

0.1. Teorema de estructura de módulos finitamente generados sobre un dominio a ideales principales

1

Teorema 0.1.1. Sean D un dominio a ideales principales y M un D -módulo finitamente generado.

1. Existen D -módulos L libre y T de torsión tales que $M \cong L \oplus T$. Además, L y T son únicos a menos de isomorfismos.
2. Existen $d_1, d_2, \dots, d_k \in D$ tales que $d_1 \mid d_2 \mid \dots \mid d_k$ y

$$T \cong \frac{D}{(d_1)} \oplus \frac{D}{(d_2)} \oplus \dots \oplus \frac{D}{(d_k)}.$$

Además, los d_i son únicos a menos de asociados.

3. Existen $p_1, p_2, \dots, p_t \in D$ irreducibles, $n_1, n_2, \dots, n_t \in \mathbb{N}$ y $\alpha_{ij}, i \in \{1, 2, \dots, t\}, j \in \{1, 2, \dots, n_j\}$ tales que

$$T \cong \frac{D}{(p_1^{\alpha_{11}})} \oplus \dots \oplus \frac{D}{(p_1^{\alpha_{1n_1}})} \oplus \dots \oplus \frac{D}{(p_t^{\alpha_{t1}})} \oplus \dots \oplus \frac{D}{(p_t^{\alpha_{tn_t}})}.$$

Más aún, los p_i son únicos a menos de asociados y los n_i, α_{ij} son únicos.

Observación 0.1.1. ■ Los d_i se dicen *divisores elementales* de M y los $p_i^{\alpha_{ij}}$ se dicen *factores invariantes* de M .

- Es claro que las afirmaciones 2) y 3) son equivalentes. De hecho, a partir de una descomposición del tipo 2) se obtiene una descomposición del tipo 3) usando el teorema chino de los restos. Recíprocamente, a partir de una descomposición del tipo 3) se obtiene una descomposición del tipo 2) tomando d_k el producto de todos los factores invariantes de exponente máximo, luego se toma d_{k-1} considerando los factores invariantes que quedaron, y tomando el producto de los de exponente máximo, y así sucesivamente. Es claro que $d_i \mid d_{i+1}, \forall i$ y que los dos procesos son inversos entre sí.
- Tanto 2) como 3) proporcionan una descomposición del módulo en submódulos cíclicos, pero la descomposición 3) es la más “fina” posible, en el sentido de que los sumandos que aparecen ya no pueden descomponerse más. En efecto, si $p \in D$ es irreducible y $\alpha \in \mathbb{N}$, los submódulos no triviales de $\frac{D}{(p^\alpha)}$ son todos de la forma $(p^\beta)(p^\alpha)$, con $0 < \beta < \alpha$, por lo que dos submódulos no triviales cualesquiera tienen intersección no trivial, lo que impide que la suma de ellos sea directa.
- Juntando las afirmaciones 1) y 3), se tiene que todo módulo finitamente generado se descompone en suma directa de submódulos cíclicos indecomponibles (la parte libre aporta sumandos del tipo D , y la parte de torsión sumandos del tipo $\frac{D}{(p^\alpha)}$ con $p \in D$ irreducible y $\alpha \in \mathbb{N}$).

Dem.

1. Alcanza con observar que en la sucesión exacta

$$0 \rightarrow \text{Tor}(M) \rightarrow M \rightarrow \frac{M}{\text{Tor}(M)} \rightarrow 0$$

¹Notas redactadas por Mariana Haim para el curso 2010

el término de la derecha es sin torsión, y por tanto libre (libre es equivalente a sin torsión para el caso finitamente generado sobre un dip). Se tiene entonces que la sucesión escinde y por consecuencia

$$M \cong \text{Tor}(M) \oplus \frac{M}{\text{Tor}(M)}.$$

Tomando $T = \text{Tor}(M)$ y $L = \frac{M}{\text{Tor}(M)}$ se tiene la descomposición buscada.

Supongamos ahora que $T \oplus L \cong T' \oplus L'$ via un isomorfismo φ . Entonces $\varphi(\text{Tor}(T \oplus L)) = \text{Tor}(T' \oplus L')$, i.e. $\varphi(T) = T'$ (nuevamente usamos que sobre un dip se tiene que todo libre es sin torsión). Tenemos entonces $T \cong T'$ y la prueba termina observando que $L \cong \frac{T \oplus L}{T} \cong \frac{\varphi(T \oplus L)}{\varphi(T)} = \frac{T' \oplus L'}{T'} \cong L'$.

