda_1 & -\lambda_2 & \cdots & -\lambda_{n-2} & -\lambda_{n-1} \end{pmatrix}$$

Se concluye que $\det(XI_n - T) = P$. CQD.

OBSERVACIÓN 5. De la construcción anterior se deduce que todo divisor irreducible del polinomio característico también es un divisor del polinomio mínimo. Se deja como ejercicio al lector.

17. Formas canónicas de Jordan

Ahora podemos interesarnos en un método práctico para obtener los invariantes completos anteriores de la clase de conjugación de un endomorfismo $f \in \mathrm{End}_k(E)$ y, eventualmente, una matriz "canónica" para f, en la que se evidencien dichos invariantes. Esta matriz puede obtenerse a partir de la descomposición del espacio vectorial E como suma directa de subespacios invariantes de tipo cíclico

$$V = \oplus_{ij} < v_{ij} >, \quad \mathrm{Ann}(v_{ij}) = (F_i^{n_{ij}}).$$

En efecto, podemos elegir bases de cada $< v_{ij} >$ que producirán matrices T_{ij}, cuyos coeficientes están determinados por los divisores elementales $F_i^{n_{ij}}$. La matriz T de f en la union de dichas bases, tiene las T_{ij} como bloques. Esto se puede hacer de muchas formas, siguiendo la observación 4. Comentaremos dos de ellas, en las cuales queda evidenciado el divisor elemental $F_i^{n_{ij}}$:

Primera forma. Escribimos

$$F_i^{n_{ij}} = \lambda_0 + \lambda_1 X + \cdots + \lambda_{n_{ij}a_i - 1}X^{n_{ij}a_i - 1} + X^{n_{ij}a_i}.$$

y tomamos la base de $< v_{ij} >$ dada por $v_{ij}, f(v_{ij}), \ldots, f^{n_{ij}a_i-1}(v_{ij})$. Se obtiene la matriz

$$T_{ij} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ & & & \cdots & & \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ -\lambda_0 & -\lambda_1 & -\lambda_2 & \cdots & -\lambda_{n_{ij}a_i-2} & -\lambda_{n_{ij}a_i-1} \end{pmatrix}$$

Segunda forma. Escribimos

$$F_i = \mu_0 + \mu_1 X + \cdots + \mu_{a_i-1} X^{a_i-1} + X^{a_i}.$$

Ahora consideramos la k-base de $< v_{ij} >$ dada por

$$\begin{array}{cccc} v_{ij}, & f(v_{ij}), & \ldots, & f^{a_i-1}(v_{ij}), \\ F_i(f)(v_{ij}), & f(F_i(f)(v_{ij})), & \ldots, & f^{a_i-1}(F_i(f)(v_{ij})) \\ F_i(f)^2(v_{ij}), & f(F_i(f)^2(v_{ij})) & \ldots, & f^{a_i-1}(F_i(f)^2(v_{ij})) \\ \cdots & \cdots & \cdots & \cdots \\ F_i(f)^{n_{ij}-1}(v_{ij}), & f(F_i(f)^{n_{ij}-1}(v_{ij})), & \ldots, & f^{a_i-1}(F_i(f)^{n_{ij}-1}(v_{ij})). \end{array}$$

Ejercicio: Escribir la matriz T'_{ij} correspondiente.

Un caso interesante es cuando $F_i = X - \lambda$, nótese que éste es el caso siempre que se tiene un cuerpo algebraicamente cerrado. En este caso, la matriz T'_{ij} correspondiente es un bloque $n_{ij} \times n_{ij}$ de la forma

$$T'_{ij} = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ & & & \cdots & & \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}.$$

Así pues, si conocemos el polinomio mínimo y la familia de divisores elementales, podemos escribir "formas canónicas para la matriz".

