Tema 6.- Teorema de estructura de los módulos finitamente generados sobre un D.I.P.. Aplicaciones: ecuaciones lineales con coeficientes enteros, formas canónicas de Jordan

6.1 Teorema de estructura de los módulos finitamente generados sobre un D.I.P.

En lo que sigue A denotará un dominio de ideales principales y K su cuerpo de fracciones.

LEMA 6.1.1.– Sean $v_1, \ldots, v_m \in A^n$. Entonces los v_i son A-linealmente independientes (en A^n) si y sólo si son K-linealmente independientes en K^n.[1]

DEFINICIÓN 6.1.2.– Dado un subconjunto cualquiera no vacío $S \subset A^n$, definimos el *rango* de S, que notaremos $\operatorname{rg}(S)$, como el número máximo de elementos de S que sean A-linealmente independientes, que por el lema anterior, coincide con el número máximo de elementos de S que sean K-linealmente independientes en K^n, o lo que es lo mismo, con $\dim_K L_K(S)$, donde $L_K(S)$ denota el subespacio vectorial de K^n generado por S.

LEMA 6.1.3.–

1. Si $S \subset A^n$, entonces $\operatorname{rg}(S) \leq n$.
2. Si $M \subset A^n$ es un submódulo, entonces los elementos de $L_K(M)$ son de la forma $a^{-1}m$, con $a \in A, a \neq 0$ y $m \in M$.
3. Si $S = A^n$, entonces $\operatorname{rg}(A^n) = n$.
4. Si $M_1, M_2 \subset A^n$ son dos submódulos tales que $M_1 \cap M_2 = 0$, entonces $\operatorname{rg}(M_1 \oplus M_2) = \operatorname{rg}(M_1) + \operatorname{rg}(M_2)$.

PROPOSICIÓN 6.1.4.– Sea M un A-módulo libre de rango $n \geq 1$ y $M' \subset M$ un submódulo no nulo. Entonces existe $e \in M$, $u_0 : M \to A$ lineal y $a \in A - \{0\}$ tales que:

1. $u_0(e) = 1$
2. $M = (Ae) \oplus \ker u_0$
3. $M' = (Aae) \oplus (M' \cap \ker u_0)$.

[1] Este resultado es válido siempre que A sea un dominio de integridad.

PRUEBA:

1) Para cada $u \in \mathrm{Hom}_A(M, A)$, la imagen por u de M', $u(M')$, es un submódulo de A, i.e. un ideal, y como A es DIP, existirá $a_u \in A$ tal que $u(M') = Aa_u$. Sea Ω el conjunto (no vacío) de todos los ideales de A de la forma $u(M') = Aa_u$, para algún $u \in \mathrm{Hom}_A(M, A)$. Como A es noetheriano, Ω posee algún elemento maximal $u_0(M') = Aa_{u_0}$, para un cierto $u_0 \in \mathrm{Hom}_A(M, A)$. Como M es libre de rango n, podemos suponer que $M = A^n$. Sean $\pi_i : M \to A$, $i = 1, \dots, n$, las proyecciones. Como $M' \neq 0$, existirá un i_0 tal que $\pi_{i_0}(M') \neq 0$, con lo que $u_0(M') \neq 0$ y $a_{u_0} \neq 0$ (en caso contrario, $u_0(M') = 0$ estaría estrictamente contenido en $\pi_{i_0}(M')$, lo que contradeciría la maximalidad de $u_0(M')$ en Ω).

Sea $e' \in M'$ tal que $u_0(e') = a_{u_0}$.

2) Dado un $v \in \mathrm{Hom}_A(M, A)$ cualquiera, veamos que a_{u_0} divide a $v(e')$. En efecto, sea $d = \mathrm{m.\,c.\,d.}(a_{u_0}, v(e'))$. Por la identidad de Bézout, existen $b, c \in A$ tales que $d = ba_{u_0} + cv(e')$, de donde $d = (bu_0 + cv)(e')$. Si notamos $\omega = bu_0 + cv \in \mathrm{Hom}_A(M, A)$, tenemos $u_0(M') = Aa_{u_0} \subset Ad \subset \omega(M')$, pero la maximalidad de $u_0(M') = Aa_{u_0}$ en Ω implica que $Aa_{u_0} = Ad$, y por tanto a_{u_0} divide a $v(e')$.

