Decomposizione primaria di moduli su un PID e teorema di Jordan

Sia A un PID (un dominio ad ideali principali). Allora è noto che A è un UFD (dominio a fattorizzazione unica). Se M è un A-modulo, con ${}^{(\lambda)}M$ si indica l'insieme $\{m \in M \mid \lambda m = 0\}$. Si verifica immediatemante che ${}^{(\lambda)}M$ è un sottomodulo di M (${}^{(\lambda)}M$ è il nucleo dell'endomorfismo di M dato da $f(m) = \lambda m$). Se $\nu \in A$ è tale che $\nu m = 0$ per ogni $m \in M$, ν si dice un annullatore di M. L'insieme di tutti gli annullatori di M è un ideale di A che si indica con $\mathrm{Ann}(M)$, quindi è un ideale principale e un suo generatore (unico, a meno di elementi invertibili), si dice l'annullatore (minimale) di M.

Lemma 1 *Sia M un A-modulo su un dominio ad ideali principali. Sia ν un annullatore di M. Se $\nu = \lambda\mu$ con λ e μ primi tra loro, allora $M = {}^{(\lambda)}M \oplus {}^{(\mu)}M$.*

Dim.: Se λ, μ sono primi tra loro, allora generano l'ideale (1) di A, quindi esistono $\alpha, \beta \in A$ tali che $1 = \alpha\lambda + \beta\mu$. Allora $m = \lambda\alpha m + \mu\beta m$. Da questo segue che $M = {}^{(\lambda)}M + {}^{\mu}M$. Inoltre, se se $m \in {}^{(\lambda)}M \cap {}^{(\mu)}M$, allora $\lambda m = 0 = \mu m$, quindi $m = 0$. Pertanto $M = {}^{(\lambda)}M \oplus {}^{(\mu)}M$.

Lemma 2 *Siano M_1 e M_2 due A-moduli e sia $\mathrm{Ann}(M_1) = (\lambda)$ e $\mathrm{Ann}(M_2) = (\mu)$, con λ, μ primi tra loro. Allora $\mathrm{Ann}(M_1 \oplus M_2) = (\lambda\mu)$.*

Dim.: Sia $\mathrm{Ann}(M_1 \oplus M_2) = (\sigma)$. Se $m \in \mathrm{Ann}(M_1) \oplus \mathrm{Ann}(M_2)$, allora, per ogni $m \in \mathrm{Ann}(M_1 \oplus M_2)$, vale: $\lambda\mu m = \lambda\mu(m_1 + m_2) = 0$ (con $m_i \in M_i$), quindi $\lambda\mu \in (\sigma)$, cioè σ divide $\lambda\mu$. In particolare, $\sigma m_1 = 0$ per ogni $m_1 \in M_1$ e $\sigma m_2 = 0$ per ogni $m_2 \in M_2$. Quindi $\sigma \in (\lambda)$ e $\sigma \in (\mu)$. Quindi sia λ, sia μ dividono σ. Essendo λ e μ primi tra loro, il loro prodotto divide σ.

Definizione Sia $p \in A$ un elemento primo. Un A-modulo M si dice un p-modulo se ogni elemento di M ha ordine p^α per un opportuno $\alpha \in \mathbb{N}$. Un A modulo M si dice *primario* se esiste un p primo tale che M è un p-modulo.

Ad esempio lo $\mathbb{Z}$-modulo $\mathbb{Z}_8$ è primario (per la precisione, è un 2-modulo).

Sia M un A-modulo e $p \in A$ primo. L'insieme

$$T_p(M) = \{m \in M \mid \text{esiste } \alpha \in \mathbb{N} : \mathrm{ord}(m) = p^\alpha\}$$

risulta essere un sottomodulo di M, è un p-modulo, ed è il più grande p-modulo contenuto in M.

Si ricordi che se $p, p' \in A$ sono due elementi primi, allora o sono primi tra loro o sono associati.

Teorema 3 *(Teorema della decomposizione primaria di moduli su un PID). Sia M un A-modulo fintamente generato e di torsione. Allora M è somma diretta di moduli primari. Più precisamente, se ν è l'annullatore minimale di M e se $\nu = up_1^{\alpha_1} \cdots p_k^{\alpha_k}$ con $p_1, \ldots, p_k$ primi non associati, allora:*

$$M = T_{p_1}(M) \oplus \cdots \oplus T_{p_k}(M) \tag{1}$$

e la decomposizione è unica.