2. Probaremos la existencia de esta descomposición en la Proposición 0.1.2. La unicidad se deduce de la unicidad de los factores invariantes en vista de la observación 0.1.1.
3. Probaremos la unicidad de esta descomposición en las Proposiciones 0.1.6 y 0.1.7. La existencia se deduce de la existencia de los divisores elementales en vista del teorema chino de los restos.

□

Proposición 0.1.2 (Existencia). *Sea T un módulo de torsión finitamente generado sobre un dominio a ideales principales. Existen $d_1, d_2, \dots, d_k \in D$ tales que $d_1 \mid d_2 \mid \dots \mid d_k$ y*

$$T \cong \frac{D}{(d_1)} \oplus \frac{D}{(d_2)} \oplus \dots \oplus \frac{D}{(d_k)}.$$

Demostración. Como T es de finitamente generado, existe $n \in \mathbb{N}$ y $p : D^n \rightarrow T$ epimorfismo. Además, $\ker(p) \subseteq D^n$ es libre, por ser submódulo de un módulo libre sobre un dip (sobre un dip, submódulo de un libre es libre: lo probamos para el caso finitamente generado, que es lo que usamos aquí).

Se tiene entonces que existen $k \in \mathbb{N}$ y $\varphi : D^k \rightarrow \ker(p)$ isomorfismo tales que el siguiente diagrama conmuta:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & D^k & \xrightarrow{\iota\varphi} & D^n & \xrightarrow{p} & T & \longrightarrow & 0 \\ & & \downarrow \varphi & & \downarrow id_{D^n} & & \downarrow id_T & & \\ 0 & \longrightarrow & \ker(p) & \xrightarrow{\iota} & D^n & \xrightarrow{p} & T & \longrightarrow & 0. \end{array}$$

Ahora bien, llamemos $\{e_1, e_2, \dots, e_k\}$ y $\{f_1, f_2, \dots, f_n\}$ a las respectivas bases canónicas de D^k y D^n . El digrama de arriba puede ser “mejorado”, en el sentido de la siguiente afirmación. Afirmación: se puede encontrar una forma “diagonal” para $\iota\varphi$, es decir un morfismo $\psi : D^k \rightarrow D^n$ que verifique $\psi(e_i) = d_i f_i, \forall i = 1, 2, \dots, k$ y dos isomorfismos \mathcal{P}, \mathcal{Q} tales que el siguiente diagrama conmuta:

$$\begin{array}{ccc} 0 & \longrightarrow & D^k \xrightarrow{\psi} D^n \\ & & \downarrow \mathcal{P} \quad \downarrow \mathcal{Q} \\ 0 & \longrightarrow & D^k \xrightarrow{\iota\varphi} D^n. \end{array}$$

Más aún, los d_i verifican $d_1 \mid d_2 \mid \dots \mid d_k$.

Probaremos la afirmación (para el caso de dominios euclídeos) en el lema 0.1.4.

Asumamos entonces la afirmación. El último diagrama puede completarse con un isomorfismo \mathcal{R} al diagrama que sigue:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & D^k & \xrightarrow{\psi} & D^n & \xrightarrow{\pi} & \frac{D^n}{\psi(D^k)} & \longrightarrow & 0 \\ & & \downarrow \mathcal{Q}^{-\infty} & & \downarrow \mathcal{P} & & \downarrow \mathcal{R} & & \\ 0 & \longrightarrow & D^k & \xrightarrow{\iota\varphi} & D^n & \xrightarrow{p} & T & \longrightarrow & 0. \end{array}$$

Se tiene entonces que $T \cong \frac{D^n}{\psi(D^k)}$. El término de la derecha es fácil de describir, en vista de que ψ es “diagonal”. En efecto, el término de la derecha tiene a $\{\overline{f_1}, \overline{f_2}, \dots, \overline{f_n}\}$ como generador, por tanto

$$T \cong D\overline{f_1} + D\overline{f_2} + \dots + D\overline{f_n}.$$

Por otra parte, la suma de arriba es directa, puesto que si $a_1\overline{f_1} + a_2\overline{f_2} + \dots + a_n\overline{f_n} = \overline{0}$, entonces $a_1f_1 + a_2f_2 + \dots + a_nf_n \in \psi(D^k)$ y por tanto $a_1f_1 + a_2f_2 + \dots + a_nf_n = b_1d_1f_1 + b_2d_2f_2 + \dots + b_kd_kf_k$, para ciertos $b_1, b_2, \dots, b_k \in D$.