En particular a_{u_0} divide a cada $\pi_i(e')$, $i = 1, \dots, n$. Pongamos $\pi_i(e') = b_i a_{u_0}$, $b_i \in A$ y sea $e = (b_1, \dots, b_n) \in A^n = M$. Se tiene $e' = a_{u_0} e$ y $a_{u_0} = u_0(e') = a_{u_0} u_0(e)$, de donde $u_0(e) = 1$.

3) Veamos que $M = (Ae) \oplus \ker u_0$ y $M' = (Aa_{u_0} e) \oplus (M' \cap \ker u_0)$.

Para cada $x \in M$ se tiene $x = u_0(x)e + (x - u_0(x)e)$, donde claramente $x - u_0(x)e \in \ker u_0$, y por tanto $M = (Ae) + \ker u_0$. Además, como $u_0(e) = 1$, deducimos que $(Ae) \cap \ker u_0 = 0$.

Para cada $y \in M'$ se tiene $u_0(y) \in u_0(M') = Aa_{u_0}$, por lo que existe $b \in A$ tal que $u_0(y) = ba_{u_0}$ y podemos escribir $y = be' + (y - u_0(y)e)$, donde $y - u_0(y)e = y - be' \in M' \cap \ker u_0$, de donde $M' = (Aa_{u_0} e) + (M' \cap \ker u_0)$. Además $(Aa_{u_0} e) \cap (M' \cap \ker u_0) \subset (Ae) \cap \ker u_0 = 0$. □

TEOREMA 6.1.5.– Sea M un módulo libre de rango $n \geq 1$ y sea $M' \subset M$ un submódulo de rango $q \geq 0$. Entonces se verifican las propiedades siguientes:

(a) M' es libre.

(b) Existe una base $\{e_1, \dots, e_n\}$ de M y unos elementos $a_1, \dots, a_q \in A - \{0\}$ únicos salvo asociados (independientes de la base anterior) tales que:

  (b-1) $\{a_1 e_1, a_2 e_2, \dots, a_q e_q\}$ es una base de M',

  (b-2) $a_1 | a_2 | \cdots | a_q$.

PRUEBA: Para demostrar (a) procederemos por inducción sobre q. Si $q = 0$, entonces $M' = 0$ y el resultado es trivial.

Supongamos (a) cierto siempre que el rango del submódulo sea $q - 1 \geq 0$ y sea $\mathrm{rg}(M') = q \geq 1$. Aplicando la proposición anterior tenemos que $M' =$

$(Aae) \oplus (M' \cap \ker u)$, y por el lema 6.1.3 deducimos que $\mathrm{rg}(M' \cap \ker u) = q - 1$. Por la hipótesis de inducción, $M' \cap \ker u$ es libre, y por tanto M' también.

Para demostrar (b) procederemos por inducción sobre $n = \mathrm{rg}\, M$. Si $n = 1$ el resultado es consecuencia de que A es un DIP.

Supongamos (b) cierto siempre que el rango del módulo libre ambiente sea $n - 1 \geq 1$ y supongamos $\mathrm{rg}\, M = n$. Aplicando de nuevo la proposición anterior, el lema 6.1.3 y el apartado (a) deducimos que $\ker u$ es libre de rango $n-1$ y que $\mathrm{rg}(M' \cap \ker u) = q - 1$. Por la hipótesis de inducción aplicada al módulo libre $\ker u$ y al submódulo $M' \cap \ker u$ deducimos la existencia de una base $\{e_2, \ldots, e_n\}$ de $\ker u$ y de unos elementos únicos $a_2, \ldots, a_q \in A$ tales que $a_2|a_3|\cdots|a_q$ y $\{a_2e_2, \ldots, a_qe_q\}$ es una base de $M' \cap \ker u$. Pongamos $e_1 = e$ y $a_1 = a$, dados también en la proposición anterior. Es claro que $\{e_1, e_2, \ldots, e_q\}$ es una base de M y que $\{a_1e_1, a_2e_2, \ldots, a_qe_q\}$ es una base de M'.

