Teoremi di struttura dei moduli finitamente generati su un dominio euclideo

Appunti al corso di Algebra
Anno accademico 2003-2004

1 Prodotti diretti.

Siano M e N due moduli sullo stesso anello A, non necessariamente sottomoduli di uno stesso modulo. Allora possiamo considerare il prodotto cartesiano $M \times N$ di M con N, che e' l'insieme delle coppie ordinate (x, y) al variare di x in M e di y in N. In tale insieme si definisce una somma componente per componente ponendo

$$(x, y) + (z, t) = (x + z, y + t).$$

Con tale somma $M \times N$ e' un gruppo abeliano: ad esempio l'elemento neutro e' la coppia $(0, 0)$, mentre l'opposto di (x, y) e' la coppia $(-x, -y)$. Possiamo dare a tale gruppo abeliano $M \times N$ la struttura di modulo su A definendo una operazione esterna

$$A \times (M \times N) \to M \times N$$

cosi':

$$(a, (x, y)) \to (ax, ay).$$

Si vede subito che con tale operazioni $M \times N$ e' un A-modulo che si chiama il **prodotto diretto** di M con N. Se $M = N = A$ invece che scrivere $A \times A$ scriveremo A^2.

Piu' in generale, se M_1, M_2, ..., M_n e' un insieme finito di A-moduli, possiamo definire il prodotto diretto $M_1 \times M_2 \times \cdots \times M_n$. Questo e' il prodotto cartesiano con una operazione di somma componente per componente

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

e un prodotto esterno cosí definito:

$$a(x_1, x_2, \ldots, x_n) = (ax_1, ax_2, \ldots, ax_n).$$

Se $M_1 = \cdots = M_n = A$, scriveremo A^n invece che $A \times A \times \cdots \times A$.

2 Somme dirette.

Siano invece N e P due sottomoduli di uno stesso A-modulo M. Allora ricordiamo che la somma di N e P e' l'insieme dei vettori di M della forma $x+y$, al variare di x in N e di y in P. Questo e' un sottomodulo di M che si indica con $N+P$. Nel caso in cui $M = N+P$, diremo che M e' la somma di N e di P.

Proposizione 2.1. *Nelle ipotesi precedenti, sono fatti equivalenti:*

1) $P \cap N = \{0\}$

2) Ogni elemento di $N+P$ *si scrive in modo unico come somma di un elemento di* N *e di uno di* P*.*

Definizione 2.2. *Se* N *e* P *verificano una delle precedenti ipotesi equivalenti, diciamo che la somma* $N+P$ *e'* **diretta** *e scriviamo* $N \oplus P$ *invece che* $N+P$*.*

Ad esempio il gruppo abeliano $2\mathbf{Z}$ dei numeri pari é la somma dei due sottogruppi $4\mathbf{Z}$ e $6\mathbf{Z}$; infatti per ogni intero n si ha:

$$2n = (-n)4 + (n)6.$$

Ma il vettore 10 si puó scrivere in tanti modi diversi come somma di un elemento di $4\mathbf{Z}$ e di uno di $6\mathbf{Z}$:

$$10 = (1)4 + (1)6 = (4)4 + (-1)6 = (-5)4 + (5)6.$$

Naturalmente $2\mathbf{Z}$ non é somma diretta di $4\mathbf{Z}$ e $6\mathbf{Z}$, e infatti si ha $12 \in 4\mathbf{Z} \cap 6\mathbf{Z}$.

Analogamente se $M_1, \ldots, M_n$ sono sottomoduli di un A-modulo M, l'insieme dei vettori di M che si possono scrivere nella forma $x_1 + x_2 + \cdots + x_n$ con $x_i \in M_i$, e' un sottomodulo di M che si indica con $\sum_{i=1}^n M_i$. Se $M = \sum_{i=1}^n M_i$, diciamo che M e' la somma dei suoi sottomoduli $M_1, \ldots, M_n$.

Osserviamo che se M_i e' un modulo ciclico per ogni i, ossia $M_i =< m_i >$, allora $M = \sum_{i=1}^n M_i$ se e solo se ogni vettore di M e' combinazione lineare dei vettori $m_1, \ldots, m_n$ ossia se e solo se i vettori $m_1, \ldots, m_n$ sono un **sistema di generatori** per M.

Come per il caso di due sottomoduli, ogni vettore di $\sum_{i=1}^n M_i$ si scrive come somma $x_1 + x_2 + \cdots + x_n$ con $x_i \in M_i$, ma tale scrittura non é necessariamente unica.

Proposizione 2.3. *Sono fatti equivalenti:*

1) $M_i \cap \sum_{j \neq i} M_j = \{0\}$ *per ogni* $i = 1, \ldots, n$*.*

2) Ogni elemento v *di* $\sum_{i=1}^n M_i$ *si scrive in modo unico nella forma*

$$v = x_1 + x_2 + \cdots + x_n$$

con $x_i \in M_i$*.*

Definizione 2.4. *Se i sottomoduli $M_1, \ldots, M_n$ verificano una delle condizioni equivalenti nella precedente proposizione, diciamo che la somma $\sum_{i=1}^n M_i$ e'* **diretta** *e scriviamo $\oplus_{i=1}^n M_i$ invece che $\sum_{i=1}^n M_i$.*

Ad esempio se M e' l'$\mathbf{R}$-modulo $\mathbf{R}^3$, allora M e' somma di due qualunque piani distinti che passano per l'origine, ma non e' la loro somma diretta. Mentre M e' la somma diretta di una retta e un piano che non contenga la retta.

Nel caso in cui $M_1, \ldots, M_n$ sono sottomoduli di uno stesso A-modulo M, possiamo dunque parlare della loro somma e del loro prodotto diretto. I due concetti sono legati dal fatto che

Proposizione 2.5. *Abbiamo un omomorfismo canonico surgettivo:*

$$\varphi : M_1 \times M_2 \times \cdots \times M_n \to \sum_{i=1}^n M_i$$

che e' definito ponendo

$$\varphi(x_1, x_2, \ldots, x_n) = x_1 + x_2 + \cdots + x_n.$$

Si ha che φ e' iniettivo se e solo se $M_i \cap \sum_{j \neq i} M_j = \{0\}$ per ogni $i = 1, \ldots, n$, ossia se e solo se $\sum M_i = \oplus M_i$.

Ci servirá il seguente facile risultato.

Proposizione 2.6. *Se $f : M \to N$ e $g : P \to Q$ sono omomorfismi di A-moduli, allora posto*

$$f \times g : M \times P \to N \times Q$$

l'omomorfismo definito da

$$(f \times g)(x, y) = (f(x), g(y),$$

risulta

$$Im(f \times g) = Im(f) \times Im(g), \qquad Ker(f \times g) = Ker(f) \times Ker(g).$$

Relativamente ai moduli finitamente generati, si prova facilmente che se M e' finitamente generato e N un suo sottomodulo, anche M/N e' finitamente generato. Si ha anche

Proposizione 2.7. *Ogni addendo diretto di un modulo finitamente generato e' finitamente generato.*

Proof. Sia $M = P \oplus Q$. Allora $M/Q \simeq P$, e quindi P e' finitamente geenrato. □

Facciamo un esempio di un ideale di un anello commutativo con identitá che non e' finitamente generato.

