Moduli su un dominio a ideali principali

Maurizio Cornalba

versione 15/5/2013

Sia A un anello commutativo con 1. Indichiamo con A^k il modulo somma diretta di k copie di A. Un A-modulo finitamente generato M si dice *libero* se è isomorfo ad A^k per qualche k; ciò equivale a dire che M ammette una *base*, cioè un sistema di generatori $m_1, \dots, m_k$ linearmente indipendenti, tali cioè che, se $a_1, \dots, a_k$ sono elementi di A con la proprietà che $\sum a_i m_i = 0$, allora $a_1 = \cdots = a_k = 0$.

Lemma 1. *Siano $m_1, \dots, m_k$ una base e $n_1, \dots, n_h$ un sistema di generatori di un A-modulo M. Allora $h \geq k$.*

Il lemma dice, in particolare, che due basi di un A-modulo libero finitamente generato M hanno lo stesso numero di elementi; questo numero viene detto *rango* di M. Il rango di A^k è k. Per dimostrare il lemma, scriviamo

$$m_i = \sum a_{ij} n_j \ , \quad n_r = \sum b_{rs} m_s \, .$$

Se $h < k$, sia U la matrice $k \times k$ il cui elemento di posto i, j è a_{ij} se $j \leq h$ e 0 altrimenti, e sia V la matrice $k \times k$ il cui elemento di posto i, j è b_{ij} se $i \leq h$ e 0 altrimenti. Il prodotto di U e V è la matrice identità $k \times k$. Ciò è assurdo perché da un lato il determinante della matrice identità è 1, dall'altro sarebbe nullo in quanto prodotto di $\det(U)$ e $\det(V)$, che sono nulli.

Diremo che un A-modulo M è *noetheriano* se, data comunque una successione di suoi sottomoduli $N_1 \subset N_2 \subset \cdots \subset N_h \subset \cdots$, si ha che $N_h = N_{h+1} = \cdots$ per h abbastanza grande.

Lemma 2. *Sia M un A-modulo e sia N un suo sottomodulo. Allora M è noetheriano se e solo se lo sono N e M/N.*

Supponiamo M noetheriano. Chiaramente lo è anche N. Data poi una successione di sottomoduli $L_1 \subset L_2 \subset \cdots \subset L_h \subset \cdots$ di M/N, e indicando con $\varphi : M \to M/N$ il passaggio al quoziente, $L_h = L_{h+1}$ se e solo se $\varphi^{-1}(L_h) = \varphi^{-1}(L_{h+1})$. Poiché M è noetheriano, la successione $\varphi^{-1}(L_1) \subset \varphi^{-1}(L_2) \subset \cdots \subset \varphi^{-1}(L_h) \subset \cdots$ si stabilizza per h sufficientemente grande, e quindi lo stesso è vero per $L_1 \subset L_2 \subset \cdots \subset L_h \subset \cdots$. Ciò mostra che M/N è noetheriano.

Supponiamo viceversa che N e M/N siano noetheriani, e sia $N_1 \subset N_2 \subset \cdots \subset N_h \subset \cdots$ una successione di sottomoduli di M. Per la noetherianità di N la successione $N \cap N_1 \subset N \cap N_2 \subset \cdots \subset N \cap N_h \subset \cdots$ si stabilizza, e lo stesso vale per la successione $N_1/(N \cap N_1) \subset N_2/(N \cap N_2) \subset \cdots \subset N_h/(N \cap N_h) \subset \cdots$ di sottomoduli di M/N, data la noetherianità di quest'ultimo. Ma se $N \cap N_h = N \cap N_{h+1}$ e $N_h/(N \cap N_h) = N_{h+1}/(N \cap N_{h+1})$, allora $N_h = N_{h+1}$. Questo mostra che anche $N_1 \subset N_2 \subset \cdots \subset N_h \subset \cdots$ si stabilizza, e quindi che M è noetheriano.

