Fogli NON riletti. Grazie per ogni segnalazione di errori.

L'esempio qui sviluppato vuole mostrare in concreto il significato dei risultati trattati a lezione e qui velocemente riassunti. Si assume che A sia un dominio d'integrità ad ideali principali (PID).

Teorema 1 *Sia M un A modulo finitamente generato e di torsione. Allora esistono (univocamente determinati) $\mu_1, \ldots, \mu_k \in A$ ognuno multiplo del succesivo tali che*

$$M = C_1 \oplus \cdots \oplus C_k$$

ove C_i sono moduli ciclici di ordini μ_i (quindi $C_i = A/(\mu_i)$).

Gli elementi $\mu_1, \ldots, \mu_k$ di A si chiamano gli invarianti fondamentali di M. Il primo di essi è l'annullatore minimale di M.

Se V è uno spazio vettoriale di dimensione finita su un campo K e $t : V \longrightarrow V$ è un endomorfismo di V, alla coppia (V, t) si può associare un $K[x]$ modulo M_V nel seguente modo: come gruppo abeliano M_V coincide con $(V, +)$, il prodotto esterno $K[x] \times M_V \longrightarrow M_V$ è dato da $x \cdot m = t(m)$, $x^2 \cdot (m) = t(t(m))$, ... e poi esteso per linearità. Viceversa, Se M è un $K[x]$-modulo, esso è in modo ovvio un K-spazio vettoriale (che indichiamo con V_M) e si può definire un endomorfismo $t_x : V_M \longrightarrow V_M$ dato da $t_x(m) = x \cdot m$. Vi è quindi una corrispondenza biunivoca tra coppie (V, t) (con V spazio vettoriale su K e t endomorfismo di V) e $K[x]$-moduli M_V.

Proposizione 2 *Il polinomio minimo di t corrisponde all'annullatore minimale di M_V.*

Proposizione 3 *Nella corrispondenza stabilita sopra, N è sottomodulo di M se e solo se $t(N_V) \subseteq N_V$, Mentre N è ciclico generato da $c \in M$ se e solo se N_V, come K-spazio vettoriale, è generato da $x, t(x), t^2(x), \ldots$.*

Proposizione 4 *Sia g polinomio monico di $K[x]$. Un $K[x]$-modulo C è ciclico di ordine g se e solo se lo spazio vettoriale V_C ha una base per cui la matrice di t_x è la matrice compagna B_g di g.*

Teorema 5 *Sia $t : V \longrightarrow V$ un endomorfismo. Esistono $g_1, \ldots, g_k \in K[x]$ polinomi monici univocamente determinati, ognuno dei quali è multiplo del successivo, tali che V ha una base rispetto a cui la matrice di t è della forma:*

$$B_{g_1} \oplus B_{g_2} \oplus \cdots \oplus B_{g_k}$$

Corollario 6 *Il polinomio g_1 è il polinomio minimo di t. Il prodotto $g_1 \cdots g_k$ è (a meno di segno) il polinomio caratteristico di t. La somma dei gradi dei polinomi g_i è la dimensione dello spazio vettoriale V.*

Corollario 7 *Ogni matrice quadrata B con entrate in un campo K è simile ad esattamente una matrice della forma*

$$B_{g_1} \oplus B_{g_2} \oplus \cdots \oplus B_{g_k}$$

(con i g_i come sopra).

La matrice $B_{g_1} \oplus B_{g_2} \oplus \cdots \oplus B_{g_k}$ si chiama forma canonica razionale della matrice B.

Se M è un A-modulo e se $\lambda \in A$, con ${}^{(\lambda)}M$ si indica il nucleo dell'omomorfismo $\phi_\lambda : M \longrightarrow M$ dato da $\phi_\lambda(m) = \lambda m$.

