Il teorema di struttura dei moduli finitamente generati su un PID

di Gabriel Antonio Videtta

5 settembre 2023

In questo documento dimostro[1] un enunciato fondamentale del celebre teorema di struttura dei moduli finitamente generati su un PID. Storicamente questo teorema nasce come una generalizzazione del teorema di struttura dei gruppi abeliani finitamente generati e diventa poi un potente strumento da cui derivano alcune celebri forme canoniche dell'algebra lineare, come la forma normale di Jordan o la forma canonica razionale.

Teorema (di struttura dei moduli finitamente generati su un PID)**.** Sia M un modulo finitamente generato su un PID R. Allora esistono unici (a meno di associati) d_1, ..., $d_k \in R$ tali per cui $d_1 \mid d_2 \mid \cdots \mid d_k$ e $M \cong R/(d_1) \times \cdots \times R/(d_k)$.

Si osserva sin da subito che il teorema può riscriversi in modo alternativo utilizzando il teorema cinese del resto. Infatti, se d_i viene scritto nella sua fattorizzazione in primi[2] $p_1^{k_1} \cdots p_{n_i}^{k_{n_i}}$, allora vale che:

$$R/(d_i) \cong R/\left(p_1^{k_1}\right) \times \cdots \times R/\left(p_{n_i}^{k_{n_i}}\right).$$

Pertanto il teorema di struttura può riscriversi come:

Teorema. Sia M un modulo finitamente generato su un PID R. Allora esistono unici (a meno di associati) p_1, ..., $p_n \in R$ primi e k_1, ..., $k_n \in \mathbb{N}$ tali per cui:

$$M \cong R/\left(p_1^{k_1}\right) \times \cdots \times R/\left(p_n^{k_n}\right).$$

Osservazione. D'ora in poi, mi riferisco ad M come un modulo finitamente generato su un PID R.

La forma del primo enunciato è detta **decomposizione in fattori invarianti**, mentre quella del secondo è detta **decomposizione primaria**.

[1] Il contenuto di questo documento è ispirato a quello del capitolo *The PID structure theorem* del *Napkin* di Evan Chen, reperibile su `https://github.com/vEnhance/napkin`.

[2] Un PID è sempre un UFD e dunque una tale fattorizzazione esiste sempre.

Definizione (fattori invarianti)**.** Si chiamano **fattori invarianti** i vari d_i che compaiono nella decomposizione in fattori invarianti di M.

Definizione (divisori elementari)**.** Si chiamano **divisori elementari** i vari $p_i^{k_i}$ che compaiono nella decomposizione primaria di M.

Definizione (rango di un modulo)**.** Si definisce rango di M il numero di volte in cui compare 0 tra i fattori invarianti.

Il documento prosegue con la dimostrazione dell'esistenza[3] dei fattori invarianti, secondo il seguente schema:

- Poiché M è finitamente generato, esiste un'applicazione lineare surgettiva ψ da R^m a M, dove m è il numero di generatori di M,
- Poiché R è noetheriano[4], anche R^m lo è; allora $\operatorname{Ker}\psi$ è finitamente generato da n elementi,
- Si può costruire allora un'altra applicazione lineare surgettiva ϕ da R^n a $\operatorname{Ker}\psi$,
- Immergendo naturalmente $\operatorname{Ker}\psi$ in M tramite la mappa naturale τ, si osserva che $\operatorname{Ker}\psi = \operatorname{Im}(\tau \circ \phi)$, dove $T = \tau \circ \phi$ è una mappa da R^n a R^m,
- Dal momento che T mappa un modulo libero[5] ad un altro, T può identificarsi con una matrice,
- Si scrive la matrice di T nella forma normale di Smith, dove compaiono i fattori invarianti d_1, ..., d_k; allora esistono $\underline{v_1}$, ..., $\underline{v_n}$ base di R^n tale per cui $R^n = \langle \underline{v_1} \rangle \oplus \cdots \oplus \langle \underline{v_n} \rangle$ e $\operatorname{Im} T = \langle d_1 \underline{v_1} \rangle \oplus \cdots \oplus \langle d_k \underline{v_k} \rangle \oplus \langle 0 \underline{v_{k+1}} \rangle \oplus \cdots \oplus \langle 0 \underline{v_n} \rangle$,
- Si costruisce un applicazione lineare ι da R^n a $R/(d_1) \times \cdots \times R/(d_k) \times R \times \cdots \times R$ tale per cui $\operatorname{Ker}\iota = \operatorname{Im} T$; allora, per il primo teorema di isomorfismo, vale che:

  $$M \cong R^n / \operatorname{Ker}\psi = R^n / \operatorname{Im} T \cong R/(d_1) \times \cdots \times R/(d_k) \times R \times \cdots \times R,$$

  concludendo la dimostrazione.