Como $\{f_1, f_2, \dots, f_n\}$ es linealmente independiente, se deduce $a_i = b_id_i, \forall i \leq k$ y $a_i = 0, \forall i > k$, y por tanto $a_if_i = 0, \forall i > k$ y $a_i\overline{f_i} = b_i\overline{d_i}f_i = \overline{0}, \forall i \leq k$.

Además, $Ann(\overline{f_i}) = \begin{cases} (d_i) & \text{si } i \leq k, \\ 0 & \text{si } i > k \end{cases}$ y por tanto $D\overline{f_i} \cong \begin{cases} \frac{D}{(d_i)} & \text{si } i \leq k, \\ D & \text{si } i > k \end{cases}$.

Deducimos

$$T = Tor(T) \cong Tor(D\overline{f_1} \oplus D\overline{f_2} \oplus \dots \oplus D\overline{f_n}) \cong \frac{D}{(d_1)} \oplus \frac{D}{(d_2)} \oplus \dots \oplus \frac{D}{(d_k)}.$$

□

Definición 0.1.1. Definimos en $M_{n \times k}(D)$ una relación como sigue: $A \sim B$ si existen matrices $P \in M_n(D)$ y $Q \in M_k(D)$ invertibles tales que $A = PBQ$. Es claro que \sim es una relación de equivalencia.

Observación 0.1.2. 1. Los siguientes cambios en una matriz A dan lugar a una matriz equivalente a A :

- Intercambiar dos filas (multiplicar a izquierda por una matriz de permutación adecuada).
- Intercambiar dos columnas (multiplicar a derecha por una matriz de permutación adecuada).
- Sustituir una fila f por df con $d \in D$ invertible (multiplicar a izquierda por una matriz diagonal invertible adecuada).
- Sustituir una columna c por dc con $d \in D$ invertible (multiplicar a derecha por una matriz diagonal invertible adecuada).
- Sustituir una fila f_i por $f_i + bf_j$ con $b \in D$ y $j \neq i$ (multiplicar a izquierda por una matriz triangular invertible adecuada).
- Sustituir una columna c_i por $c_i + bc_j$ con $b \in D$ y $j \neq i$ (multiplicar a derecha por una matriz triangular invertible adecuada).

2. Tomando las matrices asociadas a \mathcal{P}, \mathcal{Q} y $\iota\phi$ en las bases canónicas que corresponda, es claro que la afirmación que se usó en la proposición, para el caso de dominios euclídeos, se deduce del lema 0.1.4. No probaremos la afirmación en el caso general.

Lema 0.1.3. Sean D un dominio euclídeo, $A \in M_{n \times k}(D)$ y d el máximo común divisor de las entradas de A . Existe una matriz $B \in M_{(n-1) \times (k-1)}(D)$ tal que $A \sim \begin{pmatrix} d & 0 \\ 0 & B \end{pmatrix}$ y tal que d divide a todas las entradas de B .

Dem. La prueba consiste en el algoritmo que permite obtener B a partir de $A = (a_{ij})$. Diremos que la matriz (a_{ij}) es **normal** si $\delta(a_{11}) = \min\{\delta(a_{ij}) \mid a_{ij} \neq 0\}$. Es claro que toda matriz es equivalente (mediante un intercambio de filas y columnas) a una matriz normal.

Conviene aclarar que en cada paso del algoritmo (salvo en los pasos 3 y 6), la matriz se transforma en otra matriz equivalente, cuyos coeficientes seguimos llamando a_{ij} , cuyos vectores fila llamamos f_j y cuyos vectores columna llamamos c_i , para $i \in \{1, 2, \dots, k\}, j \in \{1, 2, \dots, n\}$.

Paso 1: Cambiar la matriz por otra normal equivalente.

Paso 2: Hallar $q, r \in D$ tales que $a_{21} = qa_{11} + r$ y sustituir la segunda fila f_2 por $f_2 - qf_1$.

Paso 3: Si $r = 0$: pasar al Paso 4. Si no: volver al Paso 1.

Paso 4: Idem para $a_{31}, a_{41}, \dots, a_{n1}$.