Lemma 8 *Sia M un A-modulo e sia $\sigma \in A$ un annullatore di M. Se $\sigma = \lambda\mu$ con λ e μ primi tra loro, allora vale:*

$$M = {}^{(\lambda)}M \oplus {}^{(\mu)}M.$$

Sia $p \in A$ primo. Un A modulo M si dice p-modulo se ogni elemento di M ha ordine una potenza di p. Un modulo si dice primario, se è un p-modulo per qualche p. Con $T_p(M)$ si indica l'insieme degli elementi del modulo M che hanno ordine qualche potenza di p. $T_p(M)$ è un p-modulo ed è il più grande p-modulo contenuto in M.

Teorema 9 *(decomposizione primaria) Sia M un A modulo finitamente generato e di torsione di ordine ν. Sia $\nu = p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}$ la scomposizione di ν in fattori primi distinti. Allora*

$$M \simeq T_{p_1}(M) \oplus \cdots \oplus T_{p_k}(M)$$

Inoltre i moduli $T_{p_1}(M)$ sono univocamente determinati da M.

Teorema 10 *Sia M un A-modulo finitamente generato e di torsione. Allora M è isomorfo ad una somma diretta di moduli ciclici primari (quindi della forma $A/(p_i^{\alpha_i})$), in modo essenzialmente unico.*

Le potenze di primi $p_1^{\alpha_1}, \ldots, p_l^{\alpha_l}$ che compaiono nel teorema precedente si chiamano i divisori elementari di M.

Corollario 11 *Ogni matrice B quadrata di ordine n su un campo K è simile alla somma diretta di matrici compagne della forma B_{p^α} (con p primo) in modo essenzialmente unico.*

Le potenze di primi $p_1^{\alpha_1}, \ldots, p_l^{\alpha_l}$ che compaiono nel lemma precedente si chiamano i divisori elementari di B. Il loro prodotto è, a meno di segno, il polinomio caratteristico di B. Una matrice quadrata della forma

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

si dice matrice elementare di Jordan.

Teorema 12 *(Forma canonica di Jordan). Supponiamo che il polinomio caratteristico della matrice quadrata B su un campo K sia prodotto di fattori lineari. Allora B è simile ad una somma diretta di matrici elementari di Jordan, una per ciascun divisore elementare di B.*

Esempio

Partiamo dal campo $K = \mathbb{Q}$, consideriamo lo spazio vettoriale $V = \mathbb{Q}^5$ e l'endomorfismo di V dato dalla matrice

$$B = \begin{pmatrix} -83 & 155 & 199 & 45 & -98 \\ -81 & 153 & 199 & 45 & -99 \\ -19 & 35 & 44 & 10 & -21 \\ 215 & -403 & -524 & -118 & 253 \\ -1 & 3 & 3 & 1 & -4 \end{pmatrix}$$

La matrice B dà luogo all'endomorfismo: $t : V \longrightarrow V$ definito da

$$\begin{aligned} t(a,b,c,d,e) &= B\,{}^t(a,b,c,d,e) \\ &= \begin{pmatrix} -83\,a + 155\,b + 199\,c + 45\,d - 98\,e \\ -81\,a + 153\,b + 199\,c + 45\,d - 99\,e \\ -19\,a + 35\,b + 44\,c + 10\,d - 21\,e \\ 215\,a - 403\,b - 524\,c - 118\,d + 253\,e \\ -a + 3\,b + 3\,c + d - 4\,e \end{pmatrix} \end{aligned}$$

(l'endomorfismo è riferito alla base canonica).

L'endomorfismo t definisce un prodotto esterno, come indicato precedentemente:

$$\mathbb{Q}[x] \times M_V \longrightarrow M_V$$

dato da:

$$\begin{aligned} (k,(a,b,c,d,e)) &\mapsto (ka,kb,kc,kd,ke) \ \text{ per ogni } k \in \mathbb{Q} \text{ e ogni } (a,b,c,d,e) \in M_V, \\ (x,(a,b,c,d,e)) &\mapsto t(a,b,c,d,e) \\ & \qquad \text{per ogni } (a,b,c,d,e) \in M_V \\ (x^2,(a,b,c,d,e)) &\mapsto t(t(a,b,c,d,e)) = \dots \\ \dots \quad & \quad \dots \end{aligned}$$

e l'operazione di prodotto esterno viene poi estesa per linearità. (M_V è, come insieme e gruppo abeliano, coincidente con V).