Questo schema è in parte riassunto dal seguente diagramma commutativo:

$$\begin{tikzcd}
 & \operatorname{Ker}\psi \arrow[dr, tail, "\tau"] & & \\
R^n \arrow[ur, "\phi"] \arrow[rr, "T"] & & R^m \arrow[r, two heads, "\psi"] & M
\end{tikzcd}$$

[3]La dimostrazione dell'unicità è omessa. Alcuni commenti e risultati al riguardo sono reperibili su `https://math.stackexchange.com/q/4193/769611`.

[4]Un modulo è noetheriano se ogni suo sottomodulo è finitamente generato.

[5]Un modulo è libero se ammette una base, proprio come R^n.

Dimostrazione

Dal momento che M è finitamente generato, esistono $\underline{w_1}$, ..., $\underline{w_m} \in M$ tali per cui $\langle \underline{w_1}, \ldots, \underline{w_m} \rangle = M$. Allora si costruisce l'applicazione lineare $\psi : R^m \to M$ univocamente determinata dalla relazione $\underline{e_i} \overset{\psi}{\mapsto} \underline{w_i}$. Si osserva che ψ è surgettiva: per ogni $\underline{w} \in M$, esistono α_1, ..., $\alpha_m \in R$ tali per cui $\underline{w} = \alpha_1 \underline{w_1} + \ldots + \alpha_m \underline{w_m}$; allora $(\alpha_1, \ldots, \alpha_m)^\top \overset{\psi}{\mapsto} \underline{w}$. Poiché ψ è surgettiva, $\operatorname{Im} \psi = M$, e quindi per il primo teorema di isomorfismo vale che:

$$M \cong R^m / \operatorname{Ker} \psi. \tag{1}$$

Dal momento che R è un PID, R è in particolare noetheriano (è infatti monogenerato). Allora anche R^m è noetheriano, come dimostra il seguente lemma[6]:

Lemma 1. Siano M ed N due R-moduli noetheriani. Allora $M \times N$ è anch'esso noetheriano.

Dimostrazione. Sia L un sottomodulo di $M \times N$. Si considerino i seguenti sottomoduli:

$$A = \{\underline{m} \in M \mid (\underline{m}, \underline{0}) \in L\} \subseteq M,$$

$$B = \{\underline{n} \in N \mid \exists\, \underline{m} \in M \mid (\underline{m}, \underline{n}) \in L\} \subseteq N.$$

Si osserva che A e B sono finitamente generati, essendo rispettivamente sottomoduli degli anelli noetheriani M ed N. Allora esistono $\underline{a_1}$, ..., $\underline{a_s} \in A$ e $\underline{b_1}$, ..., $\underline{b_t} \in B$ tali per cui $A = \langle \underline{a_1}, \ldots, \underline{a_s} \rangle$ e $B = \langle \underline{b_1}, \ldots, \underline{b_t} \rangle$.

Sia $\underline{\ell} \in L$. Allora esistono $\underline{m} \in M$, $\underline{n} \in N$ tali per cui $\underline{\ell} = (\underline{m}, \underline{n})$. Inoltre $\underline{n} \in B$, e dunque esistono β_1, ..., β_t tali per cui $\underline{n} = \beta_1 \underline{b_1} + \ldots + \beta_t \underline{b_t}$. Siano $\underline{x_1}$, ..., $\underline{x_s} \in M$ tali per cui $(\underline{x_i}), \underline{b_i}) \in L$ e si ponga $\underline{x} = \beta_1 \underline{x_1} + \ldots + \beta_t \underline{x_t}$. Si ottiene dunque che:

$$(\underline{m}, \underline{n}) = \underbrace{(\underline{m} - \underline{x}, \underline{0})}_{\in L} + \beta_1(\underline{x_1}, \underline{b_1}) + \ldots + \beta_t(\underline{x_t}, \underline{b_t}).$$

Allora $\underline{m'} := \underline{m} - \underline{x} \in A$, e dunque esistono α_1, ..., α_s tali per cui $\underline{m'} = \alpha_1 \underline{a_1} + \ldots + \alpha_s \underline{a_s}$. Pertanto vale che:

$$(\underline{m}, \underline{n}) = \sum_{i=1}^{s} \alpha_i (\underline{a_i}, \underline{0}) + \sum_{j=1}^{t} \beta_j (\underline{x_j}, \underline{b_j}),$$

da cui si conclude che L è finitamente generato, e dunque che $M \times N$ è noetheriano. $\square$

Poiché allora R^m è noetheriano, $\operatorname{Ker} \psi$ è finitamente generato, e dunque esistono $\underline{u_1}$, ..., $\underline{u_n} \in \operatorname{Ker} \psi$ tali per cui $\operatorname{Ker} \psi = \langle \underline{u_1}, \ldots, \underline{u_n} \rangle$. Allora, analogamente a prima, si può costruire un'applicazione lineare $\phi : R^n \to \operatorname{Ker} \psi$ tale per cui ϕ sia surgettiva, mappando $\underline{e_i}$ a $\underline{u_i}$.