Paso 5: Hallar $q, r \in D$ tales que $a_{12} = qa_{11} + r$ y sustituir la segunda columna c_2 por $c_2 - qc_1$.

Paso 6: Si $r = 0$: pasar al Paso 7. Si no: volver al paso 1.

Paso 7: Idem para $a_{13}, a_{14}, \dots, a_{1k}$.

Paso 8: Se obtiene una matriz de la forma

$$\begin{pmatrix} a & 0 \\ 0 & (B) \end{pmatrix}.$$

Si a divide a todas las entradas de B : terminar. Si no, elegir una entrada de B que no sea múltiplo de a y sustituir la fila f_1 por $f_1 + f_j$, siendo j la fila de dicha entrada, y volver al Paso 1.

Es claro que el proceso termina, pues en el Paso 8, se sustituye la matriz $\begin{pmatrix} a & 0 \\ 0 & (B) \end{pmatrix}$ por otra cuya entrada a_{11} verifica $\delta(a_{11}) < \delta(a)$.

Veamos que el a para el cual el proceso termina es asociado a d . En primer lugar, notar que a divide a todas las entradas de B y por tanto a divide a todas las entradas de $A' = \begin{pmatrix} a & 0 \\ 0 & (B) \end{pmatrix}$; como $A = PA'Q$ y las entradas de P y Q están en D , se tiene que a divide a todas las entradas de A y por tanto a divide a d . Por otra parte, como todas las entradas de A son múltiplos de d , se tiene que todas las entradas de $A' = P^{-1}AQ^{-1}$ son múltiplos de d de donde se deduce que en particular a es múltiplo de d .

□

Lema 0.1.4. Sean D un dominio euclídeo y $A \in M_{n \times k}(D)$. Existe una matriz J diagonal tal que $A \sim J$ y cada entrada de la diagonal de J divide a la siguiente.

Dem. Haremos la prueba por inducción en $k \in \mathbb{N}$.

Para $k = 1$ sale del lema 0.1.3. Supongamos ahora que vale para $k = r$ y probémoslo para $k = r + 1$.

Sabemos por el lema 0.1.3 que $A \sim \begin{pmatrix} d & 0 \\ 0 & (B) \end{pmatrix}$ para cierta $B \in M_{n-1 \times r}$ cuyas entradas son múltiplos de d . Por hipótesis de inducción, se tiene que B es equivalente a una matriz diagonal J_B tal que cada entrada diagonal divide a la siguiente. Es fácil ver que entonces $\begin{pmatrix} d & 0 \\ 0 & (B) \end{pmatrix}$ es equivalente a $\begin{pmatrix} d & 0 \\ 0 & (J_B) \end{pmatrix}$. Además d divide a la primera entrada de J_B , puesto que esta primera entrada es el máximo común divisor de las entradas de B , todas ellas múltiplos de d .

□

Definición 0.1.2. Dado un dominio a ideales principales D y un elemento $p \in D$ irreducible, llamaremos p -módulo a un módulo de la forma $\frac{D}{(p^{\alpha_1})} \oplus \frac{D}{(p^{\alpha_2})} \oplus \dots \oplus \frac{D}{(p^{\alpha_n})}$.

Diremos que dicho p -módulo es homogéneo de género α si $\alpha = \alpha_1 = \alpha_2 = \dots = \alpha_n$.

Lema 0.1.5. Sean D un dominio a ideales principales, $p, q \in D$ irreducibles, $\beta \in \mathbb{N}$ y N un p -módulo. Si existe un morfismo no nulo $\varphi : \frac{D}{(q^\beta)} \rightarrow N$, entonces $p \sim q$.

Dem. Todos los elementos $\bar{x} \in \frac{D}{(q^\beta)}$ verifican $q^\beta \bar{x} = 0$. Tomando \bar{x} tal que $(\bar{y}_1, \bar{y}_2, \dots, \bar{y}_n) = \varphi(x) \neq 0$, se tiene que para cierto i , $\bar{y}_i \neq 0$ y $q^\beta \bar{y}_i = 0$. Se deduce que p divide a q^β y por tanto p divide a q , puesto que p es irreducible. Por ser también q irreducible, se tiene que p y q son asociados. □

Proposición 0.1.6 (Unicidad de los irreducibles involucrados).