Lemma 3. *Un A-modulo M è noetheriano se e solo se ogni suo sottomodulo è finitamente generato. Se A è noetheriano e M è finitamente generato, M è noetheriano.*

Sia N un sottomodulo di M. Se N non è finitamente generato si può trovare una successione $m_1, m_2, \dots$ di elementi di N tali che $Am_1 \neq Am_1 + Am_2 \neq Am_1 + Am_2 + Am_3 \neq \cdots$. Supponiamo viceversa che ogni sottomodulo di M sia finitamente generato. Se $N_1 \subset N_2 \subset \cdots \subset N_h \subset \cdots$, poniamo $N = \bigcup N_j$. Allora $N = Am_1 + Am_2 + \cdots + Am_n$, vi è un h tale che $m_1, m_2, \dots, m_n \in N_h$, quindi $N_h = N$, e quindi $N_h = N_{h+1} = \cdots$. Supponiamo ora A noetheriano e M finitamente

generato. Mostriamo che M è noetheriano per induzione sul minimo numero di generatori di M. Se questo è uno, una successione crescente di sottomoduli di M dà una successione crescente di ideali in A, che deve essere definitivamente costante, come quindi anche l'originaria successione di sottomoduli. Sia ora $m_1, m_2, \ldots, m_n$ un sistema minimale di generatori in M, e poniamo $N = Am_2 + \cdots + Am_n$. Per ipotesi induttiva N e M/N, che è generato dalla classe di m_1 modulo N, sono noetheriani. La noetherianità di M segue dal lemma 2.

Segue dal lemma 3 che ogni dominio a ideali principali è noetheriano e che ogni modulo finitamente generato su un tale dominio è noetheriano.

D'ora in poi supporremo sempre che A sia un dominio a ideali principali. Se M è un A-modulo poniamo

$$T(M) = \{m \in M \,|\, am = 0 \text{ per qualche } a \in A\}\,.$$

Si tratta di un sottomodulo di M, il cosidetto *sottomodulo di torsione* di M. Gli elementi non nulli di $T(M)$ si dicono *di torsione*. Il modulo M si dice *di torsione* se $T(M) = M$, *senza torsione* se $T(M) = \{0\}$. Notiamo che $M/T(M)$ è senza torsione, e che ogni A-modulo libero è senza torsione. L'*annullatore* di M è

$$\mathrm{Ann}(M) = \{a \in A \,|\, am = 0 \text{ per ogni } m \in M\}\,.$$

Si verifica senza difficoltà che $\mathrm{Ann}(M)$ è un ideale in A. Se M è finitamente generato, M è di torsione se e solo se $\mathrm{Ann}(M) \neq \{0\}$. Un A-modulo M si dice *ciclico* se è generato da un solo elemento. Se M è ciclico, è isomorfo ad $A/\mathrm{Ann}(M)$.

Proposizione 1. *Sia M un A-modulo finitamente generato senza torsione. Allora M è libero.*

Ragioniamo per induzione sul numero n di generatori di M. Quando $n = 1$, cioè quando $M = Am$ con $m \neq 0$, l'elemento m è una base di M perché non è di torsione. Supponiamo ora che $n > 1$ e che la proposizione sia dimostrata per moduli generati da non più di $n - 1$ elementi. Sia t_0 un elemento non nullo di M appartenente a un sistema di n generatori. Se M/At_0 contiene elementi di torsione, ci sono $t \in M$ e $a, b \in A$, con a non invertibile, tali che

$$at = bt_0\,.$$

Se a e b hanno un fattore f in comune, dato che M non ha torsione possiamo dividere entrambi i lati per f senza inficiare la validità dell'uguaglianza. Possiamo quindi supporre che a e b siano tra loro primi, e quindi che ci siano $c, d \in A$ tali che $ca + db = 1$. Ne segue che $t_0 = cat_0 + dbt_0 = cat_0 + dat = a(bt_0 + dt)$, cioè che $t_0 = a_1 t_1$, dove $t_1 = bt_0 + dt$ e $a_1 = a$. Se M/At_1 contiene elementi di torsione possiamo ripetere il procedimento con t_1 e così via, ottenendo relazioni

$$t_0 = a_1 t_1 \quad t_1 = a_2 t_2 \quad \cdots \quad t_{j-1} = a_j t_j$$

dove gli a_i sono elementi non invertibili di A. Questo significa che le inclusioni