Sia A l'anello delle funzioni $f : \mathbb{R} \to \mathbb{R}$ con le operazioni di somma e di prodotto *pointwise*. E' chiaro che A e' un anello commutativo con identitá. Se I e' l'insieme delle funzioni $f \in A$ tali che esiste un intero $n \geq 1$ con $f(a) = 0$ se $|a| > n$, allora e' immediato verificare che I e' un ideale non finitamente generato.

3 Moduli di torsione e senza torsione

Se N e' un sottomodulo del modulo M su A, definiamo **l'annullatore** di N l'insieme

$$0 :_A N = \{a \in A \mid am = 0 \ \forall \ m \in N.\}$$

Se $m \in M$, definiamo

$$0 :_A m = \{a \in A \mid am = 0.\}$$

E' chiaro che $0 :_A m = 0 :_A < m >$ e m si dice di torsione se $0 :_A m \neq (0)$.

L'insieme degli elementi di torsione si indica con $T(M)$. Se A e' integro, allora $T(M)$ e' un sottomodulo di M. Diciamo che M e' **di torsione** se $T(M) = M$, ossia se tutti gli elementi di M sono di torsione.

All'altro estremo diciamo che M e' **senza torsione** se $T(M) = \{0\}$. E chiaro che se A e' integro, allora $M/T(M)$ e' senza torsione.

Ad esempio A^n e' senza torsione e lo stesso per gli spazi vettoriali.

Sia ora M un A-modulo ed I un ideale di A. Supponiamo che $I \subseteq 0 :_A M$; allora M 'e canonicamente un modulo su A/I mediante la moltiplicazione

$$A/I \times M \to M$$

definita da $\overline{a}m = am$. Infatti se $\overline{a} = \overline{b}$, allora $a - b \in I$ e quindi per ogni $m \in M$, si ha $(a - b)m = 0$ e quindi $am = bm$.

Infine notiamo che non possiamo in alcun modo dare senso alla moltiplicazione di due sottomoduli. Ma se I e' un ideale di A, allora definiamo

$$IM := \left\{ \sum a_i m_i, a_i \in I, m_i \in M \right\}.$$

Questo e' un sottomodulo di M tale che $I \subseteq 0 :_A (M/IM)$; se ne deduce che il modulo M/IM e' canonicamente un A/I-modulo. Applicheremo tale osservazione nel caso in cui $I = \mathfrak{m}$ e' un ideale massimale di A. Allora avremo su $M/\mathfrak{m}M$ una struttura di spazio vettoriale su $A/\mathfrak{m}$.

4 Moduli liberi

Se m é un vettore dell'A-modulo M, si ha una applicazione lineare canonica $\varphi : A \to M$ definita da $\varphi(a) = am$. Il nucleo di φ é l'annullatore di m. Il primo teorema di isomorfismo ci assicura che

Proposizione 4.1. *Per ogni $m \in M$ si ha un isomorfismo*

$$A/0 : m \simeq < m > .$$

É chiaro che φ é iniettivo se e solo se $0 : m = (0)$. Ció equivale a dire che m é un vettore linearmente indipendente, in accordo con la terminologia degli spazi vettoriali. Quindi $0 : m = 0$ se e solo se $A \simeq < m >$.

Piú in generale, dati i vettori $m_1, \ldots, m_s \in M$, possiamo considerare la applicazione lineare

$$\varphi : A^s \to M$$

definita ponendo

$$\varphi(a_1, \ldots, a_s) = a_1 m_1 + a_2 m_2 + \cdots + a_s m_s.$$

É chiaro che i vettori $m_1, \ldots, m_s$ sono **linearmente indipendenti** se e solo se φ é iniettivo, mentre φ é surgettivo se e solo se i vettori $m_1, \ldots, m_s$ generano M.

Definizione 4.2. *Diciamo che i vettori $m_1, \ldots, m_s$ sono una* **base** *di M, se φ é un isomorfismo, ossia se tali vettori sono un sistema di generatori per M e sono linearmente indipendenti.*

Definizione 4.3. *I moduli che ammettono una base sono detti* **moduli liberi**.

Esempio 4.4. *Il modulo A^s é un modulo libero per ogni $s \geq 1$.*

Infatti i vettori $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_s = (0, 0, \ldots, 0, 1)$ sono una base di A^s che chiameremo **base canonica** di A^s.

Dalle considerazioni precedenti, si ha subito che

Proposizione 4.5. *Sono fatti equivalenti:*

1) M é libero.

2) M é isomorfo ad A^s per qualche $s \geq 0$.

Nella definizione di modulo libero che abbiamo introdotto si vuole che il modulo sia finitamente generato. Si puó parlare di moduli liberi anche nel caso di moduli non finitamente generati, ma tale nozione non e' necessaria per il corso.

Una diversa condizione per avere una base é data dalla seguente proposizione.

Proposizione 4.6. *I vettori $m_1, \ldots, m_s$ sono una* **base** *di M se e solo se*

$$M = \oplus_{i=1}^{s} < m_i >$$

e inoltre $0 : m_i = (0)$ per ogni $i = 1, \ldots, s$.

Notiamo che la condizione $M = \oplus_{i=1}^{s} < m_i >$ non é sufficiente ad assicurare che i vettori $m_1, \ldots, m_s$ siano una base di M. Ad esempio $\mathbf{Z}/6\mathbf{Z} =< \overline{2} > \oplus < \overline{3} >$, ma $0 : \overline{2} = (3)$ e infatti $\mathbf{Z}/6\mathbf{Z}$ non é libero.

Ne segue che

Corollario 4.7. *M é un modulo libero se e solo M é somma diretta di moduli ciclici*

$$M = \oplus_{i=1}^{s} < m_i >$$

con

$$0 : m_i = (0)$$

per ogni $i = 1, \ldots, s$.

Se L é libero con base $v_1, \ldots, v_n$, ogni vettore $v \in L$ si scrive in modo unico come combinazione lineare $\sum_{i=1}^{n} a_i v_i$ di $v_1, \ldots, v_n$. Ossia se $\sum_{i=1}^{n} a_i v_i = \sum_{i=1}^{n} b_i v_i$ allora $a_i = b_i$ per ogni i. Questo implica che

Proposizione 4.8. *Ogni omomorfismo $\varphi : L \to M$ é univocamente determinato dai vettori $\varphi(v_1), \ldots, \varphi(v_n)$.*

Ció significa che

Corollario 4.9. *Dati i vettori $w_1, \ldots, w_n$ in M, esiste ed é unico un omomorfismo*

$$\varphi : L \to M$$

tale che $\varphi(v_i) = w_i$ per ogni $i = 1, \ldots, n$.

Notare che se i vettori $v_1, \ldots, v_n$ generano L ma non sono una base di L, un tale omomorfismo non é detto che esista. Ad esempio se $L = \mathbf{Z}^2$ e $M = \mathbf{Z}$, i vettori $v_1 = (1, 1), v_2 = (1, 5), v_3 = (1, 3)$ generano L ma non sono una base di L. Se fissiamo in M i vettori $w_1 = 3$, $w_2 = 2$, $w_3 = -1$, allora non esiste nessun omomorfismo $\varphi : L \to M$ tale che $\varphi(v_i) = w_i$ per ogni $i = 1, \ldots, 3$. Infatti se tale φ esistesse, si avrebbe la contraddizione

$$-2 = 2\varphi(v_3) = \varphi(2v_3) = \varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2) = 5.$$

Osserviamo che esistono moduli liberi e moduli non liberi. Ad esempio $\mathbf{Z}/(n)$ e' un modulo su $\mathbf{Z}$ (ossia un gruppo abeliano) che non é libero. Infatti ogni vettore $\overline{p}$ é tale che

$$n\overline{p} = \overline{np} = \overline{0}$$

e quindi non puó far parte di un insieme di vettori linearmente indipendenti.