Sean D un dominio a ideales principales y $p_1, p_2, \dots, p_t, q_1, q_2, \dots, q_r \in D$ irreducibles tales que $p_i \not\sim p_j$, $q_i \not\sim q_j$ si $i \neq j$. Supongamos que se tiene

$$M_1 \oplus M_2 \oplus \dots \oplus M_t \cong N_1 \oplus N_2 \oplus \dots \oplus N_r,$$

donde M_i es un p_i -módulo para cada $i \in \{1, 2, \dots, t\}$ y N_j es un q_j -módulo para cada $j \in \{1, 2, \dots, r\}$.

Entonces $t = r$ y para cada i existe un único j tal que $p_i \sim q_j$. Más aún, el isomorfismo lleva cada M_i en N_j .

Dem. Para cada i , existe j tal que el morfismo $\pi_j \varphi_{\nu_i} : M_i \rightarrow N_j$ es no nulo (siendo $\varphi : \bigoplus_i M_i \rightarrow \bigoplus_j N_j$ el isomorfismo involucrado). Aplicando entonces el lema 0.1.5 a este morfismo, se tiene la tesis. La unicidad de tal j se deduce del hecho de que los q_j son no asociados dos a dos. Además, también por el lema 0.1.5, se tiene que para cada k tal que $q_k \not\sim p_i$, el morfismo $\pi_k \varphi_{\nu_i}$ es nulo, de donde sale $\varphi(M_i) \subseteq N_j$. □

En vista de la proposición anterior, sólo queda verificar la unicidad de la descomposición “dentro” de cada p -módulo.

Proposición 0.1.7 (Unicidad de los exponentes).

Sean $p \in D$ irreducible, $\alpha_1 < \alpha_2 < \dots < \alpha_k$ y $\beta_1 < \beta_2 < \dots < \beta_r$ enteros. Supongamos que se tiene

$$M = M_1 \oplus M_2 \oplus \dots \oplus M_t \cong N_1 \oplus N_2 \oplus \dots \oplus N_r = N,$$

donde cada M_i es un p -módulo homogéneo de género α_i y cada N_j es un p -módulo homogéneo de género β_j . Entonces $t = r$ y para cada i se tiene $\alpha_i = \beta_i$. Más aún, si $M_i = \bigoplus_{h=1}^{m_i} \frac{D}{p^{\alpha}}$ y $N_i = \bigoplus_{h=1}^{n_i} \frac{D}{p^{\alpha}}$, entonces $m_i = n_i, \forall i$.

Dem. Observemos primero que del hecho de que todos los elementos de M son anulados por p^{α_t} , se deduce que $e_r \in N$ también y por tanto $\alpha_t \leq \beta_r$. Análogamente se prueba la otra desigualdad y por tanto $\alpha_t = \beta_r$. Llamemos $\varphi : M \rightarrow N$ al isomorfismo involucrado.

Tenemos $M = M_1 \oplus M_2 \oplus \dots \oplus M_t \cong N_1 \oplus N_2 \oplus \dots \oplus N_r = N$, con $\alpha_t = \beta_r$. Vamos a probar primero que $\alpha_1 = \beta_1$. Supongamos que $\alpha_1 < \beta_1$. Tomemos $e_1 = ((\hat{1}, 0, \dots, 0), 0, \dots, 0) \in M$ y consideremos $\varphi(e_1) = (\bar{n}_1, \dots, \bar{n}_l)$. Como e_1 es anulado por $p^{\alpha_1} < p^{\beta_j}, \forall j$, se tiene que cada $n_j \in D$ debe ser múltiplo de p . O sea que $\varphi(e_1) = p\bar{n}' = p(\bar{n}'_1, \dots, \bar{n}'_l)$. Como φ es sobreyectiva, existe $\bar{m} \in M$, tal que $\varphi(\bar{m}) = \bar{n}$, y como además es inyectiva, se tiene $p\bar{m} = e_1 \in M$, cosa que es absurda porque implica que para ciertos $x, m_1 \in D$, $pm_1 + p^\alpha x = 1$.

Se deduce que existe j tal que $\alpha_1 \geq \beta_j \geq \beta_1$ y análogamente se deduce $\beta_1 \geq \alpha_1$.

Ahora bien, argumentos similares permiten probar que $\alpha_2 = \beta_2, \alpha_3 = \beta_3, \dots, \alpha_t = \beta_t$ y como $\beta_r = \alpha_t$ y los β_j son distintos dos a dos, se concluye también $t = r$.