Nos queda por probar que $a_1|a_2$. Para ello consideremos la forma lineal $v : M \to A$ dada por $v(e_1) = v(e_2) = 1, v(e_i) = 0$ para todo $i \geq 3$. Con las notaciones de la prueba de la proposición anterior, se tiene $a_1 = a = a_{u_0} = v(a_{u_0}e_1) = v(e') \in v(M')$, de donde $Aa_{u_0} \subset v(M')$, y por el carácter maximal de $Aa_{u_0} = u_0(M')$ se tiene $v(M') = Aa_1$, pero $a_2 = v(a_2e_2) \in v(M') = Aa_1$ y por tanto $a_1|a_2$.

Veamos ahora la unicidad de los a_i. Para ellos usaremos la noción de aplicación multilineal *alternada*: diremos que una aplicación multilineal $f : M \times \overset{r}{\cdots} \times M \to A$ es alternada si $f(x_1, \ldots, x_r) = 0$ siempre que $x_i = x_j$ para algunos $i \neq j$. El conjunto de las aplicaciones multilineales alternadas de M^r en A es claramente un submódulo del A-módulo de las aplicaciones multilineales, que notaremos $\mathrm{Alt}(M^r, A)$.

Para cada $r = 1, \ldots, q$ notemos

$$J_r = \langle f(y_1, \ldots, y_r), y_i \in M', f \in \mathrm{Alt}(M^r, A) \rangle.$$

Obviamente cada J_r es un ideal de A que, fijado M, depende exclusivamente de M'.

La unicidad de los a_i es consecuencia de las igualdades $J_r = (a_1 \cdots a_r)$, que pasamos a probar.

Dados $y_j \in M'$, $j = 1, \ldots, r$, podemos expresarlos como $y_j = \sum_{i=1}^{q} c_{ji}a_ie_i$ con $c_{ji} \in A$, y por tanto, para cada aplicación multilineal f se tiene:

$$f(y_1, \ldots, y_r) = \sum_{\substack{1 \leq j \leq r \\ 1 \leq i_j \leq q}} \left(\prod_{j=1}^{r} c_{ji_j} \right) \left(\prod_{j=1}^{r} a_{i_j} \right) f(e_{i_1}, \ldots, e_{i_r}).$$

Ahora bien, si f es alternada, todos los sumandos de la expresión anterior donde haya repeticiones en $i_1, \ldots, i_r$ serán nulos, y para aquéllos donde los $i_1, \ldots, i_r$ sean distintos entre sí se tendrá $a_1 \cdots a_r | \prod_{j=1}^{r} a_{i_j}$ puesto que $a_1|a_2|\cdots|a_q$. Así deducimos que $a_1 \cdots a_r | f(y_1, \ldots, y_r)$, o de forma equivalente $J_r \subset (a_1 \cdots a_r)$.

Para la otra inclusión, consideremos las formas lineales $\omega_i : M \to A$ tales que $\omega_i(e_j) = \delta_{ij}$ y la aplicación multilineal alternada $f : M^r \to A$ dada por

$$f(x_1, \ldots, x_r) = \det(\omega_i(x_j)).$$

Se tiene que $a_1 \cdots a_r = f(a_1 e_1, \ldots, a_r e_r) \in J_r$. □

Nota 6.1.6.– Si en el teorema anterior hacemos $n = 1$, entonces M es isomorfo a A y M' correspondería a un ideal de A. En tal caso se trata de una reformulación del hecho de que A es un dominio de integridad y que todos sus ideales son principales.