É chiaro invece che ogni modulo finitamente generato su un corpo k, ossia ogni spazio vettoriale finitamente generato, é un k- modulo libero.

Sappiamo che se si considera l'anello A come modulo su se stesso, i suoi sotto-moduli sono tutti e soli gli ideali di A. Allora é facile dimostrare che

Lemma 4.10. *Un ideale I di A é un A-modulo libero se e solo se $I = (a)$, con a non zero-divisore in A.*

Proof. Basta semplicemente osservare che due elementi a e b di un anello A non sono mai linearmente indipendenti. Infatti c'é sempre la relazione $ab - ba = 0$. □

Si potrebbe pensare che la teoria dei moduli liberi e quella degli spazi vettoriali siano parallele. Le seguenti osservazioni mostrano che cosí non é. Ad esempio

Osservazione 4.11. *In un modulo libero non é sempre vero che da un sistema di generatori si possa estrarre una base.*

Ad esempio nel gruppo abeliano $G = 2\mathbf{Z}$ dei numeri pari, i vettori 4 e 6 sono un sistema di generatori per G, ma né 4 né 6 formano una base.

Osservazione 4.12. *In un modulo libero non sempre un sistema di vettori linearamente indipendenti si puó estendere ad una base.*

Ad esempio in $\mathbf{Z}$ il vettore 7 é linearmente indipendente ma non é una base e non puó far parte di una base perché abbiamo visto che, se $n \geq 2$, n vettori di un anello A, pensato come modulo su se stesso, non sono mai lineramente indipendenti.

Peró siamo capaci di dimostrare che tutte le basi di uno stesso modulo libero sono equipotenti. Mostriamo due dimostrazioni di tale risultato, la prima necessita di una interessante applicazione del Lemma di Zorn.

Proposizione 4.13. *Ogni anello commutativo A con identitá possiede un ideale massimale.*

Proof. Consideriamo la famiglia $\mathcal{F}$ degli ideali propri di A ordinata parzialmente per inclusione. $\mathcal{F}$ e' non vuota perche' contiene l'ideale nullo; proviamo che ogni catena in $\mathcal{F}$ ha un maggiorante. Se infatti $\mathcal{C} : \{I_\alpha\}_{\alpha \in \mathcal{A}}$ e' un sottoinsieme di $\mathcal{F}$ totalmente ordinato, allora la unione degli ideali di $\mathcal{F}$ e' ancora un elemento di $\mathcal{F}$ perche' e' un ideale ed e' proprio. Il Lemma di Zorn ci assicura che $\mathcal{F}$ possiede un elemento massimale e questo prova la nostra tesi. □

Proposizione 4.14. *Sia M e' un A-modulo libero, $m_1, \cdots, m_s$ una sua base e $\mathfrak{m}$ un ideale massimale di A. Allora $\overline{m_1}, \cdots, \overline{m_s}$ sono una base dello spazio vettoriale $M/\mathfrak{m}M$ sul corpo $A/\mathfrak{m}$.*

Proof. Se $m \in M$, possiamo scrivere $m = \sum a_i m_i$ e quindi

$$\overline{m} = \overline{\sum a_i m_i} = \sum \widetilde{a_i} \overline{m_i}.$$

Ció prova che $\overline{m_1}, \cdots, \overline{m_s}$ generano lo spazio vettoriale $M/\mathfrak{m}M$ sul corpo $A/\mathfrak{m}$. Proviamo che sono vettori indipendenti. Se si ha $\sum \widetilde{a_i} \overline{m_i} = 0$, allora $\sum a_i m_i \in \mathfrak{m}M$ e quindi

$$\sum a_i m_i = \sum b_i m_i$$

con $b_i \in \mathfrak{m}$. Ne segue $\sum (a_i - b_i) m_i = 0$, da cui $a_i = b_i \in \mathfrak{m}$. La conclusione segue. □

Teorema 4.15. *Tutte le basi di un modulo libero sono equipotenti.*

Possiamo dimostrare questo risultato anche usando la teoria delle matrici su un anello commutativo con identitá.

5 Matrici ad elementi in un anello

Nell'insieme $M(A)$ delle matrici ad entrate in A possiamo definire la somma di due matrici dello stesso tipo $m \times n$ al solito modo, ossia elemento per elemento. In formule

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}).$$

La somma é commutativa ed associativa. Possiamo anche definire il prodotto righe per colonne di due matrici X e Y, purché X sia di tipo $m \times n$ e Y di tipo $n \times q$. Il prodotto non é commutativo. Possiamo infine definire il prodotto di uno scalare a per una matrice $X \in M(A)$ ponendo

$$a(x_{ij}) = (ax_{ij}).$$

É chiaro che se $a, b \in A$, si ha

$$a(bX) = (ab)X = b(aX)$$

e se $a \in A$, ed X e Y sono matrici dello stesso tipo, allora

$$a(XY) = (aX)Y = X(aY).$$

Infine, data la matrice X di tipo $n \times m$, la sua trasposta é quella matrice di tipo $m \times n$ che si ottiene da X sostituendo le righe con le colonne. La trasposta di X si indicherá con ${}^tX$.

É chiaro che data una matrice quadrata $X = (x_{ij}) \in M(A)$ di tipo $n \times n$, possiamo definire il suo determinante in questo modo:

$$det(X) = \sum_{\sigma} (\pm) x_{1\ \sigma(1)} x_{2\ \sigma(2)} \dots x_{n\ \sigma(n)}$$

ove σ varia nell'insieme delle permutazioni di $\{1, 2, \dots, n\}$.

Dalla definizione segue che $det(X)$ é un elemento di A ed é facile provare che le solite proprietá dei determinanti restano valide. In particolare si puó dimostrare il Teorema di Binet che afferma

Teorema 5.1. *Il determinante del prodotto di due matrici quadrate é uguale al prodotto dei determinanti.*

Al solito modo possiamo definire per una matrice quadrata X di tipo $n \times n$ la sua aggiunta X^*. Si ha la formula

$$X\ X^* = X^*\ X = det(X) I_n$$

ove I_n é la matrice identica $n \times n$.

Definizione 5.2. *Diciamo che la matrice quadrata $X \in M(A)$ é invertibile se esiste una matrice quadrata $Y \in M(A)$ tale che $XY = YX = I_n$.*

Si puó facilmente dimostrare che se

Proposizione 5.3. *Se X é invertibile allora la sua inversa é unica.*

Si ottiene cosí

Teorema 5.4. *Se $X \in M(A)$ é una matrice quadrata, allora X é invertibile se e solo se $det(X)$ é un elemento invertibile dell'anello A.*

Proof. Si ha infatti che se $XY = I_n$ allora $det(X)det(Y) = det(I_n) = 1$ e quindi $det(X)$ é invertibile. Se invece $a = det(X)$ é invertibile in A, allora la matrice $a^{-1}X^*$ é la inversa di X: infatti si ha

$$(a^{-1}X^*)X = a^{-1}(aI) = I = X(a^{-1}X^*).$$

□

Ad esempio la matrice $\begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$ ha determinante diverso da zero ma non é un elemento invertibile in $M(\mathbb{Z})$.