Veamos cómo conocer el polinomio mínimo y la familia de divisores elementales a partir de una matriz T que represente el endomorfismo f. El primer dato al que tenemos acceso es el polinomio característico

$$P_f^{\mathfrak{c}} = \det(XI_m - T).$$

Se trata de un polinomio mónico divisible por el polinomio mínimo P_f y que además tiene la propiedad de que todo factor irreducible de $P_f^{\mathfrak{c}}$ es asimismo un factor irreducible de P_f. Es decir, tenemos

$$P_f = F_1^{m_1} F_2^{m_2} \cdots F_t^{m_t},$$

donde cada F_i es mónico e irreducible, de grado $a_i \geq 1$ y cada $m_i \geq 1$, para $i = 1, 2, \ldots, t$. Por otro lado, el polinomio característico se escribe

$$P_f^{\mathfrak{c}} = F_1^{c_1} F_2^{c_2} \cdots F_t^{c_t},$$

donde $c_i \geq m_i$ para cada $i = 1, 2, \ldots, t$ y además

$$\text{grado}(P_f^{\mathfrak{c}}) = \sum_{i=1}^{t} a_i c_i = \dim_k E.$$

Ahora nos gustaría determinar los exponentes m_i. Sabemos que $1 \leq m_i \leq c_i$ para todo $i = 1, 2, \ldots, t$. Tenemos la sucesión creciente de núcleos

$$\{0\} \subset \mathrm{Ker}F_i(f) \subset \mathrm{Ker}F_i(f)^2 \subset \mathrm{Ker}F_i(f)^3 \subset \cdots,$$

nótese que todos ellos son subespacios vectoriales invariantes por f, o lo que es lo mismo, submódulos de $M_f(E)$.

LEMA 6. *El exponente m_i está determinado por las siguientes propiedades*

(1) *Para cada $0 \leq \ell \leq m_i - 1$, se tiene $\mathrm{Ker}F_i(f)^\ell \neq \mathrm{Ker}F_i(f)^{\ell+1}$.*
(2) *Para cada $m_i \leq \ell$, se tiene $\mathrm{Ker}F_i(f)^\ell = \mathrm{Ker}F_i(f)^{\ell+1}$.*

Demostración: En virtud de la proposición 19, tenemos una descomposición en subespacios invariantes

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_t$$

tales que $W_i = \mathrm{Ker}(F_i(f)^{m_i})$ y $\mathrm{Ann}(W_i) = (F_i^{m_i})$ para cada $i = 1, 2, \ldots, t$.

Dado $j \neq i$, consideremos el endomorfismo $F_i(f)_{|W_j} : W_j \to W_j$. Se tiene que:

$$\mathrm{Ker}\left(F_i(f)_{|W_j}\right) = \mathrm{Ker}F_i(f) \cap W_j \subset W_i \cap W_j = \{0\}.$$

Esto significa que $F_i(f)_{|W_j}$ es un endomorfismo inyectivo de W_j y por dimensionalidad, es un isomorfismo vectorial. Por ende $F_i(f)^\ell_{|W_j}$ también es isomorfismo para todo $\ell \geq 0$. Veamos ahora que

$$\mathrm{Ker}F_i(f)^\ell = W_i, \text{ para todo } \ell \geq m_i.$$

Ya sabemos que $W_i \subset \mathrm{Ker}F_i(f)^\ell = \mathrm{Ker}\left(F_i(f)^{\ell-m_i} \circ F_i(f)^{m_i}\right)$. Dado $v \in V$, escribamos $v = \sum_j w_j$, con $w_j \in W_j$. Se tiene

$$F_i(f)^\ell(v) = \sum_{j \neq i} F_i(f)^\ell(w_j), \quad F_i(f)^\ell(w_j) \in W_j.$$

Si $F_i(f)^\ell(v) = 0$, entonces $F_i(f)^\ell(w_j) = 0$ para cada $j \neq i$ y así $w_j = 0$, para cada $j \neq i$, dado que $F_i(f)^\ell_{|W_j}$ es un isomorfismo. Esto implica que $v \in W_i$. La afirmación (2) queda probada.