Corolario 6.1.7.– Si E es un A-módulo finitamente generado no nulo, entonces existen unos ideales únicos $\mathfrak{a}_m \subset \mathfrak{a}_{m-1} \subset \cdots \subset \mathfrak{a}_2 \subset \mathfrak{a}_1 \subset A$, con $\mathfrak{a}_1 \neq A$, tales que:

$$E \simeq (A/\mathfrak{a}_1) \times (A/\mathfrak{a}_2) \times \cdots \times (A/\mathfrak{a}_m).$$

Prueba: Como E es un módulo finitamente generado, se puede expresar como cociente de un módulo libre A^n por un cierto submódulo M'. Aplicando el teorema anterior, si ninguno de los a_i es unidad, basta tomar $\mathfrak{a}_i = Aa_i$, $i = 1, \ldots, q$ y $\mathfrak{a}_i = 0$ para $q < i \leq n$. En caso contrario, procederíamos a quedarnos sólo con los $\mathfrak{a}_i = Aa_i$ tales que a_i no sea unidad.

`Falta la unicidad` □

Definición 6.1.8.– Los ideales $\mathfrak{a}_m \subset \mathfrak{a}_{m-1} \subset \cdots \subset \mathfrak{a}_2 \subset \mathfrak{a}_1$ se denominan *factores invariantes* del módulo E.

Definición 6.1.9.– Dado un A-módulo M, diremos que un elemento $x \in M$ es un *elemento de torsión* si existe un $a \in A, a \neq 0$ tal que $ax = 0$.
Diremos que M es un *módulo de torsión* si todos sus elementos son elementos de torsión.

Lema 6.1.10.– Dado un A-módulo M, el conjunto de sus elementos de torsión $\mathrm{Tor}(M)$ es un submódulo de M.

Corolario 6.1.11.– Todo A-módulo finitamente generado es suma directa de su módulo de torsión $\mathrm{Tor}(M)$ y de un módulo libre de rango finito, cuyo rango está determinado unívocamente por M. En particular todo A-módulo finitamente generado sin torsión es libre.

Corolario 6.1.12.– Dado un A-módulo M finitamente generado existen un entero $d \geq 0$, unos ideales primos $\mathfrak{p}_i \subset A$ no nulos y unos enteros $s_i \geq 1$, $i = 1, \ldots, r$, tales que:

$$M \simeq (A/\mathfrak{p}_1^{s_1}) \times \cdots \times (A/\mathfrak{p}_r^{s_r}) \times A^d.$$

Además, el isomorfismo anterior establece otro isomorfismo:

$$\mathrm{Tor}(M) \simeq (A/\mathfrak{p}_1^{s_1}) \times \cdots \times (A/\mathfrak{p}_r^{s_r}).$$

Prueba: Basta tener en cuenta que si $\mathfrak{a}$ es un ideal propio de A, de que A sea un DIP deducimos la existencia de unos ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ y unos enteros $e_1, \ldots, e_m \geq 1$ (todos ellos únicos) tales que

$$\mathfrak{a} = \prod_{i=1}^{m} \mathfrak{p}_i^{e_i}.$$

$\square$

Teorema 6.1.13.– Sea Q una matriz $m \times n$ con coeficientes en A. Entonces existen unas matrices P y R de orden $m \times m$ y $n \times n$ respectivamente, con coeficientes en A e inversibles (i.e. $\det(P)$ y $\det(R)$ son unidades de A) tales que

$$PQR = \begin{pmatrix} a_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & a_q & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

donde $q = \mathrm{rg}(Q)$, $a_i \in A - \{0\}$ y $a_1 | a_2 | \cdots | a_q$.

Además, se tiene lo siguiente:

1. Si denotamos por Δ_i el máximo común divisor de los menores $i \times i$ no nulos de Q, con $i = 1, \ldots, q$, se tiene:

$$a_1 = \Delta_1, \quad a_i = \frac{\Delta_i}{\Delta_{i-1}}, \quad i = 2, \ldots, q.$$

2. Si $M \subset A^n$ es el sub-A-módulo generado por las filas de la matriz Q, entonces los a_i anteriores coinciden con los del teorema 6.1.5.