$$At_0 \subset At_1 \subset \cdots \subset At_j$$

sono tutte strette. Dato che M è noetheriano il procedimento non può continuare all'infinito, e quindi si giunge in un numero finito di passi a un $t_j \neq 0$ tale che M/At_j non abbia torsione. Dato che M/At_j è generato da $n - 1$ elementi, è libero per ipotesi induttiva. Scegliamo elementi $m_2, \ldots, m_h$ di M le cui classi modulo t_j siano una base di M/At_j e poniamo $m_1 = t_j$. È chiaro che $m_1, \ldots, m_h$ generano M. Inoltre, se $c_1, \ldots, c_h$ sono elementi di A tali che $\sum c_i m_i = 0$, riducendo modulo m_1 se ne deduce che $c_2 = \cdots = c_h = 0$, e quindi anche che $c_1 = 0$ dato che $m_1 \neq 0$ e M non ha torsione. In conclusione, $m_1, \ldots, m_h$ è una base di M.

Corollario 1. *Sia M un A-modulo finitamente generato, e sia N un suo sottomodulo. Sia $\alpha : M \to M/N$ l'omomorfismo naturale. Se M/N non ha torsione, esiste un sottomodulo L di M tale che $M = N \oplus L$. Inoltre, se M' è un sottomodulo di M tale che $\alpha(M') = M/N$, si può scegliere L in modo che $L \subset M'$.*

La dimostrazione è immediata. Dato che M/N è senza torsione, è libero: siano $m_1, \dots, m_h$ elementi di M' tali che $\alpha(m_1), \dots, \alpha(m_h)$ sia una base di M/N. Si può scegliere come L il sottomodulo di M generato da $m_1, \dots, m_h$. Osserviamo che una conseguenza del corollario è che ogni A-modulo finitamente generato M è somma diretta di $T(M)$ e di un sottomodulo libero di M.

Studieremo ora la struttura degli A-moduli di torsione. Sia M un A-modulo finitamente generato di torsione, e sia a un elemento non nullo di $\mathrm{Ann}(M)$. Se b è primo con a si può scrivere $1 = \alpha a + \beta b$. Quindi la moltiplicazione per b è un automorfismo di M e ha come inversa la moltiplicazione per β. Scriviamo ora $a = \prod a_i$, dove gli a_i sono primi fra loro. Indichiamo con M_i il nucleo della moltiplicazione per a_i e poniamo $b_i = \displaystyle\prod_{j \neq i} a_j$.

Lemma 4. *$M_i = b_i M$ per ogni i. Inoltre $M = \bigoplus_i M_i$.*

Notiamo innanzitutto che $b_i M \subset M_i$ dato che $0 = aM = a_i b_i M$. Poiché a_i e b_i sono primi fra loro e $a_i \in \mathrm{Ann}(M_i)$, si ha che $b_i M \supset b_i M_i = M_i \supset b_i M$. Questo mostra che $M_i = b_i M$. Dato che i b_i non hanno fattori comuni vi sono elementi β_i di A tali che $1 = \sum \beta_i b_i$. Quindi

$$M = \sum b_i \beta_i M \subset \sum b_i M \,.$$

D'altra parte, se $\sum m_j = 0$, $m_j \in M_j$, si ha che, per ogni i,

$$0 = b_i \left(\sum m_j \right) = b_i m_i \,.$$

Poiché su M_i la moltiplicazione per b_i è iniettiva ciò implica che $m_i = 0$ per ogni i. La dimostrazione del lemma è completa.

Il lemma 4 riduce lo studio degli A-moduli finitamente generati di torsione a quello degli A-moduli finitamente generati il cui annullatore sia generato dalla potenza di un elemento primo di A.

Lemma 5. *Sia M un A-modulo finitamente generato tale che $\mathrm{Ann}(M) = Ap^h$, dove p è primo. Allora M è somma diretta di moduli ciclici della forma A/Ap^k. Di più, per ogni k, il numero degli addendi isomorfi a A/Ap^k che compaiono in questa decomposizione è univocamente determinato.*