Si $\mathrm{Ker}F_i(f)^\ell = \mathrm{Ker}F_i(f)^{\ell+1}$, también tenemos que $\mathrm{Ker}F_i(f)^{\ell+1} = \mathrm{Ker}F_i(f)^{\ell+2}$ y finalmente $\mathrm{Ker}F_i(f)^\ell = \mathrm{Ker}F_i(f)^{m_i} = W_i$. En particular $F_i(f)^\ell$ anula todos los elementos de W_i, lo que implica que el polinomio mínimo $F_i^{m_i}$ divide F_i^ℓ y por consiguiente $\ell \geq m_i$. Por tanto, si $\ell < m_i$ se tiene $\mathrm{Ker}F_i(f)^\ell \neq \mathrm{Ker}F_i(f)^{\ell+1}$. CQD.

Gracias al lema anterior, quedan determinados los exponentes m_i sin más que calcular la dimensiones de los núcleos sucesivos y observar en qué momento se estabilizan. De este modo podemos calcular el polinomio mínimo, así como la descomposición

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_t,$$

puesto que $W_i = \mathrm{Ker}F_i(f)^{m_i} = \mathrm{Ker}F_i(f)^{c_i}$.

Ahora podemos trabajar en cada W_i, que está dotado del endomorfismo f_i obtenido por restricción de f y así reducirnos al caso de que el polinomio mínimo, o el característico, sean potencia de un polinomio mónico irreducible. Concretamente, sabemos que $P_{f_i} = F_i^{m_i}$. Para calcular la familia $\{(F_i^{n_{ij}})\}$ de divisores elementales, procedemos de acuerdo con la prueba de la proposición 22. Más precisamente, calculamos las dimensiones

$$\ell_{in} = \dim_k \mathrm{Ker}(F_i(f)^n);\ n = 0, 1, 2, \ldots.$$

Para calcular los exponentes n_{ij}, primero calculamos los números κ_{ij} definidos por las fórmulas:

$$\kappa_{ij} = \frac{1}{a_i}\left(2\ell_{ij} - \ell_{i,j-1} - \ell_{i,j+1}\right), \quad j \geq 1, \ (\ell_{i0} = 0), \quad a_i = \text{grado}(F_i).$$

Teniendo en cuenta que:

$$(n_{i1}, n_{i2}, \ldots) = (1, 1, \overset{\kappa_{i1})}{\ldots}, 1, 2, 2, \overset{\kappa_{i2})}{\ldots}, 2, 3, 3, \ldots).$$

se tiene que $n_{ij} = d$ si y sólo si $\kappa_{i1} + \kappa_{i2} + \cdots \kappa_{i,d-1} < j \leq \kappa_{i1} + \kappa_{i2} + \cdots \kappa_{id}$.

Observación 6. Basta calcular las dimensiones ℓ_{in} hasta $n = m_i$, ya que $\ell_{in} = \ell_{i,m_i}$, para todo $n \geq m_i$. Del mismo modo, los números κ_{ij} sólo necesitan ser calculados hasta $j = m_i$, pues $\kappa_{ij} = 0$, para todo $j \geq m_i$. Recuérdese asimismo que $n_{ij} \leq m_i$ para todo j.

18. Bases de Jordan

Sabemos obtener el polinomio mínimo y la familia de divisores elementales a partir de una matriz T que represente el endomorfismo f, y dar matrices canónicas que lo representen en una base adecuada. No obstante, todavía no hemos dado un método sistemático para obtener dichas bases. Más precisamente, no hemos indicado cómo obtener los vectores v_{ij} generadores de los correspondientes módulos cíclicos.

Dado que los espacios invariantes W_i son fáciles de calcular como

$$W_i = \text{Ker}F_i(f)^{m_i} = \text{Ker}F_i(f)^{c_i},$$

nos restringiremos al caso en el que el polinomio mínimo sea potencia de un polinomio irreducible $P_f = F^m$. En este caso, la descomposición en suma directa de cíclicos surge de la forma normal de Smith de una matriz, como ya sabemos. Recordemos cómo se puede proceder.