[6] Si costruisce infatti R^m come il prodotto di R effettuato m volte.

Si considera adesso l'immersione naturale τ di $\operatorname{Ker}\psi$ in R^m, ossia l'applicazione lineare $\tau : \operatorname{Ker}\psi \to R^m$ tale per cui $\tau(\underline{u}) = \underline{u}$ per ogni $\underline{u} \in \operatorname{Ker}\psi$. Chiaramente τ è iniettiva e $\operatorname{Im}\tau = \operatorname{Ker}\psi$. Detta allora $T = \tau \circ \phi$, vale che $\operatorname{Im} T = \operatorname{Im}(\tau \circ \phi) = \operatorname{Im}\tau = \operatorname{Ker}\psi$, dove si è usata la surgettività della mappa ϕ. Sostituendo allora $\operatorname{Im}\tau$ nell'identità (1), si ottiene che:

$$M \cong R^m / \operatorname{Im} T. \tag{2}$$

Pertanto adesso è sufficiente studiare l'applicazione T per ricavare la tesi. Dal momento che T ha come dominio il modulo libero R^n e come codominio R^m, T si può rappresentare come una matrice S a elementi in R dove S^j è la valutazione in $\underline{e_j}$ di T. Adesso il punto cruciale della dimostrazione dipende dalla seguente proposizione:

Proposizione (forma normale di Smith)**.** Sia $S = (s_{ij})$ una matrice $m \times n$ a elementi in R. Allora esistono unici (a meno di associati) d_1, ..., $d_k \in R$ con $d_1 \mid d_2 \mid \cdots \mid d_k$ e $k = \min\{m, n\}$ tali per cui esistano due basi $\mathcal{B}$, $\mathcal{B}'$ di R^n e R^m che soddisfano l'identità[7]:

$$S' := M^{\mathcal{B}}_{\mathcal{B}'}(f_S) = \begin{pmatrix} d_1 & 0 & 0 & 0 & \dots & 0 \\ 0 & d_2 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & d_k & \dots & 0 \end{pmatrix},$$

dove con f_S si intende l'applicazione lineare indotta dalla matrice S.

Dimostrazione dell'esistenza. Le uniche operazioni consentite sulla matrice che consentono di individuare una nuova coppia di basi opportune sono le stesse[8] contemplate dall'algoritmo di eliminazione di Gauss eccetto per quella di moltiplicazione di una riga (o di una colonna) per un elemento non invertibile di R. Pertanto, si presenta la dimostrazione dell'esistenza della forma normale di Smith come un algoritmo che permette di alterare la matrice tramite le uniche operazioni consentite.

Se $S = 0$, la tesi è già dimostrata. Altrimenti, si possono utilizzare le operazioni consentite per far sì che si verifichi $s_{11} \neq 0$. Si distinguono ora tre casi:

(i) s_{11} non divide almeno un elemento di S^1,

(ii) s_{11} non divide almeno un elemento di S_1,

(iii) s_{11} divide tutti gli elementi di S^1 e S_1.

[7]La matrice S' mostra in realtà il caso in cui $m > n$. Tuttavia la struttura di S' si può generalizzare facilmente per $m \leq n$.

[8]Si verifica facilmente che ogni tale operazione modifica una delle due basi tramite le operazioni elementari di riordinamento e di somma per un multiplo.