Falta ver que $m_i = n_i, \forall i$. Para esto, basta observar que en M la cantidad máxima de elementos linealmente independientes cuyo anulador es (p^α) es m_i , mientras que en N es n_i . El hecho de ser linealmente independiente se preserva por isomorfismos, y el anulador de un elemento también se preserva por isomorfismos; deducimos entonces que $m_i = n_i$. □

0.2. Formas canónicas racional y de Jordan

2

En lo que sigue \mathbb{k} es un cuerpo cualquiera, V es un \mathbb{k} -espacio vectorial y $T : V \rightarrow V$ es una transformación lineal.

Usaremos el teorema de estructura para, en el caso en que V tenga dimensión finita, obtener una descomposición de V en subespacios T -cíclicos (i.e. generados por un elemento v y sus transformados a través de T y sus iteradas), que da lugar a una base B de V para la cual la matriz asociada ${}_B[T]_B$ es en algún sentido “simple”. Dicha matriz es esencialmente única y se llama forma canónica racional de T . Además, probaremos que si el polinomio característico de T se descompone en $\mathbb{k}[x]$ como producto de polinomios de grado 1 (por ejemplo cuando $\mathbb{k} = \mathbb{C}$), deduciremos la existencia de la forma de Jordan para T .

Antes de enunciar el primer resultado, conviene recordar algunas definiciones. Decimos que un subespacio W de V es T -invariante si $T(W) \subseteq W$, y que es T -cíclico si para cierto $w \in W$, se tiene que el conjunto $\{w, T(w), T^2(w), \dots, T^n(w), \dots\}$ es un generador de W . En este último caso, notamos $W = Z(T, w)$. Recordemos además que un A -módulo M se dice **cíclico** si $M = \{am \mid a \in A\}$ para cierto $m \in M$.

La siguiente proposición permite poner nuestra situación en contexto de módulos sobre $\mathbb{k}[x]$.

Proposición 0.2.1. Sean \mathbb{k} un cuerpo, V un \mathbb{k} -espacio vectorial y $T : V \rightarrow V$ una transformación lineal. Entonces:

1. Definiendo $p \cdot v = p(T)(v), \forall v \in V, p \in \mathbb{k}[x]$, se obtiene que $((V, +, 0), \cdot)$ es un $\mathbb{k}[x]$ -módulo.
2. Si $W \subseteq V$ es un subespacio, entonces se tiene que:
 - a) W es T -invariante si y sólo si W es un submódulo de V ,
 - b) W es T -cíclico si y sólo si W es un módulo cíclico.

Dem.

1. Es claro que $(V, +, 0)$ es un grupo abeliano, puesto que es la estructura aditiva de un espacio vectorial. Por otra parte es claro que la operación $\cdot : \mathbb{k}[x] \times V \rightarrow V$ es distributiva con respecto a la suma en $\mathbb{k}[x]$ y con respecto a la suma en V . Observemos además que $1 \cdot v = Id(v) = v, \forall v \in V$. Falta entonces verificar que

$$p \cdot (q \cdot v) = (pq) \cdot v, \forall p, q \in \mathbb{k}[x], v \in V.$$

Para esto, es claro que alcanza con verificarlo para p y q monomios de $\mathbb{k}[x]$. En efecto, basta con observar que si $p = \sum_{i=0}^k a_i x^i$, entonces

$$p \cdot v = \sum_{i=0}^k a_i (x^i \cdot v). \quad (*)$$

Tomemos entonces $p = ax^i, q = bx^j$. Tenemos que $q \cdot v = (bT^j)(v) = bT^j(v)$. Entonces

$$p \cdot (q \cdot v) = p \cdot (bT^j(v)) = (aT^i)(bT^j(v)) = aT^i(bT^j(v)) = abT^i(T^j(v)) = abT^{i+j}(v).$$

Como $pq = abx^{i+j}$, se deduce la tesis.

2. Tomemos ahora $W \subseteq V$ subespacio.

- a) W es T -invariante si y sólo si $T(w) \in W, \forall w \in W$ si y sólo si $x \cdot w \in W, \forall w \in W$. Es claro por (*) que esto último equivale a $p \cdot w \in W, \forall w \in W, p \in \mathbb{k}[x]$, es decir a que W sea un $\mathbb{k}[x]$ -submódulo de V .
- b) $W = Z(T, w)$ si y sólo si W es generado como \mathbb{k} -espacio vectorial por $\{T^i(w) \mid i \in \mathbb{N}\}$ si y sólo si W es generado como $\mathbb{k}[x]$ -módulo por w (puesto que $T^n(w) = x^n \cdot w$).