6 Basi diverse di un modulo libero

Supponiamo ora di avere un sistema di generatori $v_1, v_2, \ldots, v_s$ di un A-modulo M. Se $w_1, \ldots, w_t$ sono vettori di M, allora possiamo scrivere per ogni $i = 1, \ldots, t$

$$w_i = \sum_{j=1}^{s} x_{ji} v_j.$$

Se si introduce la matrice $X := (x_{ij})$ che é di tipo $t \times s$, possiamo chiaramente compendiare questa scrittura con la notazione

$$(w_1, \ldots, w_t) = (v_1, v_2, \ldots, v_s)X.$$

Osservazione 6.1. *Fare attenzione che abbiamo moltiplicato una matrice di vettori con una matrice di scalari: non si potrá peró moltiplicare una matrice di vettori con una altra di vettori.*

Ad esempio la notazione

$$(w_1, w_2, w_3) = (v_1, v_2) \begin{pmatrix} 2 & -3 & 5 \\ 4 & 7 & -5 \end{pmatrix}$$

significa

$$w_1 = 2v_1 + 4v_2,\ w_2 = -3v_1 + 7v_2,\ w_3 = 5v_1 - 5v_2.$$

Teorema 6.2. *Sia L un modulo libero, $e_1, \ldots, e_s$ una base di L e $v_1, \ldots, v_t \in L$; possiamo scrivere*

$$(v_1, \ldots, v_t) = (e_1, \ldots, e_s)X$$

ove X é una matrice quadrata $s \times t$.

Allora sono equivalenti:

1) $v_1, \ldots, v_t \in L$ generano L
2) X e' invertibile a destra.
3) $t \geq s$.

Proof. É chiaro che $v_1, \ldots, v_t \in L$ generano L se e solo se

$$(e_1, \ldots, e_s) = (v_1, \ldots, v_t)Y$$

per qualche matrice Y di tipo $t \times s$. Quindi se vale 1), si ha

$$(e_1, \ldots, e_s) = (v_1, \ldots, v_t)Y = (e_1, \ldots, e_s)XY.$$

La indipendenza di $e_1, \ldots, e_s$ prova che deve essere $XY = I_s$ e quindi X e' invertibile a destra.

Viceversa, se X e' invertibile a destra, ossia $XY = I_s$ si ha

$$(e_1, \ldots, e_s) = (e_1, \ldots, e_s)I_s = (e_1, \ldots, e_s)XY = (v_1, \ldots, v_t)Y$$

e quindi $v_1, \ldots, v_t$ generano L.

Suponiamo ora che $XY = I_s$ e, per assurdo, $t < s$. Consideriamo la matrice X' ottenuta da X completandola con degli 0 ad una matrice quadrata $s \times s$ e la matrice Y' ottenuta da Y completandola con degli 0 ad una matrice quadrata $t \times t$. É chiaro che si ha

$$X'Y' = XY = I_s.$$

Ció implica che $det(X')$ é invertibile, ma questo é assurdo perché X' ha almeno una colonna di 0. □

Corollario 6.3. *Due basi di un modulo libero L sono equipotenti.*

Proof. Siano $e_1, \ldots, e_s$ e $a_1, \ldots, a_t$ basi di L. Applicando il teorema precedente alle due basi a ruoli invertiti, si ha $t \geq s$, e $s \geq t$. □

La cardinalitá di una base di un modulo libero L non dipende dunque dalla base scelta e quindi é un invariante di L. Lo chiameremo il **rango** di L e lo indicheremo con $rg(L)$. Ad esempio $rg(A^s) = s$.

Come conseguenza del teorema precedente si ha:

Corollario 6.4. *Se si ha un isomorfismo $\phi : A^s \to A^t$, allora $t = s$.*

Corollario 6.5. *Se si ha un epimorfismo $\phi : A^s \to A^t$, allora $t \geq s$.*

Osserviamo che se L é un modulo libero di rango s, é possibile che L possieda un sottomodulo libero H di rango s che non coincide con L.

Ad esempio $\mathbb{Z}$ é libero di rango 1 e il sottomodulo H dei numeri pari non coincide con $\mathbb{Z}$ ed é libero di rango 1.

Un altro importante risultato é il seguente.

Teorema 6.6. *Sia L un modulo libero e siano $e_1, \dots, e_s$ una base di L. Siano poi $v_1, \dots, v_t$ elementi di L; possiamo scrivere $(v_1, \dots, v_t) = (e_1, e_2, \dots, e_s)X$ ove X é una matrice in $M_{s,t}(A)$. Allora*

X é invertibile a sinistra $\Longrightarrow$ $v_1, \dots, v_t$ sono linearmente indipendenti.

Proof. Supponiamo di avere $\sum_{i=1}^{t} a_i v_i = 0$. Allora possiamo scrivere in forma matriciale

$$0 = (v_1, \dots, v_t) \begin{pmatrix} a_1 \\ \vdots \\ a_t \end{pmatrix} = (e_1, \dots, e_s) X \begin{pmatrix} a_1 \\ \vdots \\ a_t \end{pmatrix}.$$

Poiché $e_1, \dots, e_s$ sono linearmente indipendenti, ció implica

$$X \begin{pmatrix} a_1 \\ \vdots \\ a_t \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Ma esiste $Y \in M_{t,s}(A)$ tale che $YX = I_t$ e quindi si ottiene

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = YX \begin{pmatrix} a_1 \\ \vdots \\ a_t \end{pmatrix} = I_t \begin{pmatrix} a_1 \\ \vdots \\ a_t \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_t \end{pmatrix}.$$

Dunque $a_1 = a_2 = \cdots = a_t = 0$, come volevasi. □

É chiaro che la implicazione "$v_1, \dots, v_t$ sono linearmente indipendenti $\Longrightarrow$ A é invertibile a sinistra" non vale. Sia $v = (2, 0) \in \mathbb{Z}^2$, ed e_1, e_2 la base canonica di $\mathbb{Z}^2$. Allora

$$v = 2e_1 = (e_1, e_2) \begin{pmatrix} 2 \\ 0 \end{pmatrix}.$$

Ora v é linearmente indipendente, ma la matrice $\begin{pmatrix} 2 \\ 0 \end{pmatrix}$ non ha inversa a sinistra: se infatti $(n, m) \begin{pmatrix} 2 \\ 0 \end{pmatrix} = 1$, si avrebbe $2n = 1$, impossibile in $\mathbb{Z}$.

Possiamo ora dimostrare il seguente teorema che illustra come ottenere tutte le basi di un modulo libero, a partire dalla conoscenza di una base fissata.

Teorema 6.7. *Sia $e_1, \ldots, e_s$ una base di L e $(v_1, \ldots, v_s) = (e_1, \ldots, e_s)X$ ove X é una matrice in $M_s(\mathbb{Z})$.*

Allora sono equivalenti:

1) X é invertibile.
2) $v_1, \ldots, v_s$ é base di L.
3) $v_1, \ldots, v_s$ generano L.