Se s_{11} non divide almeno un elemento di S^1, detto s_{i1}, si possono effettuare operazioni di riga per spostare s_{i1} in s_{21}. Poiché R è un PID, l'ideale (s_{11}, s_{21}) è monogenerato, e dunque esistono α, $\beta \in R$ tali per cui $(s_{11}, s_{21}) = (\alpha s_{11} + \beta s_{21})$. Vale inoltre che $(\alpha, \beta) = R$[9], e dunque che esistono γ, $\delta \in R$ tali per cui $\gamma\alpha + \delta\beta = 1$. Si può allora moltiplicare la matrice a sinistra per la matrice invertibile[10]:

$$\begin{pmatrix} \alpha & \beta \\ -\delta & \gamma \end{pmatrix},$$

opportunamente inserita al posto del blocco $(I_m)_{1,2}^{1,2}$ in I_m. Si effettua un analogo ragionamento per il caso (ii), moltiplicando a destra per la stessa matrice, opportunamente trasposta. Si continua a effettuare questo tipo di moltiplicazioni fino a quando non si ricade nel caso (iii). Il caso (iii) è sempre raggiungibile, dal momento che ad ogni operazione si sostituisce s_{11} con un suo divisore, creando una successione ascendente di ideali $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$ che, per la noetherianità di R, deve stabilizzarsi.

Giunti nel caso (iii), si annullano i primi elementi di tutte le colonne di S eccetto per S^1, sottraendo un opportuno multiplo di S^1. Si effettua poi la stessa cosa per le righe eccetto che per S_1. Se $m = 1$ o $n = 1$, l'algoritmo termina. Altrimenti si ottiene una matrice della forma:

$$\begin{pmatrix} s_{11} & 0 \\ 0 & \tilde{S} \end{pmatrix}.$$

Se s_{11} divide ora ogni elemento di $\tilde{S}$, si riapplica l'algoritmo soltanto su $\tilde{S}$ (ogni operazione su $\tilde{S}$ può essere estesa a un'operazione su S che lascia l'elemento s_{11} invariato. Se invece esiste un elemento s_{ij} non diviso da s_{11}, si somma la riga S_i alla riga S_1 (o la colonna S^j alla colonna S^1) e si riapplica l'algoritmo. Per le stesse motivazioni di prima, ad un passo dell'algoritmo s_{11} dovrà dividere ogni elemento di $\tilde{S}$.

Dopo aver impiegato con successo l'algoritmo, si otterrà una matrice nella forma normale di Smith, dimostrando la tesi. $\square$

Pertanto esistono due basi $\mathcal{B}$ e $\mathcal{B}' = \{\underline{v_1}, \ldots, \underline{v_n}\}$ di R^m e R^n tali per cui $M_{\mathcal{B}'}^{\mathcal{B}}(f_S)$ assume la forma normale di Smith. In particolare, vale che:

$$\operatorname{Im} T = \langle d_1\underline{v_1}\rangle \oplus \cdots \oplus \langle d_k\underline{v_k}\rangle \oplus \langle 0\underline{v_{k+1}}\rangle \oplus \cdots \oplus \langle 0\underline{v_n}\rangle.$$

Sia allora $\iota : R^n \to R/(d_1) \times \cdots \times R/(d_k) \times R \times \cdots \times R$ l'applicazione lineare determinata dalla relazione:

$$a_1\underline{v_1} + \ldots + a_n\underline{v_n} \overset{\iota}{\mapsto} ([a_1]_{d_1}, \ldots, [a_k]_{d_k}, a_{k+1}, \ldots, a_n).$$

Chiaramente ι è surgettiva. Sia adesso $\underline{v} = a_1\underline{v_1} + \ldots + a_n\underline{v_n}$ tale per cui $\iota(\underline{v}) = \underline{0}$. Allora d_1 deve dividere a_1, d_2 deve dividere a_2, e così fino ad a_k. Infine $a_{k+1} = \cdots = a_n = 0$.

[9] Infatti, se $d = \alpha s_{11} + \beta s_{21}$, vale che $\frac{s_{11}}{d}\alpha + \frac{s_{21}}{d}\beta = 1$.

[10] Tale matrice è invertibile poiché unimodulare. Alternativamente, si può fornire esplicitamente l'inverso $\left(\begin{smallmatrix} \gamma & -\beta \\ \delta & \alpha \end{smallmatrix}\right)$.

Pertanto $\underline{v}$ dovrà necessariamente appartenere a $\operatorname{Im} T$; viceversa ogni elemento di $\operatorname{Im} T$ appartiene a $\operatorname{Ker} \iota$, da cui $\operatorname{Ker} \iota = \operatorname{Im} T$. Allora, per il primo teorema di isomorfismo, vale che:

$$R^n / \operatorname{Im} T \cong R^n / \operatorname{Ker} \iota \cong R/(d_1) \times \cdots \times R/(d_k) \times R \times \cdots \times R. \tag{3}$$

Combinando allora le identità (2) e (3), si ottiene la tesi[11]:

$$M \cong R/(d_1) \times \cdots \times R/(d_k) \times R \times \cdots \times R.$$

■

[11]Si tiene presente dell'isomorfismo $R/(0) \cong R$.