Per dimostrare la prima affermazione del lemma ragioniamo per induzione sul numero dei generatori di M. Se questo numero è 1 non c'è niente da dimostrare. Supponiamo che M abbia un insieme di generatori consistente di n elementi. Uno tra questi generatori, che indichiamo con m_1, deve avere per annullatore Ap^h. Dunque $p^h m_1 = 0$ ma $p^{h-1} m_1 \neq 0$. Per ipotesi induttiva il quoziente M/Am_1 è somma diretta $A\overline{m}_2 \oplus \cdots \oplus A\overline{m}_n$ di $p-$moduli ciclici, dove $m_i \in M$ e $\overline{m}_i$ indica la classe di m_i modulo Am_1. Per ogni $i \geq 2$ sia Ap^{ℓ_i} l'annullatore di $\overline{m}_i$; in particolare $\ell_i \leq h$, $p^{\ell_i}\overline{m}_i = 0$ ma $p^{\ell_i - 1}\overline{m}_i \neq 0$. Dunque $p^{\ell_i} m_i \in Am_1$, cioè esistono $a \in A$ primo con p e un intero k tali che

$$p^{\ell_i} m_i = p^k a m_1 \,.$$

Dato che a è primo con p, l'annullatore di am_1 è lo stesso di m_1, cioè Ap^h. Dunque $p^{h-k-1+\ell_i}m_i = p^{h-1}am_1 \neq 0$. Ne segue che $\ell_i \leq k$ e quindi, ponendo $m_i' = m_i - p^{k-\ell_i}am_1$, che

$$p^{\ell_i}m_i' = p^{\ell_i}m_i - p^k am_1 = 0\,.$$

D'altra parte $\overline{m}_i = \overline{m}_i'$ per ogni i. Possiamo dunque supporre che $p^{\ell_i}m_i = 0$, cioè che i moduli ciclici Am_i e $A\overline{m}_i$ siano isomorfi per ogni $i \geq 2$. Ne segue che $L = \sum_{i\geq 2} Am_i$ è isomorfo a M/Am_1 ed è quindi, in particolare, una somma diretta. Ne segue anche che M è somma diretta di Am_1 e L e quindi, in definitiva, che M è somma diretta dei sottomoduli ciclici Am_i, $i = 1, \ldots, n$.

Passiamo alla seconda affermazione del lemma. Scriviamo $M = M_1 \oplus \cdots \oplus M_n$, dove $M_i \simeq A/Ap^{h_i}$, e per ogni i scegliamo un generatore m_i di M_i. Poniamo anche

$$N_k(M) = \{m \in M : p^k m = 0\}\,.$$

È evidente che $N_k(M_i)$ è il sottomodulo di M_i generato da $p^{h_i-k}m_i$ se $0 < k \leq h_i$ e coincide con M_i quando $k > h_i$. Ne segue, in particolare, che $N_k(M_i)/N_{k-1}(M_i)$ è uno spazio vettoriale di dimensione 1 sul campo $F = A/Ap$ se $0 < k \leq h_i$, ed è nullo se $k > h_i$. Dunque, per ogni $k \geq 1$, il quoziente

$$V_k(M) = N_k(M)/N_{k-1}(M) = \bigoplus_i \big(N_k(M_i)/N_{k-1}(M_i)\big)$$

è uno spazio vettoriale su F di dimensione pari al numero degli i tali che $k \leq h_i$. Ne segue che, per ogni k,

$$\#\{i : h_i = k\} = \dim_F V_k(M) - \dim_F V_{k+1}(M)\,,$$

e dunque che questo numero è intrinsecamente associato a M e non dipende dalla particolare decomposizione di M in somma di moduli ciclici. La dimostrazione del lemma 5 è completa.

Combinando i risultati finora dimostrati possiamo descrivere completamente la struttura dei moduli finitamente generati su A.

Teorema 1 (Struttura dei moduli finitamente generati su un dominio a ideali principali)**.** *Ogni modulo finitamente generato su un dominio a ideali principali A è somma diretta di un numero finito di moduli ciclici isomorfi ad A o a un quoziente A/Ap^h, dove p è un elemento primo di A. Il numero di addendi isomorfi ad A e il numero degli addendi isomorfi ad A/Ap^h, per ogni fissato h, sono univocamente determinati.*

Per giustificare questo risultato notiamo innanzitutto che segue dalla proposizione 1 e dal corollario 1 che M è somma diretta di $T(M)$ e di un modulo libero. Possiamo dunque supporre che M sia di torsione. Sia $d = p_1^{k_1} \ldots p_r^{k_r}$ un generatore dell'annullatore di M, dove $p_1, \ldots, p_r$ sono primi distinti, e sia M_i il nucleo della moltiplicazione per $p_i^{k_i}$. Il lemma 4 mostra che M è somma diretta degli M_i, e il lemma 5 che quest'ultimo è somma diretta di moduli ciclici della forma A/p_i^h. L'affermazione di unicità nell'enunciato del teorema 1 segue dall'analoga affermazione nell'enunciato del lemma 5.