Proof. Se X e' invertibile, allora e' invertibile a destra e a sinistra e quindi $v_1, \ldots, v_s$ sono linearmente indipendenti e sistema di generatori per L. Ció prova che 1) implica 2). Resta solo da provare che 3) implica 1). Ció segue dal fatto che se una matrice quadrata X é invertibile a destra, $XY = I_s$, allora $det(X) = \pm 1$ e quindi X é invertibile. □

Se in particolare $L = A^n$, si consideri la base canonica $e_1, \ldots, e_n$ di L ed elementi $v_1, \ldots, v_n \in L$. Allora é chiaro che $(v_1, \ldots, v_n) = (e_1, \ldots, e_n)X$ ove X é la matrice che ha come colonne le coordinate di $v_1, \ldots, v_n$. Quindi $v_1, \ldots, v_n$ sono una base di A^n se e solo se la matrice delle loro coordinate ha determinante invertibile in A.

Ad esempio $v_1 = (2, 1), v_2 = (3, 1)$ sono una base di $\mathbb{Z}^2$ perché

$$det \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix} = -1.$$

Terminiamo questo paragrafo con alcune considerazioni su questo problema: É vero che in un A^n non ci possono essere $n + 1$ vettori linearmente indipendenti? In altre parole e' vero che non puó esserci un omomorfismo iniettivo $f : A^{n+1} \to A^n$?

Proveremo che la risposta e' affermativa per i moduli su un dominio euclideo. In realtá il risultato vale in generale per un anello commutativo, ma la prova e ' difficile. Una maniera di risolvere il problema e' quella di usare il Teorema di McCoy (vedi Kaplanski). Non si puó tentare una prova attraverso lo studio dello spazio vettoriale $M/\mathfrak{m}M$ perché il prodotto tensore non e' esatto a sinistra. Vediamo di provare il risultato nel caso $n = 2$.

Dobbiamo provare che tre vettori di A^2 non possono essere indipendenti. Siano $v_1 = (a, b), v_2 = (c, d), v_3 = (f, g)$. Si ha

$$(v_1, v_2, v_3) = (e_1, e_2)X$$

dove

$$X = \begin{pmatrix} a & c & f \\ b & d & g \end{pmatrix}.$$

Se $\rho(X) = 2$, allora, indicando con d_1, d_2, d_3 i minori 2×2 a segni alterni di X, si ha

$$(v_1, v_2, v_3) \begin{pmatrix} d_1 \\ d_2 \\ d_3 \end{pmatrix} = (e_1, e_2)X \begin{pmatrix} d_1 \\ d_2 \\ d_3 \end{pmatrix} = (0, 0, 0).$$

Se invece $\rho(X) = 1$, e, ad esempio $a \neq 0$, allora si ha

$$(v_1, v_2, v_3) \begin{pmatrix} c \\ -a \\ 0 \end{pmatrix} = (e_1, e_2) \begin{pmatrix} a & c & f \\ b & d & g \end{pmatrix} \begin{pmatrix} c \\ -a \\ 0 \end{pmatrix} = (e_1, e_2) \begin{pmatrix} 0 \\ bc - da \end{pmatrix} = 0.$$

7 Sottomoduli e quozienti di un modulo libero

I sottomoduli di $\mathbf{Z}$ pensato come modulo su se stesso, sono gli ideali di $\mathbf{Z}$. Poiché tali ideali sono principali e generati da un non-zero-divisore, sono tutti liberi di rango 1.

Ma se consideriamo il modulo $\mathbf{Z}[X]$ come modulo su se stesso, allora il sottomodulo generato da 2 e da X é un ideale non principale. Ne segue che non puó essere libero.

Proveremo che questa patologia non avviene per i moduli liberi su un dominio euclideo.

Iniziamo a provare che ogni sottomodulo di un modulo libero su un dominio euclideo e' finitamente generato. Basterá naturalmente provarlo per A^n.

Teorema 7.1. *Se A e' un dominio euclideo, i sottomoduli di $\mathbb{A}^n$ sono finitamente generati.*

Proof. Se $n = 1$, i sottomoduli di A sono ideali principali e quindi finitamente generati. Dimostriamo il teorema per induzione su n. Sia $n \geq 2$ e consideriamo la proiezione

$$\pi : A^n \to A^{n-1}$$

definita da $\pi(a_1, \ldots, a_n) = (a_1, \ldots, a_{n-1})$.

E' chiaro che π e' surgettiva e che $Ker(\pi) = \{(0, \ldots, 0, a_n)\} \simeq A$. Se consideriamo la restrizione ad H di π, sia $f : H \to A^{n-1}$, allora $Im(f)$ e' finitamente generato per l'ipotesi induttiva e $Ker(f) = Ker(\pi) \cap H$ e' un sottogruppo di A e quindi finitamente generato. Se $Im(f) =< w_1, \ldots, w_r >$ e $Ker(f) =< v_1, \ldots, v_s >$, si ha facilmente $H =< v_1, \ldots, v_s, z_1, \ldots, z_r >$ ove $w_i = f(z_i)$. □

Per provare che i sottomoduli di A^n sono liberi, lo strumento essenziale e' il teorema di diagonalizzazione delle matrici ad entrate in un dominio euclideo.

Ci serve qualche richiamo sulle **matrici elementari**.

Ci sono tre tipi di matrici elementari:

1. Matrice $E_{ij}(a)$, con $i \neq j$ interi positivi e $a \in A$. Questa é la matrice che ha tutti 1 sulla diagonale principale e tutti 0 altrove, escluso l'elemento di posto (i, j) che é a. In altre parole e' la matrice che si ottiene dalla matrice identica I_n aggiungendo alla riga i-ma la riga j-ma moltiplicata per a.

2. Matrice E_{ij} con $i \neq j$ interi positivi. Questa é la matrice che ha tutti 0 fuori della diagonale principale escluso le posizioni (i, j) e (j, i) ove ha 1, e sulla diagonale principale ha tutti 1 escluso le posizioni (i, i) e (j, j) dove ha 0. In altre parole e' la matrice che si ottiene dalla matrice I_n scambiando la riga i-ma con la riga j-ma.

3. Matrice $E_i(u)$ ove u é un elemento invertibile in A e i é un intero positivo. Questa é la matrice che é eguale alla matrice identica, solo che nella posizione (i, i) ha u.

Ad esempio le matrici elementari 2×2 sono

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix}$$

al variare di $a \in A$ e di u tra gli elementi invertibili di A.

Sia X una matrice $n \times m$, Y una matrice $m \times n$ e supponiamo che $E_{ij}(a)$, E_{ij}, $E_i(u)$ siano matrici $n \times n$. Allora

Lemma 7.2. *Con le notazioni precedenti, si ha:*

1. $E_{ij}(a)X$ é la matrice che si ottiene da X aggiungendo alla riga i la riga j moltiplicata per a, mentre $YE_{ij}(a)$ é la matrice che si ottiene da Y aggiungendo alla colonna j la colonna i moltiplicata per a.

2. $E_{ij}X$ é la matrice che si ottiene da X scambiando la riga i con la riga j, mentre YE_{ij} é quella che si ottiene facendo la stessa operazione sulle colonne di Y.

3. $E_i(u)X$ é la matrice che si ottiene da X sostituendo la riga i con la riga i moltiplicata per u, mentre $YE_i(u)$ é quella che si ottiene da Y operando allo stesso modo sulle colonne di Y.

Lemma 7.3. *Tutte le matrici elementari sono invertibili, e infatti la inversa di $E_{ij}(a)$ é la matrice $E_{ij}(-a)$, E_{ij} é l'inversa di se stessa e infine $E_i(u^{-1})$ é l'inversa di $E_i(u)$.*

Ricordiamo che una matrice, non necessariamente quadrata, si dice **diagonale** se tutte le entrate sono nulle, eccetto che sulla diagonale principale.