Dim.: Per brevità, possiamo assumere $u = 1$. Induzione su k. Se $k = 1$ non c'è nulla da provare. Consideriamo allora $v = \lambda\mu$ dove $\lambda = p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}}$ e $\mu = p_k^{\alpha_k}$. Allora, dal lemma 1, segue che $M = {}^{(\lambda)}M \oplus {}^{(\mu)}M$. Vale: ${}^{(\mu)}M = \{m \in M \mid p_k^{\alpha_k} m = 0\} \subseteq T_{p_k}(M)$. Se, viceversa, $m \in T_{p_k}(M)$, allora esiste un β tale che $p_k^{\beta} m = 0$ e possiamo assumere che β sia minimo possibile (cioè assumiamo che p_k^{β} sia l'annullatore minimale di m), allora $\beta \leq \alpha_k$ (infatti $\nu m = 0$, quindi $\nu \in \left(p_k^{\beta}\right)$, e pertanto $\beta \leq \alpha$). Quindi ${}^{(\mu)}M = T_{p_k}(M)$. Sia $\mathrm{Ann}({}^{(\lambda)}M) = (\sigma)$. Per come è definito il modulo ${}^{(\lambda)}M$, σ divide λ, quindi σ e μ sono primi tra loro e per il lemma 2, $\sigma = p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}}$. Pertanto, per ipotesi induttiva:

$$ {}^{(\lambda)}M = T_{p_1}({}^{(\lambda)}M) \oplus \cdots \oplus T_{p_{k-1}}({}^{(\lambda)}M) $$

Per ottenere la la decomposizione voluta, basta provare che $T_{p_i}({}^{(\lambda)}M) = T_{p_i}(M)$. Chiaro che se $m \in T_{p_i}({}^{(\lambda)}M)$, allora $m \in T_{p_i}(M)$. Sia ora $m \in T_{p_i}(M)$, allora esiste un β tale $p_i^{\beta} m = 0$ e anche ora, come già fatto in precedenza, possiamo assumere che β sia minimo, quindi p_i^{β} è l'annullatore minimale di m. Pertanto $\nu \in (p_i^{\beta})$, quindi $\beta \leq \alpha_i$ e pertanto $\lambda m = 0$, cioè $m \in {}^{(\lambda)}M$. Infine l'unicità segue dall'unicità dei $T_{p_i}(M)$.

Sia M un modulo finitamente generato e di torsione. Se decomponiamo M come in (1), possiamo ulteriormente decomporre ciascun $T_{p_i}(M)$ in somma diretta di ciclici (usando il teorema di decomposizione di un modulo in somma diretta di ciclici). Gli ordini dei moduli ciclici in cui si decompone $T_{p_i}(M)$ sono potenze di p_i (il teorema di decomposizione afferma poi che l'ordine di ciascun modulo ciclico divide il successivo, ma in questo caso, essendo gli ordini tutti potenze di p_i questa condizione è sempre soddisfatta). Abbiamo quindi:

Teorema 4 *(Decomposizione primaria ciclica). Sia M un A-modulo di torsione e finitamete generato (con A PID). Allora M è somma diretta di moduli ciclici primari. La lista degli ordini degli addendi diretti di M è una lista di potenze di elementi primi di A ed è univocamente determinata da M (a meno di elementi unitari e di permutazioni).*

Definizione Le potenze dei primi della lista degli ordini degli addendi diretti di un modulo M stabilita nel precedente teorema si chiama lista dei *divisori elementari* del modulo M.

Il teorema ora enunciato si particolarizza per i gruppi abeliani finiti: ogni gruppo abeliano finito è somma diretta di gruppi ciclici i cui ordini sono potenze di numeri primi. La lista è unica, a meno di permutazioni.

Cerchiamo ad esempio tutti i possibili gruppi abeliani finiti di ordine 180. Dobbiamo cercare tutte le possibili liste di divisori elementari dei gruppi di ordine $180 = 2^4 \cdot 3^2 \cdot 5$, che sono quindi: $(4, 9, 5), (2, 2, 9, 5), (4, 3, 3, 5), (2, 2, 3, 3, 5)$ e quindi tutti i possibili gruppi abeliani di ordine 180, a meno di isomorfismi,

sono i seguenti:

$$\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5,$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5,$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5,$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

Se volessimo classificare i gruppi abeliani di ordine 180 utilizzando il teorema di decomposizione in moduli ciclici con i fattori invarianti, avremmo invece i seguenti gruppi:

$$\mathbb{Z}_{180}, \quad \mathbb{Z}_2 \oplus \mathbb{Z}_{90}, \quad \mathbb{Z}_3 \oplus \mathbb{Z}_{60}, \quad \mathbb{Z}_6 \oplus \mathbb{Z}_{30}$$

Interpretiamo ora il teorema 4 nell'ambito delle matrici con coefficienti in un campo K (o degli endomorfismi di spazi vettoriali).