Teorema 2 (Struttura dei moduli finitamente generati su un dominio a ideali principali: seconda versione)**.** *Ogni modulo finitamente generato su un dominio a ideali principali A è somma diretta di un numero finito di copie di A e di moduli ciclici $A/Ad_1, \ldots, A/Ad_m$, dove $d_1, \ldots, d_m$ sono elementi di A tali che $d_m | d_{m-1} | \ldots | d_1$. Gli elementi $d_1, \ldots, d_m$ sono univocamente determinati, a meno di moltiplicazione per elementi invertibili di A.*

Gli elementi $d_1, \dots, d_m$ vengono chiamati *divisori elementari* di M. Questa seconda versione del teorema di struttura segue dalla prima se si osserva che vale il seguente risultato.

Lemma 6. *Siano M e N moduli ciclici su A e ne siano Aa e Ab gli annullatori. Se a e b sono primi tra loro $M \oplus N$ è ciclico e il suo annullatore è Aab.*

La dimostrazione è del lemma è semplicissima. Siano m e n generatori di M e N e scriviamo $1 = \alpha a + \beta b$. Allora

$$\begin{aligned} m =& \alpha a m + \beta b m = \beta b(m+n)\,, \\ n =& \alpha a n + \beta b n = \alpha a(m+n)\,, \end{aligned}$$

e quindi $m+n$ genera $M \oplus N$. È chiaro che $ab(m+n) = 0$. D'altra parte, se c è un elemento di A tale che $c(m+n) = 0$, deve essere $cm = cn = 0$, e quindi a e b dividono c. Dato che a e b sono primi tra loro anche ab divide c.

Per applicare il lemma procediamo come segue. Possiamo limitarci a dimostrare il teorema nel caso in cui M sia di torsione. Siano $p_1, \dots, p_r$ i fattori primi distinti di un generatore dell'annullatore di M. Per ogni i indichiamo con $M_{i,1} \simeq A/Ap_i^{h_{i,1}}, M_{i,2} \simeq A/Ap_i^{h_{i,2}}, \dots, M_{i,m_i} \simeq A/Ap_i^{h_{i,m_i}}$ gli addendi, nella decomposizione data dal teorema 1, il cui annullatore è una potenza di p_i, ordinati in modo che $h_{i,1} \geq h_{i,2} \geq \cdots$. Poniamo poi $d_j = \prod_i p_i^{h_{i,j}}$, dove $h_{i,j} = 0$ se $j > m_i$, e indichiamo con m il massimo intero per cui $d_m \neq 1$. Poniamo anche $M_{i,j} = \{0\}$ se $j > m_i$. Allora ripetute applicazioni del lemma 6 mostrano che il modulo $N_j = \bigoplus_i M_{i,j}$ è ciclico e isomorfo a A/Ad_j. Inoltre $M = \bigoplus_j N_j$, e $d_m | d_{m-1} | \dots | d_1$. L'unicità dei d_j segue dalla parte unicità del teorema 1.

Osservando che l'annullatore di A è l'ideale $\{0\}$ e quello di A/Ad l'ideale Ad, si vede che il teorema 2 può essere rienunciato come segue.

Teorema 3 (Struttura dei moduli finitamente generati su un dominio a ideali principali: terza versione)**.** *Ogni modulo finitamente generato su un dominio a ideali principali A è somma diretta di un numero finito di moduli ciclici $M_1, \dots, M_h$ tali che* $\mathrm{Ann}(M_1) \supset \mathrm{Ann}(M_2) \supset \cdots \supset \mathrm{Ann}(M_h)$. *Gli ideali* $\mathrm{Ann}(M_i)$ *sono univocamente determinati.*

I teoremi di struttura per i moduli finitamente generati su anelli a ideali principali danno ovviamente, come caso particolare, un teorema di struttura per i gruppi abeliani (cioè per gli $\mathbb{Z}$-moduli) finitamente generati. Un esempio un po' meno ovvio di applicazione è il seguente.