Teorema 7.4. *Sia A una matrice $s \times t$ ad entrate in un dominio euclideo A. Allora esistono matrici U e V prodotto di matrici elementari, tali che $UAV = \Delta$ ove Δ e' una matrice diagonale.*

Proof. Per la dimostrazione di questo risultato vedere il libro di Artin a pagina 541. □

Vediamo su esempi concreti come procedere con operazioni elementari per trasformare una matrice data in una matrice diagonale.

$$A = \begin{pmatrix} 3 & 4 \\ 2 & -5 \end{pmatrix} \overset{E_{1,2}(-1)}{\longrightarrow} \begin{pmatrix} 1 & 9 \\ 2 & -5 \end{pmatrix} \overset{E_{2,1}(-2)}{\longrightarrow} \begin{pmatrix} 1 & 9 \\ 0 & -23 \end{pmatrix} \underset{E_{1,2}(-9)}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & -23 \end{pmatrix} \underset{E_2}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & 23 \end{pmatrix}$$

$$A = \begin{pmatrix} 6 & 2 \\ 3 & 8 \end{pmatrix} \underset{E_{1,2}}{\longrightarrow} \begin{pmatrix} 2 & 6 \\ 8 & 3 \end{pmatrix} \overset{E_{2,1}(-4)}{\longrightarrow} \begin{pmatrix} 2 & 6 \\ 0 & -21 \end{pmatrix} \underset{E_{1,2}(-3)}{\longrightarrow} \begin{pmatrix} 2 & 0 \\ 0 & -21 \end{pmatrix} \underset{E_2}{\longrightarrow} \begin{pmatrix} 2 & 0 \\ 0 & 21 \end{pmatrix}$$

Ma anche

$$A = \begin{pmatrix} 6 & 2 \\ 3 & 8 \end{pmatrix} \overset{E_{1,2}(-2)}{\longrightarrow} \begin{pmatrix} 0 & -14 \\ 3 & 8 \end{pmatrix} \overset{E_{1,2}(1)}{\longrightarrow} \begin{pmatrix} 3 & -6 \\ 3 & 8 \end{pmatrix} \overset{E_{2,1}(-1)}{\longrightarrow} \begin{pmatrix} 3 & -6 \\ 0 & 14 \end{pmatrix} \underset{E_{1,2}(2)}{\longrightarrow} \begin{pmatrix} 3 & 0 \\ 0 & 14 \end{pmatrix}$$

e si trova una matrice diagonale diversa!

$$A = \begin{pmatrix} 21 & 14 \\ 3 & 2 \\ 6 & 4 \end{pmatrix} \overset{E_{3,2}(-2)}{\longrightarrow} \begin{pmatrix} 21 & 14 \\ 3 & 2 \\ 0 & 0 \end{pmatrix} \overset{E_{1,2}(-7)}{\longrightarrow} \begin{pmatrix} 0 & 0 \\ 3 & 2 \\ 0 & 0 \end{pmatrix} \overset{E_{1,2}}{\longrightarrow} \begin{pmatrix} 3 & 2 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 3 & 2 \\ 1 & -4 \\ 5 & 1 \end{pmatrix} \overset{E_{1,2}}{\longrightarrow} \begin{pmatrix} 1 & -4 \\ 3 & 2 \\ 5 & 1 \end{pmatrix} \overset{E_{2,1}(-3)}{\longrightarrow} \begin{pmatrix} 1 & -4 \\ 0 & 14 \\ 5 & 1 \end{pmatrix} \overset{E_{3,1}(-5)}{\longrightarrow} \begin{pmatrix} 1 & -4 \\ 0 & 14 \\ 0 & 21 \end{pmatrix} \underset{E_{1,2}(4)}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & 14 \\ 0 & 21 \end{pmatrix}$$

$$\overset{E_{3,2}(-1)}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & 14 \\ 0 & 7 \end{pmatrix} \overset{E_{2,3}(-2)}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 7 \end{pmatrix} \overset{E_{2,3}}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & 7 \\ 0 & 0 \end{pmatrix}$$

Facciamo un esempio con una matrice ad elementi in $k[X]$.

$$\begin{pmatrix} (X-1)(X-2) & X-2 \\ (X-1)^3 & (X-1)(X-2) \end{pmatrix} \overset{E_{2,1}(-(X-1))}{\longrightarrow} \begin{pmatrix} (X-1)(X-2) & X-2 \\ (X-1)^2 & 0 \end{pmatrix}$$

$$\overset{E_{1,2}(-1)}{\longrightarrow} \begin{pmatrix} -X+1 & X-2 \\ (X-1)^2 & 0 \end{pmatrix} \underset{E_{1,2}(1)}{\longrightarrow} \begin{pmatrix} -1 & X-2 \\ (X-1)^2 & 0 \end{pmatrix}$$

$$\underset{E_{1,2}(X-2)}{\longrightarrow} \begin{pmatrix} -1 & 0 \\ (X-1)^2 & (X-2)(X-1)^2 \end{pmatrix} \overset{E_{2,1}((X-1)^2)}{\longrightarrow} \begin{pmatrix} -1 & 0 \\ 0 & (X-2)(X-1)^2 \end{pmatrix}$$

Possiamo ora dimostrare che ogni sottomodulo di un modulo libero L su un dominio euclideo A, e' libero di rango minore o eguale al rango di L. In realtá il seguente teorema precisa come costruire una base del sottomodulo, usando il teorema di diagonalizzazione delle matrici ad entrate in un dominio euclideo.

Teorema 7.5. ***(Il teorema delle due basi)*** *Se L é un modulo libero di rango s su un dominio euclideo A e F é un suo sottomodulo, é possibile determinare una base $v_1, \ldots, v_s$ di L e scalari $d_1, \ldots, d_t \in A$, tali che $d_1 v_1, \ldots, d_t v_t$ sono una base di F.*

Proof. Abbiamo giá visto che F e' finitamente generato. Supponiamo di conoscere una base $e_1, \ldots, e_s$ di L e un sistema di generatori $g_1, \ldots, g_t$ di F. Potremo scrivere

$$(g_1, \ldots, g_t) = (e_1, \ldots, e_s)X$$

dove X é una matrice $s \times t$. Per il teorema precedente possiamo determinare matrici invertibili U e V tali che $UXV = \Delta$ con Δ matrice diagonale. Possiamo supporre che $d_1, \cdots, d_t$ siano gli elementi non nulli sulla diagonale principale di Δ. Allora $t \leq s$ e si ha

$$(g_1, \ldots, g_t)V = (e_1, \ldots, e_s)XV = (e_1, \ldots, e_s)U^{-1}\Delta.$$

Siccome U^{-1} é invertibile, i vettori $(v_1, \ldots, v_s) := (e_1, \ldots, e_s)U^{-1}$ sono un base di L. Avendosi

$$(g_1, \ldots, g_t)V = (v_1, \ldots, v_s)\Delta,$$

i vettori $d_1v_1, \cdots, d_tv_t$ stanno in F, ed essendo V invertibile, generano F. Resta da provare che sono vettori linearmente indipendenti. Ma se fosse $\sum a_i d_i v_i = 0$, sarebbe $\sum(a_i d_i)v_i = 0$ e quindi $a_i d_i = 0$ per ogni i. Poiché A e' integro e $d_i \neq 0$, ció implica $a_i = 0$ per ogni i. □

Notiamo che, nel precedente teorema, la nuova base di L é determinata dalla matrice U^{-1}. Quindi, nel procedere, **dobbiamo solo ricordarci delle operazioni sulle righe che sono state compiute nel processo di diagonalizzazione**. Infatti le operazioni sulle righe corrispondono alla moltiplicazione a sinistra per matrici elementari e quindi sono quelle che determinano U.