Poiché V è di dimensione finita, sappiamo che M_V è un modulo di torsione e poiché V, come spazio vettoriale ha dimensione 5, sappiamo che il polinomio minimo di t (e di B) sarà al massimo di grado 5 e sarà anche l'annullatore minimale del modulo M_V.

Fatto 13 *L'annullatore minimale di M_V vale:*

$$g = x^4 + 6\,x^3 + 13\,x^2 + 12\,x + 4 = (x+2)^2(x+1)^2$$

Infatti: consideriamo il generico polinomio di grado al più 5: $f = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. Calcoliamo $f \cdot (a, b, c, d, e)$, cioè il prodotto esterno di f per un generico elemento di M_V. Usando la legge del prodotto esterno definita sopra si può calcolare esplicitamente $f \cdot (a, b, c, d, e)$ e vedere per quali valori di $a_0, \dots, a_5$ questo prodotto si annulla per ogni valore di a, b, c, d, e. Si ottengono così dei polinomi lineari in $a_0, \dots, a_5$ e in a, b, c, d, e che devono essere 0 per ogni valore di a, b, c, d, e. Questo si traduce in un sistema lineare nelle variabili $a_0, \dots, a_5$ dalle cui soluzioni si trova che il polinomio f di grado più piccolo possibile è il polinomio g scritto sopra.

Cerchiamo ora gli invarianti fondamentali di M_V e la sua decomposizione in somma diretta di ciclici (teorema 1).

Innanzitutto bisogna trovare un elemento di M_V di ordine g. Ad esempio si vede che l'elemento $m = (1, 0, 0, 0, 0)$ ha per annullatore g, quindi sarà:

$$M_V = \langle m \rangle \oplus \cdots = K[x]/(g) \oplus \cdots$$

(dove i puntini indicano che bisogna trovare ancora degli addendi). Per ora sappiamo che il primo invariante fondamentale è g. Il modulo ciclico generato da m è anche un sottospazio vettoriale di V che ha, come generatori,

$$\begin{aligned}
v_1 = m &= (1, 0, 0, 0, 0) \\
v_2 = xm &= (-83, -81, -19, 215, -1) \\
v_3 = x^2m &= (326, 323, 77, -869, 2) \\
v_4 = x^3m &= (-971, -967, -233, 2621, -3) \\
&\dots
\end{aligned}$$

(v. proposizione 3). Si verifica che x^4m è linearmente dipendente da v_1, v_2, v_3, v_4, mentre v_1, v_2, v_3, v_4 sono linearmente indipendenti, quindi la dimensione di $\langle m \rangle$ come K-spazio vettoriale, è 4. Poiché M_V, come K-spazio vettoriale, ha dimensione 5, ci deve essere ancora un invariante fondamentale h.

Si tratta di trovare un sottomodulo N di M_V tale che $M_V = \langle m \rangle \oplus N$ (per una costruzione teorica precedentemente fatta, si sa che N deve esistere). Senza ripercorrere tutta la costruzione del modulo N, possiamo osservare che h deve essere un divisore di g, quindi ci sono poche possibilità. Proviamo ad esempio a prendere $h = x + 1$. Cerchiamo se c'è un elemento di M_V che ha ordine $x + 1$. Allora si tratta di trovare a, b, c, d, e tali che $(x+1) \cdot (a, b, c, d, e) = 0$. Si trovano le seguenti soluzioni: $a = \lambda, b = 0, c = 0, d = 4\lambda, e = \lambda$. In particolare abbiamo che l'insieme di tutti gli elementi di M_V che hanno ordine $x + 1$ è dato da:

$$N_1 = \{\lambda(1, 0, 0, 4, 1) \mid \lambda \in K\} \tag{1}$$

In particolare l'elemento $m_1 = (1, 0, 0, 4, 1)$ è un elemento di ordine $x+1$. Però si verifica che m_1 è combinazione lineare di v_1, v_2, v_3, v_4, quindi $m_1 \in \langle m \rangle$, quindi $h = x + 1$ non è una scelta corretta. Allora proviamo con $h = x + 2$. In questo caso si trova che la totalità degli elementi di M_V di ordine $x + 2$ è dato da:

$$N_2 = \{\lambda(-3, 1, -2, 0, 0) + \mu(-16, 0, -9, 11, 0) \mid \lambda, \mu \in K\} \tag{2}$$