Sia V uno spazio vettoriale di dimensione finita sul campo K, e sia φ un endomorfismo di V. Sia $A = K[T]$, dove T è una indeterminata: si tratta di un anello a ideali principali. Lo spazio vettoriale V diventa un A-modulo ponendo

$$Pv = P(\varphi)(v)\,.$$

Osserviamo che un sotto-A-modulo di V non è altro che un sottospazio vettoriale φ-invariante di V (cioè un sottospazio W tale che $\varphi(W) \subset W$). È chiaro che V, come A-modulo, è finitamente generato. Inoltre, se P è il polinomio caratteristico di φ, il teorema di Cayley-Hamilton dice che per ogni $v \in V$ si ha che $Pv = 0$. Dunque V è un A-modulo di torsione. Il teorema 1 (bastano in effetti 4 e 5) dice che V è somma diretta di sottospazi ciclici $V_1 = Av_1, \dots, V_h = Av_h$ tali che, per ogni i, l'annullatore di v_i è della forma $P_i^{r_i}$, dove P_i è un polinomio monico irriducibile e r_i è un intero positivo. Rispetto a una base di V costruita mettendo insieme basi per i sottospazi V_i, la matrice di φ è dunque una matrice diagonale a blocchi: i blocchi non sono altro che le matrici delle restrizioni di φ ai V_i.

Scegliamo ora per V_i una base particolare. Sia d_i il grado di P_i. I vettori $u_k = \varphi^{k-1}(v_i)$, per $0 < k \leq r_i d_i$, sono indipendenti, in quanto una relazione lineare tra di essi potrebbe essere riscritta sotto la forma $Qv_i = 0$, dove Q è un polinomio di grado al più $r_i d_i - 1$, in contraddizione con il fatto che l'annullatore di v_i è generato da $P_i^{r_i}$, che ha grado $r_i d_i$. I vettori in questione generano V_i; per vederlo basta mostrare che il sottospazio che essi generano è φ-invariante. Ora $\varphi(u_k) = \varphi^k(v_i)$, che è uguale a u_{k+1} se $k < r_i d_i$. Quando invece $k = r_i d_i$, la relazione $P_i^{r_i} v_i = 0$ permette di scrivere $\varphi^k(v_i)$ come combinazione lineare di $u_1, \dots, u_{r_i d_i}$. Più esattamente, se scriviamo

$$P_i^{r_i}(T) = T^{r_i d_i} + a_{r_i d_i} T^{r_i d_i - 1} + a_{r_i d_i - 1} T^{r_i d_i - 2} + \cdots + a_1 \,,$$

otteniamo

$$\varphi(u_{r_i d_i}) = \varphi^{r_i d_i}(v_i) = -\sum_{j=1}^{r_i d_i} a_j u_j \,.$$

Rispetto alla base $u_1, \dots, u_{r_i d_i}$, la matrice della restrizione di φ a V_i è dunque

$$\begin{pmatrix} 0 & 1 & 0 & 0 & & \\ 0 & 0 & 1 & 0 & \dots & \\ & & & & & \\ & & \dots & & & \\ & & & & & 1 \\ -a_1 & -a_2 & & \dots & & -a_{r_i d_i} \end{pmatrix} \tag{1}$$

Rispetto a una opportuna base di V la matrice di φ è dunque diagonale a blocchi, con blocchi della forma (1).

Trattiamo ora il caso in cui $K = \mathbb{C}$ o, più in generale, il caso in cui K sia algebricamente chiuso. I polinomi P_i sono allora di grado 1: scriviamo $P_i = T - \lambda_i$. Conviene scegliere una base $w_1, \dots, w_{r_i}$ per V_i diversa da quella scelta prima, ponendo

$$w_k = P_i^{k-1} v_i \,.$$

È chiaro che i w_k generano V_i. Inoltre essi sono indipendenti. Supponiamo infatti che $\sum c_k w_k = 0$, dove $c_k \in K$. Applicando $P_i^{r_i - 1}$ a questa uguaglianza si ottiene che $c_1 w_{r_i} = 0$, e quindi $c_1 = 0$. Applicando poi $P_i^{r_i - 2}$ si ricava che $c_2 w_{r_i} = 0$, e quindi $c_2 = 0$, e così via. Notiamo che

$$\begin{aligned} \varphi(w_k) &= w_{k+1} + \lambda_i w_k \qquad \text{se } k < r_i \,, \\ \varphi(w_{r_i}) &= \lambda_i w_{r_i} \,. \end{aligned}$$