Nel teorema precedente abbiamo visto come ogni sottomodulo di un modulo libero sia anche lui libero e come si possa determinare una sua base speciale. L'esistenza di tale base speciale permette di dimostrare che ogni quoziente di un modulo libero su un dominio euclideo e' la somma diretta di sottomoduli ciclici.

Teorema 7.6. *Sia L un modulo libero ed $e_1, \ldots, e_s$ una sua base. Se $t \leq s$ e $d_1, \ldots, d_t$ sono elementi di A, consideriamo il modulo N generato da $d_1e_1, \ldots, d_te_t$. Allora L/N é somma diretta di moduli ciclici:*

$$L/N = < \overline{e}_1 > \oplus < \overline{e}_2 > \oplus \cdots \oplus < \overline{e}_s > .$$

Inoltre si ha

$$0 : \overline{e}_i = \begin{cases} (d_i) & \text{se } i \leq t \\ (0) & \text{se } i \geq t+1. \end{cases}$$

Quindi

$$L/N \simeq A/(d_1) \times A/(d_2) \times \cdots \times A/(d_t) \times A^{s-t}.$$

Proof. Siccome $\overline{e}_1, \ldots, \overline{e}_s$ generano L/N, é chiaro che $L/N = \sum_{i=1}^{s} < \overline{e}_i >$. Per provare che la somma é diretta, sia $a\overline{e}_i \in \sum_{j \neq i} < \overline{e}_j >$. Allora $a\overline{e}_i = \sum_{j \neq i} a_j \overline{e}_j$ e quindi $ae_i - \sum_{j \neq i} a_j e_j \in N$. Questo implica

$$ae_i - \sum_{j \neq i} a_j e_j = \sum_{i=1}^{t} b_r d_r e_r.$$

Quindi $a = 0$ se $i > t$, $a = b_i d_i$ se $i \leq t$. In ogni caso $a\overline{e}_i = \overline{0}$ e quindi la somma $\sum_{i=1}^{s} < \overline{e}_i >$ é diretta.

Infine $a\overline{e}_i = \overline{0}$ se e solo se $ae_i = \sum_{j=1}^{t} b_j d_j e_j$; se $i \leq t$, ció avviene se e solo se $a = b_i d_i$ ossia $a \in (d_i)$, mentre, se $i > t$, ció avviene se e solo se $a = 0$.

L'isomorfismo $L/N \simeq A/(d_1) \times A/(d_2) \times \cdots \times A/(d_t) \times A^{s-t}$ segue poi dal fatto che $< \overline{e}_i > \simeq A/0 : \overline{e}_i$. □

Notiamo che qualche d_i nel teorema precedente puó essere invertibile in A. Naturalmente se d_i e' invertibile, allora $\overline{e}_i = 0$ e non porta contributo nella decomposizione di L/N. Invece chiaramente nessun d_i e' 0.

8 Il teorema di struttura per i moduli finitamente generati su un dominio euclideo

Possiamo ora dimostrare il teorema di struttura per i moduli finitamente generati su un dominio euclideo.

Teorema 8.1. *Sia M un modulo finitamente generato su un dominio euclideo A. Allora M e' la somma diretta di sottomoduli ciclici.*

Proof. Sia infatti $m_1, \ldots, m_s$ un sistema di generatori di M. Allora si ha un epimorfismo canonico

$$\varphi : A^s \to M$$

definito per ogni $i = 1, \ldots, s$ da $\varphi(e_i) = m_i$.

Un tale epimorfismo si dirá **una presentazione** di M.

Per il primo teorema di omomorfismo si ha

$$A^s/Ker(\varphi) \simeq M$$

ove l'isomorfismo é quello che manda $\overline{v}$ in $\varphi(v)$. Per il teorema delle due basi (7.5), esiste una base $v_1, \ldots, v_s$ di A^s e scalari $d_1, \ldots, d_t \in A$, tali che $d_1 v_1, \ldots, d_t v_t$ é base di $Ker(\varphi)$.

Per il teorema 7.6 abbiamo:

$$A^s/Ker(\varphi) = \oplus_{i=1}^{s} < \overline{v_i} >$$

con

$$0 : \overline{v_i} = \begin{cases} (d_i) & i \leq t \\ (0) & i \geq t+1. \end{cases}$$

Ne segue

$$M = < \varphi(v_1) > \oplus < \varphi(v_2) > \oplus \cdots \oplus < \varphi(v_s) >$$

ove

$$0 : \varphi(v_i) = \begin{cases} (d_i) & i \leq r \\ (0) & i \geq r+1 \end{cases}$$

Ció implica anche

$$M \simeq A/(d_1) \times A/(d_2) \times \cdots \times A/(d_t) \times A^{s-t}.$$

□

Notiamo che, nel teorema precedente, qualche d_i puó essere invertibile in A. In tal caso il corrispondente modulo ciclico $< \varphi(v_i) >$ e' nullo e quindi non contribuisce alla decomposizione di M.

Facciamo un esempio. Consideriamo il modulo libero $\mathbf{Z}^2 = L$ e sia F il sottomodulo di L generato da $(3, 2)$ e $(4, -5)$. É facile osservare che questi vettori sono lineramente indipendenti e quindi costituiscono una base di F. Vogliamo decomporre il modulo L/F come somma diretta di moduli ciclici.

É chiaro che una presentazione del nostro modulo é data dalla proiezione canonica sul quoziente

$$\varphi : L \to L/F$$

il cui nucleo é F stesso. Se e_1, e_2 é la base canonica di L, si ha

$$((3, 2), (4, -5)) = ((e_1, e_2)) \begin{pmatrix} 3 & 4 \\ 2 & -5 \end{pmatrix}.$$

Diagonalizziamo la matrice:

$$\begin{pmatrix} 3 & 4 \\ 2 & -5 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 9 \\ 2 & -5 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 9 \\ 0 & -23 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -23 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 23 \end{pmatrix}$$

Le operazioni eseguite sono nell'ordine:

I riga - II riga: corrispondente alla moltiplicazione a sinistra per $E_{1,2}(-1)$.

II riga - 2(I riga): corrispondente alla moltiplicazione a sinistra per $E_{2,1}(-2)$.

II colonna - 9(I colonna): corrispondente alla moltiplicazione a destra per $E_{1,2}(-9)$.

(-1) (II colonna): corrispondente alla moltiplicazione a destra per $E_2(-1)$.