Si vede che, ad esempio l'elemento $m_1 = (-19, 1, -11, 11, 0)$ (somma dei due generatori di N_2) che è di ordine $x+2$ e non sta in $\langle m \rangle$. Ovviamente una base di $\langle m_1 \rangle$ come K spazio vettoriale è data da $v_5 = m_1$, poiché $\langle m_1 \rangle$ è di dimensione 1 su K (e infatti si vede subito che $xm_1 = 2m_1$).

Pertanto vale:

Fatto 14 *In accordo con il teorema 1, vale:*

$$M_V = \langle m \rangle \oplus \langle m_1 \rangle = K[x]/(g) \oplus K[x]/(h)$$

Gli invarianti fondamentali di M_V *sono quindi* g *e* h*.*

Dalla decomposizione di M_V ora scritta si ricava una base di V data da v_1, v_2, v_3, v_4, v_5. Rispetto a questa base, l'endomorfismo t (e la matrice B) sono rappresentati dalla seguente matrice:

$$\begin{pmatrix} 0 & 0 & 0 & -4 \\ 1 & 0 & 0 & -12 \\ 0 & 1 & 0 & -13 \\ 0 & 0 & 1 & -6 \end{pmatrix} \oplus (-2) = \begin{pmatrix} 0 & 0 & 0 & -4 & 0 \\ 1 & 0 & 0 & -12 & 0 \\ 0 & 1 & 0 & -13 & 0 \\ 0 & 0 & 1 & -6 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

e questa è la forma canonica razionale di B (somma diretta della matrice compagna di g e della matrice compagna di h). Il polinomio caratteristico di B, cioè $\det(B - xI)$, vale $(x+1)^2(x+2)^3$ che coincide proprio con gh (a meno di segno) (cfr. teorema 5, lemma 6, corollario 7).

Vediamo ora la decomposizione in moduli primari di M_V. Dalla definizione del modulo N_1 definito in (1), abbiamo che tutti gli elementi di N_1 sono di ordine $x+1$. Cerchiamo in M_V elementi di ordine $(x+1)^2$. Calcolando $(x+1)^2 \cdot (a, b, c, d, e)$ si ottiene che questo prodotto è zero se (a, b, c, d, e) sta nel K-spazio vettoriale generato da $(1, -4, 4, 0, 1)$, $(0, 1, -1, 1, 0)$. Poiché nell'annullatore di M_V il fattore $(x+1)$ compare a grado 2, non ci possono essere in M_V elementi di ordine $(x+1)^\alpha$ con $\alpha > 2$. [Infatti: se ci fosse un elemento m di ordine $(x+1)^\alpha$ con $\alpha > 2$, poiché $(x+1)^2(x+2)^3$ è sicuramente un annullatore di m, avremmo che $(x+1)^2(x+2)^3 \in \operatorname{ord}(m) = ((x+1)^\alpha)$, quindi $(x+1)^2(x+2)^3 = \sigma(x+1)^\alpha$ che è assurdo]. Si noti poi che il generatore di N_1 è combinazione lineare dei due elementi di V scritti sopra, pertanto abbiamo provato che:

Fatto 15 *Il modulo* $T_{x+1}(M_V)$*, il più grande* $(x+1)$*-modulo contenuto in* M_V*, è dato da:*

$$T_{x+1}(M_V) = \{\lambda(1, -4, 4, 0, 1) + \mu(0, 1, -1, 1, 0) \mid \lambda, \mu \in K\}$$