Consideramos el $k[X]$-módulo $M_f(E)$. Seleccionamos una k-base $\beta = \{w_r\}_{r=1}^d$ de E en la cual f tiene la matriz $T = (t_{rs})$. Esta base da un sistema de generadores del $k[X]$-módulo $M_f(E)$ y así tenemos un morfismo suprayectivo de $k[X]$-módulos

$$\phi : k[X]^d \to V$$

tal que $\phi(\mathbf{e}_r^d) = w_r$, para $r = 1, 2, \ldots, d$. Ahora necesitamos encontrar el núcleo $\text{Ker}\phi$. Los elementos σ_r definidos por

$$\sigma_r = X\mathbf{e}_r^d - \sum_{s=1}^{d} t_{rs}\mathbf{e}_s^d, \quad r = 1, 2, \ldots, d,$$

están manifiestamente en el núcleo de ϕ. Más aún, tenemos el siguiente lema

Lema 7. $\text{Ker}\phi =< \sigma_r; \ r = 1, 2, \ldots, d >$.

Demostración:
Todo $\sigma \in k[X]^d$ no nulo, se puede escribir

$$\sigma = \sum_{j=0}^{\delta} X^j \sum_{i=1}^{d} \lambda_{ij}\mathbf{e}_i^d,$$

donde $\lambda_{ij} \in k$ y existe un i tal que $\lambda_{i\delta} \neq 0$. Diremos que δ es el grado de σ. Por convención, diremos que el grado de $\sigma = 0$ es -1.

Denotemos $K =< \sigma_r;\ r = 1, 2, \ldots, d >$. Dado $\sigma \in \mathrm{Ker}\phi$, probaremos que $\sigma \in K$ por inducción sobre el grado δ de σ. Si $\delta = -1$, el resultado es evidente. Suponemos por inducción que el resultado es cierto para σ' con grado $\delta' < \delta$. Consideremos

$$\sigma' = \sigma - X^{\delta-1} \sum_{i=1}^{d} \lambda_{i\delta} \sigma_i.$$

Tenemos que $\sigma' \in \mathrm{Ker}\phi$ y además su grado $\delta' < \delta$. Aplicando inducción, $\sigma' \in K$ y por consiguiente

$$\sigma = \sigma' + X^{\delta-1} \sum_{i=1}^{d} \lambda_{i\delta} \sigma_i \in K.$$

Esto termina la prueba CQD.

Ahora podemos considerar el morfismo ψ de $k[X]$-módulos definido por

$$\psi : k[X]^d \to k[X]^d; \quad \psi(\mathbf{e}_r^d) = \sigma_r,\ r = 1, 2, \ldots, d.$$

Tenemos que $\mathrm{Im}\psi = \mathrm{Ker}\phi$, así pues

$$k[X]^d \overset{\psi}{\to} k[X]^d \overset{\phi}{\to} V$$

es una "presentación" del $k[X]$-módulo $M_f(E)$. Ahora aplicamos el teorema de Smith y tenemos isomorfismos de $k[X]$-módulos $\alpha, \beta : k[X]^d \to k[X]^d$ tales que si $\tilde{\psi} = \beta \circ \psi \circ \alpha^{-1}$ se tiene

$$\tilde{\psi}(\mathbf{e}_r^d) = F^{\tilde{n}_r} \mathbf{e}_r^d,$$

donde $0 \leq \tilde{n}_1 \leq \tilde{n}_2 \leq \cdots \leq \tilde{n}_d = m$. Escribamos $n_i = \tilde{n}_{i+d-s}$, donde $\tilde{n}_{1+d-s}$ es el primer exponente no nulo. El teorema de descomposición en módulos cíclicos, nos permite concluir que

$$V =< v_1 > \oplus < v_2 > \oplus \cdots \oplus < v_s >,\ \mathrm{Ann}(v_i) = F^{n_i},$$

donde $v_i = \phi \circ \beta^{-1}(\mathbf{e}_{i+d-s}^d)$. Esto nos permite encontrar la base deseada.