Dal teorema 4 e ricordando i risultati visti sulla decomposizione di una matrice in somma diretta di matrici compagne, otteniamo:

Teorema 5 *Data una matrice B quadrata di ordine n su un campo K, esiste una lista*

$$L = (p_1^{\alpha_{11}}, p_1^{\alpha_{12}}, \ldots, p_1^{\alpha_{1r_1}}, p_2^{\alpha_{21}}, p_2^{\alpha_{22}}, \ldots, p_2^{\alpha_{2r_2}}, \ldots, p_s^{\alpha_{s1}}, p_s^{\alpha_{s2}}, \ldots, p_s^{\alpha_{sr_s}})$$

dove $p_1, p_2, \ldots, p_s$ sono polinomi monici irriducibili di $K[x]$ e $\alpha_{ij} \leq \alpha_{i\,j+1}$. L è tale che la matrice B è la somma diretta delle matrici compagne dei polinomi $p_i^{\alpha_{jh}}$. Inoltre la lista L è univocamente determinata da B, a meno di permutazioni.

La lista delle potenze di primi univocamente determinata da B (a meno di qualche permutazione) si chiama lista dei *divisori elementari* di B.

Corollario 6 *Sia p un polinomio monico irriducibile in $K[x]$ (con K campo). Allora la matrice compagna di p^e ha come divisore elementare la lista con unico elemento p^e. Se due matrici B_1 e B_2 hanno come divisori elementari due liste L_1 e L_2 allora la matrice $B_1 \oplus B_2$ ha come divisori elementari la lista (L_1, L_2) (cioè la giustapposizione delle due liste).*

Se M è un $K[x]$-modulo, si ricordi che ad esso si associa uno spazio vettoriale V_M che, come gruppo abeliano, è M stesso e il prodotto esterno $K \times V_M \longrightarrow V_M$ è dato dalla restrizione del prodotto esterno del modulo M. Inoltre, la struttura di $K[x]$-modulo permette di definire un endomorfismo $t : V_M \longrightarrow V_M$ dato da $t(m) = x \cdot m$.

Lemma 7 *Sia $p = x - \lambda \in K[x]$ e sia C un $K[x]$-modulo ciclico di ordine p^e. Sia (V_C, t) lo spazio vettoriale e l'endomorfismo associati a C. Allora esiste in V_C una base tale che la matrice associata a t, rispetto a tale base, è della forma:*

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

Dim.: Il modulo ciclico C è isomorfo a $K[x]/((x-\lambda)^e)$. Sia c_0 un generatore del modulo ciclico C. Poiché $(x-\lambda)^e$ è l'ordine di C, vale: $(x-\lambda)^e c_0 = 0$ e $(x-\lambda)^i c_0 \neq 0$ se $i < e$. Consideriamo i vettori $b_1 = c_0$, $b_2 = (t-\lambda I)(c_0)$, $b_e = (t-\lambda I)b_{e-1}$ (I indica l'omomorfismo identico). Questi vettori sono linearmente indipendenti su K (se ci fosse una loro combinazione lineare nulla, avremmo che esiste un polinomio di grado più basso di e che annulla c_0 e quindi C). Se calcoliamo la matrice associata a t relativa a questa base, otteniamo:
$t(b_1) = t(c_0) - \lambda c_0 + \lambda c_0 = (t-\lambda I)c_0 + \lambda b_1 = b_2 + \lambda b_1$
$t(b_2) = t(b_2) - \lambda b_2 + \lambda b_2 = (t-\lambda I)b_2 + \lambda b_2 = b_3 + \lambda b_2$
...
$t(b_e) = t(b_e) - \lambda b_e + \lambda b_e = (t-\lambda I)b_e + \lambda b_e = (t-\lambda I)^e c_0 + \lambda b_e = \lambda b_e$.
Questo prova che la matrice associata a t rispetto alla base $b_1, \ldots, b_e$ è della forma enunciata.
Definizione Una matrice della forma descritta sopra, si chiama matrice elementare di Jordan.

Si noti che il polinomio caratteristico di una matrice elementare di Jordan vale $(x-\lambda)^e$ e coicide con il polinomio minimo.

Teorema 8 *(Forma canonica di Jordan) Sia B una matrice con polinomio caratteristico prodotto di potenze di polinomi irriducibili di grado 1. Allora B è simile ad una matrice somma diretta di matrici elementari di Jordan.*

Dim.: La dimostrazione è un'immediata conseguenza dei risultati precedenti.