6.2 Aplicaciones: formas canónicas de Jordan

En lo que sigue k será un cuerpo y V un k-espacio vectorial de dimensión finita $d \geq 1$. Dado un endomorfismo $f : V \to V$, podemos definir una estructura de $k[X]$-módulo sobre V de la siguiente forma:

$$(\sum_{i=0}^{m} a_i X^i) \cdot v := \sum_{i=0}^{m} a_i f^i(v)$$

para todo polinomio $\sum_{i=0}^{m} a_i X^i \in k[X]$ y todo $v \in V$.

Lema 6.2.1.– El $k[X]$-módulo V anterior es f.g. y de torsión.

Prueba: Es claro que todo sistema (finito) de generadores de V como espacio vectorial también es un sistema de generadores de V como $k[X]$-módulo.

Para ver que V es un $k[X]$-módulo de torsión, tomemos un $v \in V$ cualquiera y consideremos la familia de elementos de V siguiente:

$$v, f(v), f^2(v), f^3(v), \ldots$$

Como V es de dimensión finita, la familia anterior ha de ser linealmente dependiente, de donde deducimos la existencia de un polinomio no nulo $p(X) \in k[X]$ tal que $p(X) \cdot v = 0$. □

Consideremos una base $\mathcal{B} = \{u_1, \ldots, u_d\}$ de V (como k-espacio vectorial) y la aplicación $k[X]$-lineal $\pi : k[X]^d \to V$ dada por:

$$\pi(p_1, \ldots, p_d) = \sum_{i=1}^{d} p_i u_i,$$

que es sobreyectiva.

Proposición 6.2.2.– En la situación anterior, sea $M = (a_{ij})$ la matriz de f respecto de $\mathcal{B}$, i.e. $f(u_i) = \sum_{j=1}^{d} a_{ij} u_j$. Entonces las filas de la matriz

$$XI - M = \begin{pmatrix} X - a_{11} & -a_{12} & \ldots & -a_{1d} \\ -a_{21} & X - a_{22} & \cdots & -a_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{d1} & -a_{d2} & \ldots & X - a_{dd} \end{pmatrix}$$

forman un sistema de generadores (y de hecho una base) de $\ker \pi$.

Lema 6.2.3.– Dado $\lambda \in k$, el $k[X]$-módulo $k[X]/((X - \lambda)^n)$ admite una base como k-espacio vectorial $\mathcal{B} = \{e_1, \ldots, e_n\}$ tal que

$$X \cdot e_1 = \lambda e_1 + e_2, \ldots, X \cdot e_{n-1} = \lambda e_{n-1} + e_n, X \cdot e_n = \lambda e_n,$$

o lo que es lo mismo, la forma matricial de la multiplicación por X respecto de la base $\mathcal{B}$ es

$$\begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 & 0 \\ 0 & \lambda & 1 & \ldots & 0 & 0 \\ 0 & 0 & \lambda & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & \lambda & 1 \\ 0 & 0 & 0 & \ldots & 0 & \lambda \end{pmatrix}.$$

Nota 6.2.4.– El teorema de estructura aplicado al $k[X]$-módulo V ($k[X]$ es un D.I.P.) (teoremas 6.1.5, 6.1.13, corolario 6.1.12) junto con la proposición 6.2.2 y el lema 6.2.3 nos permiten dar una nueva prueba del Teorema de Jordan en el caso de que k sea algebraicamente cerrado, o si se quiere, en el caso en que todos los autovalores de f estén en k. Es más, el teorema 6.1.13 nos proporciona un método de cálculo de la forma de Jordan.

En el caso $k = \mathbb{R}$ también podemos obtener una prueba de la existencia de la forma canónica real, así como un método de cálculo.