□

Observación 0.2.1.

- 1. Si consideramos \mathbb{k} como un subconjunto de $\mathbb{k}[x]$ de la manera obvia, la acción de $\mathbb{k}[x]$ en V definida arriba, extiende a la acción original de \mathbb{k} en V . En efecto, $\lambda \cdot v = (\lambda Id)(v) = \lambda v$.
- 2. A partir de la observación 1, se deduce que un generador de V como \mathbb{k} -espacio vectorial, también es generador de V como $\mathbb{k}[x]$ -módulo.
- 3. Es claro que si V es de dimensión finita $Z(T, w)$ también lo es, y por lo tanto existe $k \in \mathbb{N}$ tal que el conjunto $\{w, T(w), T^2(w), \dots, T^{k-1}(w)\}$ es generador de $Z(T, w)$. Más adelante, veremos que se puede optimizar dicho k para obtener una base.
- 4. Si $f \in \mathbb{k}[x]$, se tiene que $\frac{\mathbb{k}[x]}{(f)}$ es un espacio vectorial de dimensión $deg(f)$. En efecto, es fácil verificar que el conjunto $\{\bar{1}, \bar{x}, \dots, \bar{x}^{deg(f)-1}\}$ es una base.

Polinomios característico y minimal

Consideremos la inclusión $\iota : \mathbb{k} \rightarrow End(V)$, definida por $\iota(\lambda) = \lambda Id$. Es claro que es un morfismo de anillos y por tanto se extiende de manera única a un morfismo de anillos $\varepsilon_T : \mathbb{k}[x] \rightarrow End(V)$ tal que $\varepsilon(x) = T$. Explícitamente, se tiene $\varepsilon_T(p) = p(T)$.

Si V tiene dimensión finita, podemos considerar el polinomio $\chi_T = det(T - xId)$. Dicho polinomio se llama **polinomio característico de T**, es de grado $dim(V)$ y por tanto no nulo. El Teorema de Cailey-Hamilton asegura que $\chi_T(T) = 0$.

Se deduce que $ker(\varepsilon_T)$ es un ideal de $\mathbb{k}[x]$ no nulo, y por tanto generado por un polinomio no nulo $m_T \in \mathbb{k}[x]$ que se elige mónico y se llama **polinomio minimal de T**. (Notar que al elegir m_T mónico, forzamos a que sea único).

Es claro entonces que $m_T(T) = 0$, que $m_T | \chi_T$ y que m_T es el polinomio mónico de menor grado entre los que anulan a T .

La siguiente proposición permite poner a V , en el caso en que tenga dimensión finita, en el contexto del teorema de estructura.

Proposición 0.2.2. Sean \mathbb{k}, V y T como antes. Supongamos además que V es de dimensión finita. Entonces V es un $\mathbb{k}[x]$ -módulo finitamente generado y de torsión.

Dem. Por la observación 2 es claro que V es finitamente generado, puesto que es de dimensión finita. Además si V es de dimensión finita, podemos considerar el polinomio característico de T . Como $\chi_T(T) = 0$, tenemos $\chi_T \cdot v = 0, \forall v \in V$. Se deduce que todo $v \in V$ es de torsión.

□

Estamos entonces en condiciones de aplicar el teorema de estructura al $\mathbb{k}[x]$ -módulo V y eso es lo que nos permitirá demostrar el siguiente resultado.

Teorema 0.2.3. *Sean V un espacio vectorial de dimensión finita $n \in \mathbb{N}$ y $T \in \text{End}(V)$. Sea además $m_T = q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}$ la descomposición en irreducibles mónicos no asociados dos a dos del polinomio minimal. Existen naturales k_1, k_2, \dots, k_r y subespacios $V_{ij}, i \in \{1, 2, \dots, r\}, j \in \{1, 2, \dots, k_i\}$ de V , tales que*

1. $V = \bigoplus_{i=1}^r \bigoplus_{j=1}^{k_i} V_{ij}$,
2. para todo par (i, j) , V_{ij} es T -cíclico,
3. para todo par (i, j) , existe $n_{ij} \in \mathbb{N}$ tal que $\text{Ann}(V_{ij}) = (q_i^{n_{ij}})$,
4. para todo $i \in \{1, 2, \dots, r\}$ se tiene $n_i = \max\{n_{ij} \mid j \in \{1, 2, \dots, k_i\}\}$,
5. $n = \sum_{ij} \deg(q_i) n_{ij}$.