Un analogo conto prova che gli elementi di ordine $x+2$ in M_V sono N_2 e gli elementi annullati da $(x+2)^2$ sono generati, come spazio vettoriale da:

$$(3, 1, 0, 0, 0),\ (1, 0, 0, 1, 0),\ (3, 0, 1, 0, 0).$$

Anche tutti gli elementi di M_V che sono annullati da $(x+2)^3$ sono generati dai 3 vettori scritti sopra; inoltre i generatori di N_2 sono combinazione dei tre vettori indicati, quindi abbiamo:

Fatto 16 *Il modulo $T_{x+2}(M_V)$ è dato da:*

$$T_{x+2}(M_V) = \{\lambda(3,1,0,0,0) + \mu(1,0,0,1,0) + \nu(3,0,1,0,0) \mid \lambda, \mu, \nu \in K\}$$

Pertanto

Fatto 17 *La decomposizione di M_V in moduli primari è data da:*

$$M_V = T_{x+1}(M_V) \oplus T_{x+2}(M_V).$$

(cfr. teorema 9).

Questa stessa decomposizione poteva essere ottenuta usando il lemma 8, poiché $(x+1)^2(x+2)^2$ è l'annullatore di M_V e quindi vale:

$$M_V = {}^{((x+1)^2)}M_V \oplus {}^{((x+2)^2)}M_V$$

(essendo i due fattori $(x+1)^2$ e $(x+2)^2$ primi tra loro).

Vediamo allora di calcolare ${}^{((x+1)^2)}M_V$ e ${}^{((x+2)^2)}M_V$, che, per definizione, sono il nucleo della mappa $\phi : M_V \longrightarrow M_V$ data da $\phi(m) = (x+1)^2 m$ e, rispettivamente, della mappa $\psi : M_V \longrightarrow M_V$ data da $\psi(m) = (x+2)^2 m$. Quindi $\ker(\phi) = \{m \mid (x+1)^2 \cdot m = 0\}$ e quindi si tratta di trovare i vettori (a,b,c,d,e) tali che $(x+1)^2 \cdot (a,b,d,c,e) = 0$. Questo conto è lo stesso di sopra e ci dà come risultato $T_{x+1}(M_V)$. Analogamente, dal $\ker(\psi)$ si riottiene $T_{x+2}(M_V)$, come doveva essere.

Per ottenere la decomposizione primaria ciclica di M_V dobbiamo ancora decomporre i due moduli $T_{x+1}(M_V)$ e $T_{x+2}(M_V)$ in somma di ciclici (dobbiamo cioè applicare il teorema della decomposizione con gli invarianti fondamentali ai due addendi). Calcoliamo l'ordine di $T_{x+1}(M_V)$ e $T_{x+2}(M_V)$. Il generico elemento di $T_{x+1}(M_V)$ è $(a, -4a+b, 4a-b, b, a)$. Moltiplicando questo elemento per un generico polinomio (di grado massimo 5, ma in verità basta meno) e imponendo che il risultato sia 0 per ogni scelta di a, b, si ottiene un sistema lineare che fornisce l'annullatore di $T_{x+1}(M_V)$. Si trova:

$$\mathrm{Ann}(T_{x+1}(M_V)) = (x+1)^2.$$

Allora dobbiamo cercare un elemento in $T_{x+1}(M_V)$ di ordine $(x+1)^2$. Una scelta possibile è il suo primo generatore: $m_1 = (1,-4,4,0,1)$. Vale: $xm_1 = (-5,4,-4,-16,-5)$ e si vede subito che m_1, xm_1 sono una base di $T_{x+1}(M_V)$. Quindi questo modulo è ciclico, generato da m_1, è di ordine $(x+1)^2$ ed è primario, essendo $x+1$ un primo di $K[x]$.