In altre parole, la matrice della restrizione di φ a V_i, rispetto alla base $w_1, \dots, w_{r_i}$, è

$$\begin{pmatrix} \lambda_i & 1 & 0 & & \dots \\ 0 & \lambda_i & 1 & 0 & \\ & & & & \\ & & \dots & & \\ & & & & 1 \\ & \dots & 0 & 0 & \lambda_i \end{pmatrix} .$$

Una matrice di questo tipo si chiama *blocco di Jordan*. In conclusione, rispetto a una opportuna base di V la matrice di φ è una matrice diagonale a blocchi costituita da blocchi di Jordan. Una matrice siffatta si dice *in forma normale di Jordan*.

Proposizione 2. *Siano M un modulo finitamente generato senza torsione su A e $N \subset M$ un sottomodulo. Allora esistono una base $m_1, \dots, m_n$ di M, un intero $h \leq n$ e $d_1, \dots, d_h \in A$ tali che $d_1 \,|\, d_2 \,|\, \cdots \,|\, d_h$ e che $d_1 m_1, \dots, d_h m_h$ sia una base di N.*

Per ogni sottomodulo L di M poniamo

$$\overline{L} = \{m \in M \,|\, \text{esiste } a \in A,\ a \neq 0, \text{ tale che } am \in L\}\,.$$

È chiaro che $\overline{L}$ è un sottomodulo di M e che $M/\overline{L}$ non ha torsione. Il sottomodulo $\overline{L}$ viene a volte detto il *saturato* di L. Diremo "buona" una base di M come nell'enunciato. Si può supporre che M/N sia di torsione. Infatti se la proposizione è vera per l'inclusione di N in $\overline{N}$ e $m_1, \dots, m_h$ è una base "buona" di $\overline{N}$, si può trovare una base "buona" di M aggiungendole una base di un complementare di $\overline{N}$.

Supponiamo dunque che M/N sia di torsione e indichiamo con d un generatore del suo annullatore. Scegliamo un elemento μ di M tale che la sua classe modulo N, che indicheremo con $[\mu]$, abbia annullatore Ad. Ragionando come nella dimostrazione della proposizione 1 si mostra che esiste $m \in M$ tale che μ sia multiplo di m e che M/Am non abbia torsione. L'annullatore di $[m]$ è generato da un multiplo di d, e quindi deve essere generato da d. Supponiamo che hm appartenga a N, ciè che $h[m] = 0$. Allora $d \,|\, h$. Ne segue che $Am \cap N = Adm$. Notiamo che N/Adm non ha torsione; quindi, in base al corollario 1, esiste un sottomodulo L di N tale che $N = Adm \oplus L$. Dico che $M = Am \oplus \overline{L}$. Infatti se $m' \in M$, allora $dm' \in N$ e quindi $dm' = adm + \ell$, dove $a \in A$ e $\ell \in L$; ne segue che $d(m' - am) \in L$, cioè che $m' - am \in \overline{L}$. D'altra parte, se $am \in \overline{L}$, cioè se $ham \in L$ per qualche $h \neq 0$, allora in particolare $ham \in N$, quindi $ham \in Adm$, e dunque $ham = 0$. Visto che M non ha torsione se ne deduce che $am = 0$. Notiamo infine che $\overline{L} \cap N = L$.

Il fatto che esista una decomposizione in somma diretta $M = Am \oplus H$, dove si è posto $H = \overline{L}$, tale che $N = Adm \oplus L$, $L = H \cap N$ e $Am \cap N = Adm$, permette di procedere per induzione sul numero di generatori di M, o meglio sul numero di addendi ciclici in una decomposizione $M/N = A/Ad_1 \oplus \cdots \oplus A/Ad_k$ con $d_1 \,|\, d_2 \,|\, \cdots \,|\, d_k$.