Una observación muy importante es que la matriz de ψ es precisamente la matriz característica $XI_d - T$. Los divisores elementales podrían, de este modo, obtenerse a partir de los máximos comunes divisores de los menores de la matriz característica de acuerdo con la nota 1.

19. Apéndice

Presentamos aquí otro método para encontrar los generadores de los submódulos cíclicos correspondientes a los divisores elementales, para el caso de un endomorfismo $f \in \mathrm{End}_k(E)$ cuyo polinomio mínimo se escribe

$$P_f(X) = (X - \lambda)^m.$$

Observación 7. Después de aplicar el corolario 3 a $M_f(E)$, sabemos cómo reducirnos al caso de un polinomio mínimo que es potencia de un irreducible. Así pues, el caso que vamos a tratar cubre completamente la situación para un cuerpo algebraicamente cerrado, en el que todos los polinomios irreducibles tienen grado uno. Por ejemplo, cuando el cuerpo es el de los números complejos.

Consideremos el endomorfismo $h = f - \lambda \operatorname{Id} : V \to V$. Es decir

$$h(v) = (X - \lambda) \bullet_f v = f(v) - \lambda v.$$

Denotemos $K_i = \operatorname{Ker} h^i$, para $i = 0, 1, \ldots, m$. Tenemos una sucesión encajada de núcleos

$$\{0\} = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_m = V.$$

Nótese que $h(K_{i+1}) \subset K_i$ y por tanto tenemos una aplicación lineal por restricción, que denotaremos del mismo modo $h : K_{i+1} \to K_i$. Es decir, la aplicación lineal h induce una serie de aplicaciones lineales

$$\{0\} \xleftarrow{h} K_1 \xleftarrow{h} K_2 \xleftarrow{h} \ldots \xleftarrow{h} K_{m-1} \xleftarrow{h} K_m = V.$$

Sabemos que existe un vector $v_m^{1m} \in K_m \setminus K_{m-1}$. Denotemos

$$v_i^{1m} = h^{m-i}(v_m^{1m}) \in K_i, \quad i = 1, 2, \ldots, m.$$

Nótese que $v_i^{1m} \neq 0$, para $i = 1, 2, \ldots, m$. En efecto, sabemos que

$$v_1^{1m} = h^{m-1}(v_m^{1m}) \neq 0.$$

Entonces $0 \neq v_1^{1m} = h^{i-1}(v_i^{1m})$, luego $v_i^{1m} \neq 0$, para $i = 1, 2, \ldots, m$.

Consideremos ahora un subespacio vectorial $K_1^{1m} \subset K_1$ complementario de $L(v_1^{1m})$ en K_1, es decir, tenemos la suma directa interna

$$K_1 = L(v_1^{1m}) \oplus K_1^{1m}.$$

Ahora consideramos los subespacios vectoriales $K_i^{1m} \subset K_i$ definidos por

$$K_i^{1m} = (h^{i-1})^{-1}(K_1^{1m}) \cap K_i; \quad i = 1, 2, \ldots, m.$$

LEMA 8. *Se tienen las siguientes propiedades*

(1) $K_i = L(v_i^{1m}) \oplus K_i^{1m}$, *para* $i = 1, 2, \ldots, m$.
(2) $h^{i-j}(K_i^{1m}) \subset K_j^{1m}$, *para* $1 \leq j < i \leq m$.
(3) $K_j^{1m} \subset K_i^{1m}$, *para* $1 \leq j < i \leq m$.

