Tema 13.- Teorema de estructura de los módulos finitamente generados sobre un D.I.P.. Aplicaciones

13.1 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 13.1.1.– Todo conjunto Ω no vacío de ideales de A tiene algún elemento maximal (relativo a Ω).

PRUEBA: Aunque este resultado puede probarse a través de la noción general de *anillo noetheriano* y usando el lema de Zorn, vamos a dar una prueba que evita éste último.
1) Veamos primeramente que para cada ideal $I \subset A$ no nulo, el conjunto $\nu(I) = \{J \subset A \mid J \text{ es ideal de } A\ , I \subset J\}$ es finito.

Si $I = A$, el resultado es obvio. Supongamos $I \neq A$. Como A es un DIP, existe un $a \in A$ no unidad tal que $I = (a)$. Sea $a = p_1^{e_1} \cdots p_r^{e_r}$ la descomposición en factores primos de a (recordemos que todo DIP es DFU). Está claro que los ideales J de A tales que $I \subset J$ son exactamente los ideales de la forma $(p_1^{e_1'} \cdots p_r^{e_r'})$, con $0 \leq e_i' \leq e_i$, $i = 1, \ldots, r$, y por tanto son un número finito.

2) En segundo lugar, observemos que todo conjunto finito parcialmente ordenado, posee elementos maximales. Basta proceder por inducción sobre el cardinal del conjunto.[1]

3) Probemos ahora el lema. Si Ω se reduce al conjunto formado por el ideal 0, está claro que este ideal sería un elemento maximal de Ω.[2]

Supongamos ahora que Ω no se reduce al conjunto formado por el ideal 0. Entonces existirá un $I \in \Omega$, $I \neq 0$. Según hemos visto en 1), el conjunto $\nu(I) \cap \Omega$ es finito. Pero $\nu(I) \cap \Omega$ es un conjunto parcialmente ordenado por la inclusión, y por 2), posee algún elemento maximal. Ahora bien, cualquier elemento maximal en $\nu(I) \cap \Omega$ es también maximal en Ω. □

LEMA 13.1.2.– Sean $v_1, \ldots, v_m \in A^n$. Entonces los v_i son A-linealmente equivalentes (en A^n) si y sólo si son K-linealmente independientes en K^n.[3]

DEFINICIÓN 13.1.3.– Dado un subconjunto cualquiera no vacío $S \subset A^n$, definimos el *rango* de S, que notaremos $\mathrm{rg}(S)$, 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 vetorial de K^n generado por S.

[1] Obsérvese que es este resultado el que nos permite evitar el uso del lema de Zorn.
[2] Con más generalidad, Si Ω es finito, el resultado es una consecuencia directa de 2).
[3] Este resultado es válido siempre que A sea un dominio de integridad.

LEMA 13.1.4.–

1. Si $S \subset A^n$, entonces $\mathrm{rg}(S) \leq n$.
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 $\mathrm{rg}(A^n) = n$.
4. Si $M_1, M_2 \subset A^n$ son dos submódulos tales que $M_1 \cap M_2 = 0$, entonces $\mathrm{rg}(M_1 \oplus M_2) = \mathrm{rg}(M_1) + \mathrm{rg}(M_2)$.

PROPOSICIÓN 13.1.5.– 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. $u(e) = 1$
2. $M = (Ae) \oplus \ker u$
3. $M' = (Aae) \oplus (M' \cap \ker u)$.

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 de todos los ideales de A de la forma $u(M') = Aa_u$, para algún $u \in \mathrm{Hom}_A(M, A)$. Por el lema 13.1.1, 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 $\pi_i : M \to A$, $i = 1, \ldots, n$, 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) Dada 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 $\pi_i(e')$, $i = 1, \ldots, n$. Pongamos $\pi_i(e') = b_i a_{u_0}$, $b_i \in A$ y sea $e = (b_1, \ldots, b_n) \in A^n = M$. 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 $b \in B$ 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 13.1.6.– 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 $\{e_1, \ldots, e_n\}$ de M y unos elementos $a_1, \ldots, a_q \in A - \{0\}$ únicos salvo asociados (independientes de la base anterior) tales que:

(b-1) $\{a_1e_1, a_2e_2, \ldots, a_qe_q\}$ 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 $\operatorname{rg}(M') = q \geq 1$. Aplicando la proposición anterior tenemos que $M' = (Aae) \oplus (M' \cap \ker u)$, y por el lema 13.1.4 deducimos que $\operatorname{rg}(M' \cap \ker u) = q - 1$. Por la hipótesis de inducción, $M' \cap \ker u$ es libre, y por tanto M' también.

Para demostrar (b) procederemos por inducción sobre $n = \operatorname{rg} M$. 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 $\operatorname{rg} M = n$. Aplicando de nuevo la proposición anterior y el lema 13.1.4 deducimos que $\ker u$ es libre de rango $n-1$ y que $\operatorname{rg}(M' \cap \ker u) = q-1$. 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 $a_2 = v(a_2e_2) \in v(M') = Aa_1$.

`falta la unicidad` □

NOTA 13.1.7.– 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 la tesis del teorema anterior es una reformaulación del hecho de que A es un dominio de integridad y que todos sus ideales son principales.

COROLARIO 13.1.8.– Si E es un A-módulo finitamente generado no nulo, entonces existen unos ideales $\mathfrak{a}_n \subset \mathfrak{a}_{n-1} \subset \cdots \subset \mathfrak{a}_2 \subset \mathfrak{a}_1 \subset A$, con $\mathfrak{a}_1 \neq A$, tales

que:

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

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, basta tomar $\mathfrak{a}_i = Aa_i$, $i = 1, \ldots, q$ y $\mathfrak{a}_i = 0$ para $q < i \leq n$.

□

DEFINICIÓN 13.1.9.– 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 13.1.10.– Dado un A-módulo M, el conjunto de sus elementos de torsión $\tau(M)$ es un submódulo de M.

COROLARIO 13.1.11.– Todo A-módulo finitamente generado es suma directa de su módulo de torsión $\tau(M)$ 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 13.1.12.– Dado un A-módulo M finitamente generado existen unos enteros $q, r \geq 0$, unos ideales primos $\mathfrak{p}_i \subset A$ no nulos y unos enteros $s_i \geq 1$, $i = 1, \ldots, s$, tales que:

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

PRUEBA: Basta tener en cuenta que si $\mathfrak{a}$ es un ideal propio de A, de que A sea un DIP deducimos que existen 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

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

Notemos que el isomorfismo del enunciado establece otro isomorfismo

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

□

13.2 Aplicaciones

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

$$(\sum_{i=1}^{m} a_i X^i) \cdot v := \sum_{i=1}^{m} a_i f^i(v)$$

para todo polinomio $\sum_{i=1}^{m} a_i X^i \in k[X]$ y todo $v \in V$.

LEMA 13.2.1.– El $k[X]$-módulo V anterior es f.g. y de torsión.

LEMA 13.2.2.– Dado $\lambda \in k$, el $k[X]$-módulo $k[X]/((X-\lambda)^n)$ admite una base como k-espacio vectorial $\{e_1, \ldots, e_n\}$ tal que

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

NOTA 13.2.3.– El teorema de estructura del $k[X]$-módulo V ($k[X]$ es un D.I.P.) nos permite 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.
En el caso $k = \mathbb{R}$ también obtenemos una prueba de la existencia de la forma canónica real.