Más aún, los V_{ij} son únicos a menos de isomorfismos y de reordenaciones.

Dem. Como V es de torsión y finitamente generado sobre el dominio a ideales principales $\mathbb{k}[x]$, el teorema de estructura nos da una descomposición de V en submódulos cíclicos indescomponibles:

$$V \cong \bigoplus_{i=1}^t \bigoplus_{j=1}^{s_i} \frac{\mathbb{k}[x]}{(p_i^{n_{ij}})},$$

para ciertos $p_i \in \mathbb{k}[x]$ irreducibles no asociados dos a dos y ciertos $n_{ij} \in \mathbb{N}$ no nulos. Es claro que los p_{ij} pueden elegirse mónicos, y eso hacemos.

Llamemos $\varphi : \bigoplus_{i=1}^t \bigoplus_{j=1}^{s_i} \frac{\mathbb{k}[x]}{(p_i^{n_{ij}})} \rightarrow V$ al isomorfismo involucrado y definamos entonces, para cada $i \in \{1, 2, \dots, r\}$ y para $j \in \{1, 2, \dots, s_i\}$,

$$V_{ij} := \varphi \left(\frac{\mathbb{k}[x]}{(p_i^{n_{ij}})} \right).$$

Es claro que $V = \bigoplus_{i=1}^t \bigoplus_{j=1}^{s_i} V_{ij}$ y que $\text{Ann}(V_{ij}) = (p_i^{n_{ij}})$ y que los p_{ij} pueden elegirse mónicos. Además, para cada $i \in \{1, 2, \dots, t\}$, podemos reordenar los $j \in \{1, 2, \dots, s_i\}$ para que $n_{i1} \geq n_{i2} \geq \dots \geq n_{is_i}$. Veamos ahora que

- $r = t$,
- podemos reordenar los $i \in \{1, 2, \dots, r = t\}$ para que $r_i = s_i$ y $p_i = q_i, \forall i \in \{1, 2, \dots, r = t\}$,
- $n_i = n_{i1}, \forall i \in \{1, 2, \dots, r\}$.

Como $\mathbb{k}[x]$ es un dominio factorial, m_T se descompone de manera única (a menos de reordenaciones) en producto de irreducibles mónicos, por lo que alcanza con ver que

$$m_T = p_1^{n_{i1}} p_2^{n_{i2}} \cdots p_r^{n_{ir}}, (**)$$

para deducir las tres afirmaciones de arriba. Llamemos p al polinomio de la derecha de la igualdad (**). Como $p_i^{n_{ij}}$ anula a cada V_{ij} , se tiene que $p_i^{n_{i1}}$ anula a cada V_{ij} y por tanto p anula a V y se deduce que p es múltiplo de m_T . Para el recíproco, observar que el polinomio minimal de $T|_{V_{ij}}$ es $p_i^{n_{ij}}$; como m_T anula a

□

Definición 0.2.1. La matriz R del corolario 0.2.4 se dice **forma canónica racional** de la matriz A en el cuerpo \mathbb{k} , mientras que la matriz J del corolario 0.2.5 se dice **forma canónica de Jordan** de la matriz A en el cuerpo \mathbb{k} .

Observación 0.2.2. 1. Ambas formas son únicas a menos de reordenar bloques, por eso comunmente se habla de *la forma canónica racional* o *la forma canónica de Jordan*.

2. La forma de Jordan sobre un cuerpo \mathbb{k} no siempre está definida, mientras que la racional siempre lo está.
3. Si A es diagonalizable semejante a D , la forma canónica de Jordan de A está definida (puesto que el polinomio minimal es el producto de los polinomios $x - d_i$, variando d_i en todas las entradas distintas de la diagonal de D). Además ambas formas coinciden y son D .
4. Si A es nilpotente, la forma canónica de Jordan de A está definida (puesto que su polinomio minimal es de la forma X^n y por tanto se descompone en producto de polinomios irreducibles de grado 1) y coincide con la forma canónica racional de A (puesto que se tiene $\lambda_i = 0, \forall i$).