Demostración: Para probar (1), consideremos $\lambda v_i^{1m} \in L(v_i^{1m})$. Si tenemos que $\lambda v_i^{1m} \in K_i^{1m}$, esto implica que $h^{i-1}(\lambda v_i^{1m}) \in K_1^{1m}$, es decir

$$h^{i-1}(\lambda v_i^{1m}) = \lambda h^{i-1}(v_i^{1m}) = \lambda v_1^{1m} \in K_1^{1m}.$$

Se sigue que $\lambda = 0$, ya que $K_1 = L(v_1^{1m}) \oplus K_1^{1m}$. Tomemos ahora un elemento cualquiera $v \in K_i$. Escribamos

$$h^{i-1}(v) = \lambda v_1^{1m} + w, \quad w \in K_1^{1m}.$$

Entonces $v - \lambda v_i^{1m} \in K_i^{1m}$ ya que $h^{i-1}(v - \lambda v_i^{1m}) = w \in K_1^{1m}$. Así pues, podemos escribir

$$v = \lambda v_i^{1m} + (v - \lambda v_i^{1m}) \in L(v_i^{1m}) + K_i^{1m}.$$

Esto completa la prueba de (1). La afirmación (2) se sigue de la definición de los subespacios K_i^{1m}. La afirmación (3) es consecuencia de que

$$h^{i-1}(v) = 0, \text{para cada } v \in K_j, \text{con } 1 \leq j < i \leq m,$$

dado que $j \leq i - 1$, recordando que $K_j = \operatorname{Ker} h^j$. CQD.

Ahora tenemos una sucesión encajada

$$\{0\} \subset K_1^{1m} \subset K_2^{1m} \subset \ldots \subset K_m^{1m} \subset K_m = V,$$

para la cual la aplicación lineal h induce una serie de aplicaciones lineales

$$\{0\} \xleftarrow{h} K_1^{1m} \xleftarrow{h} K_2^{1m} \xleftarrow{h} \ldots \xleftarrow{h} K_{m-1}^{1m} \xleftarrow{h} K_m^{1m} \subset K_m = V.$$

Podemos buscar un elemento $v_m^{2m} \in K_m^{1m} \setminus K_{m-1}^{1m}$, si existe. En este caso definimos como antes $v_i^{2m} = h^{i-1}(v_m^{2m})$ para $i = 1, 2, \ldots, m$ y planteamos una descomposición

$$K_1^{1m} = L(v_1^{2m}) \oplus K_1^{2m}.$$

Definimos $K_i^{2m} = h^{i-1}(K_1^{2m}) \subset K_i^{1m}$. Tenemos una situación similar a la vista en el lema anterior. Contimuamos de esta manera y así obtenemos elementos y subespacios

$$v_i^{jm} \in K_i^{j-1m}; \quad K_i^{jm} \subset K_i^{j-1m},$$

para $1 = 1, 2, \ldots, m$; $j = 1, 2, \ldots, t_m$. Además, en algún momento, digamos para $j = t_m$ no podemos continuar, por razones dimensionales, es decir, que se tiene $K_{m-1}^{t_m m} = K_m^{t_m m}$. En este momento trabajamos con la sucesión más corta

$$\{0\} \subset K_1^{t_m m} \subset K_2^{t_m m} \subset \ldots \subset K_{m-1}^{t_m m} = K_m^{t_m m}.$$

Repetimos el proceso y entonces tenemos

$$v_i^{j\ell} \in K_i^{j-1\ell}; K_i^{j\ell} \subset K_i^{j-1\ell},$$

para $\ell = 1, 2, \ldots, m$, $i = 1, 2, \ldots, \ell$, $j = 1, 2, \ldots, t_m$. De todo este proceso se puede comprobar que se ha obtenido una decomposición del espacio V en suma directa

$$V = < v_m^{1m} > \oplus < v_m^{2m} > \oplus \cdots < v_1^{t_1 1} >,$$

donde

$$< v_\ell^{j\ell} >= L(\{v_\ell^{j\ell}, v_{\ell-1}^{j\ell}, \ldots, v_1^{j\ell}\}) = L(\{v_\ell^{j\ell}, h(v_\ell^{j\ell}), \ldots, h^{\ell-1}(v_\ell^{j\ell})\}),$$

que es la descomposición buscada.

Este método de encontrar la base que evidencia los divisores elementales es una alternativa al cálculo de la matriz de Smith. Aunque su desarrollo teórico parezca largo, en muchos casos prácticos de pequeña dimensión resulta conveniente.