Analogo calcolo per trovare l'annullatore di $T_{x+2}(M_V)$. Si trova che vale:

$$\mathrm{Ann}(T_{x+2}(M_V)) = (x+2)^2.$$

Cerchiamo, al solito, un elemento di ordine $(x+2)^2$ in $T_{x+2}(M_V)$. Per esempio l'elemento $m_2 = (3,1,0,0,0)$ è di ordine 2. Siccome vale:

$$xm_2 = (-94,-90,-22,242,0), \quad x^2 m_2 = (364,356,88,-968,0)$$

si verifica che m_2 e xm_2 sono linearmente indipendenti, mentre x^2m_2 è combinazione lineare dei due elementi precedenti. Pertanto il modulo ciclico generato da m_2 non è tutto $T_{x+2}(M_V)$, ma solo un suo sottospazio di dimensione 2. Dobbiamo quindi trovare un altro sottomodulo ciclico C di $T_{x+2}(M_V)$ (che deve necessariamente essere di dimensione 1), tale che $T_{x+2}(M_V) = \langle m_2\rangle \oplus C$. L'ordine di C deve essere un fattore di $(x+2)^2$ ma non può essere $(x+2)^2$ perché in questo caso C avrebbe, come spazio vettoriale, dimensione maggiore di 1. Si tratta allora di trovare elementi di $T_{x+2}(M_V)$ di ordine $x+2$. Quindi cerchiamo λ, μ, ν tali che

$$(x+2)\cdot(\lambda(3,1,0,0,0)+\mu(1,0,0,1,0)+\nu(3,0,1,0,0)) = 0$$

Risolvendo le equazioni lineari ottenute, si ottiene che deve essere: $\lambda = -9/22\mu - 1/2\nu$. Allora un elemento di ordine $x+2$ è ad esempio $m_3 = (-2,-10,2,22,0)$ (ottenuto per $\mu = 22, \nu = 2$). Si vede subito che il modulo ciclico generato da m_3 è uno spazio vettoriale di dimensione 1 e, come modulo, è un modulo ciclico primario. Pertanto:

Fatto 18 *La decomposizione di M_V in moduli ciclici primari è:*

$$\begin{aligned} M_V &= \langle m_1\rangle \oplus \langle m_2\rangle \oplus \langle m_3\rangle \\ &= K[x]/((x+1)^2) \oplus K[x]/((x+2)^2) \oplus K[x]/(x+2) \end{aligned}$$

Quindi i divisori elementari sono: $(x+1)^2, (x+2)^2, (x+2)$.

(cfr. teorema 10).

La costruzione fino a qui fatta ci dà una nuova base di V che è:

$$m_1, xm_1, m_2, xm_2, m_3.$$

Rispetto a questa base otteniamo:

Fatto 19 *L'endomorfismo t, rispetto alla base ora indicata, ha per matrice associata la matrice ottenuta come somma diretta delle 3 matrici compagne di $(x+1)^2$, $(x+2)^2$, $x+2$, quindi:*

$$\begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix} \oplus \begin{pmatrix} 0 & -4 \\ 1 & -4 \end{pmatrix} \oplus (-2) = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -4 & 0 \\ 0 & 0 & 1 & -4 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

Analogamente, la matrice B è simile alla somma diretta delle tre matrici compagne scritte sopra (cfr. corollario 11).

Si noti che il polinomio caratteristico di B è prodotto di fattori lineari, quindi la matrice B ha una forma canonica di Jordan. La base rispetto a cui ottenere la forma di Jordan è la seguente: $m_1, (t-(-1)I_2)m_1, m_2, (t-(-2)I_2)m_2, m_3$, cioè

$$w_1 = (1,-4,4,0,1),\ w_2 = (-4,0,0,-16,-4),\ w_3 = (3,1,0,0,0),$$

$$w_4 = (-88, -88, -22, 242, 0), \;\; w_5 = (-2, -10, 2, 22, 0)$$

Poiché vale: $t(w_1) = (7, 1, 0, 16, 4) = -w_2 + w_3$, $t(w_2) = -w_2$, $t(w_3) = -2w_3 + w_4$, $t(w_4) = -2w_4$, $t(w_5) = -2w_5$ si ottiene che la matrice di t riferita alla base $w_1, \dots, w_5$ è la seguente:

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

che è proprio la forma canonica di Jordan della matrice B.