Quindi si ha

$$E_{2,1}(-2).E_{1,2}(-1) \begin{pmatrix} 3 & 4 \\ 2 & -5 \end{pmatrix} E_{1,2}(-9)E_2(-1) = \begin{pmatrix} 1 & 0 \\ 0 & 23. \end{pmatrix}$$

Ne segue

$$U^{-1} = E_{1-2}^{-1} E_{2-2(1)}^{-1} = E_{1+2} E_{2+2(1)} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$$

Dunque si ha $d_1 = 1$, $d_2 = 23$, e se scegliamo come nuova base di L i vettori

$$(v_1, v_2) = (e_1, e_2)U^{-1} = ((3, 2), (1, 1))$$

la base cercata di F é $\{d_1 v_1, d_2 v_2\} = \{v_1, 23v_2\} = \{(3, 2), (23, 23)\}$. Si ha dunque

$$L/F =< \overline{v_1} > \oplus < \overline{v_2} >=< \overline{v_2} >=< \overline{(1, 1)} >\simeq \mathbf{Z}/(\mathbf{23}).$$

Facciamo un altro esempio. Sia L il sottomodulo di $\mathbf{Z}^2$ generato dai vettori $(5, 12), (3, 10), (2, 14)$. Vogliamo determinare una base di L, che é sicuramente libero in quanto abbiamo visto che ogni sottomodulo di un modulo libero su un dominio euclideo é libero.

Si ha una presentazione

$$\varphi : \mathbf{Z}^3 \to L$$

definita da

$$\varphi(e_1) = (5, 12), \varphi(e_2) = (3, 10), \varphi(e_3) = (2, 14).$$

Cerchiamo una base di $Ker(\varphi)$. Dobbiamo risolvere il sistema

$$\begin{cases} 5a + 3b + 2c & = 0 \\ 12a + 10b + 14c & = 0. \end{cases}$$

Si vede facilmente che una base di $Ker(\varphi)$ é il vettore $(-11, 23, -7)$ e quindi $t = 1$. Si completa subito questo vettore ad una matrice invertibile

$$\begin{pmatrix} -11 & -1 & 0 \\ 23 & 2 & 0 \\ -7 & 0 & 1 \end{pmatrix}$$

Quindi se si pone

$$(v_1, v_2, v_3) := (e_1, e_2, e_3) \begin{pmatrix} -11 & -1 & 0 \\ 23 & 2 & 0 \\ -7 & 0 & 1 \end{pmatrix}$$

i vettori $v_1 = (-11, 23, -7), v_2 = (-1, 2, 0), v_3 = (0, 0, -1)$ sono una base di $\mathbf{Z}^3$ tale che v_1 é base di $Ker(\varphi)$. Notiamo che in questo caso non c'é stato bisogno di diagonalizzare per trovare la base opportuna di $\mathbf{Z}^3$.

Dunque $d_1 = 1$ e si ha

$$L =< \varphi(v_1) > \oplus < \varphi(v_2) > \oplus < \varphi(v_3) >=< (1, 8) > \oplus < (2, 14) > .$$

Poiché $0 : (1, 8) = 0 : (2, 14) = (0)$, questi vettori sono una base di L. Notare che L é un sottomodulo proprio di $\mathbf{Z}^2$.

Facciamo un esempio con $A = \mathbb{Q}[X]$. Sia $M = A^2$ e

$$F =< (X^2 - 3X + 2, (X - 1)^3), (X - 2, X^2 - 3X + 2) > .$$

Abbiamo giá visto come si diagonalizzi la matrice

$$\begin{pmatrix} (X-1)(X-2) & X-2 \\ (X-1)^3 & (X-1)(X-2) \end{pmatrix}$$

Si ottiene la matrice diagonale

$$\begin{pmatrix} -1 & 0 \\ 0 & (X-2)(X-1)^2 \end{pmatrix}$$

e quindi si ha

$$A^2/F \simeq \mathbb{Q}[X]/((X-2)(X-1)^2) \times \mathbb{Q}[X]/(1) \simeq \mathbb{Q}[X]/((X-2)(X-1)^2).$$

Dunque il modulo quoziente A^2/F e' ciclico.

Il Teorema 8.1 fornisce la decomposizione di un modulo M finitamente generato su un dominio euclideo in una parte libera L e in una parte di torsione. Naturalmente una delle due parti puó essere nulla. Se é nulla la parte di torsione, il modulo é libero, se é nulla la parte libera allora il modulo é di torsione.

Ci possiamo chiedere se la decomposizione ottenuta sia minimale o se e' possibile ancora decomporre qualche modulo ciclico in somma diretta di ciclici piú piccoli. Il seguente lemma ci dice quando ció é possibile.

Lemma 8.2. *Sia A un dominio euclideo e M un A-modulo. Se $m \in M$ e $0 : m = (ab)$ con $(a, b) = 1$, allora*

$$< m >=< am > \oplus < bm >$$

con $0 : ma = (b)$ e $0 : mb = (a)$.

Proof. Sappiamo che per qualche $x, y \in A$ si ha $ax + by = 1$. Allora

$$m = axm + bym \in < am > + < bm > .$$

Ció prova $< m >=< am > + < bm >$. Ma se $cam = dbm$, allora $ca - db \in (ab)$ e quindi $ca - db = abe$. Siccome a e b sono primi tra loro, ció implica $d = ar$. Sostituendo e cancellando a si trova $c = b(r + e)$ e infine $cam = (r + e)abm = 0$.

Inoltre si ha $tbm = 0$ se e solo se $tb \in (ab)$ se e solo se $t \in (a)$. Quindi $0 : mb = (a)$ e analogamente $0 : ma = (b)$. □

Come conseguenza si ha il seguente risultato che prova come la decomposizione ottenuta si possa ancora raffinare giungendo ad una decomposizione in moduli ciclici **primari**.

Teorema 8.3. *Sia A un dominio euclideo, M un A-modulo e sia $m \in M$ tale che $0 : m = (d)$. Se $d = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ e' la decomposizione di d come prodotto di potenze di elementi irriducibili distinti, allora, posto $d_i := d/p_i^{r_i}$, si ha*

$$< m >=< d_1 m > \oplus < d_2 m > \oplus \cdots \oplus < d_s m >$$

e inoltre $0 : d_i m = (p_i^{r_i})$ per ogni i.

Proof. Poniamo $a := p_1^{r_1}$, e $b := p_2^{r_2} \cdots p_s^{r_s} = d_1$. Allora $(a, b) = 1$ e quindi per il precedente lemma si ha

$$< m >=< am > \oplus < md_1 >$$

con $0 : am = (b)$ e $0 : md_1 = (p_1^{r_1})$. Iterando il procedimento si conclude facilmente. □

Un modulo ciclico $< m >$ tale che $0 : m = (p^r)$ con p elemento primo (=irriducibile) di A e $r \geq 1$, si dice **primario**.

Ad esempio se $A = \mathbb{Q}[X]$, $M = A^2$ e

$$F =< (X^2 - 3X + 2, (X - 1)^3), (X - 2, X^2 - 3X + 2) >,$$

abbiamo giá visto che

$$A^2/F \simeq \mathbb{Q}[X]/((X - 2)(X - 1)^2).$$

La dsecomposizione in moduli ciclici primari e' dunque

$$A^2/F \simeq \mathbb{Q}[X]/((X - 2)(X - 1)^2) =< \overline{1} >=< \overline{(X - 1)^2} > \oplus < \overline{X - 2} > .$$

Abbiamo dunque provato che ogni modulo finitamente generato su un dominio euclideo si puó decomporre come somma diretta di moduli ciclici primari. Si potrebbe pensare che la decomposizione si possa ulteriormente raffinare. Ma non e' difficile provare che ogni modulo ciclico primario e' indecomponibile, nel senso che non possiede addendi diretti propri.

Teorema 8.4. *Se $M =< m >$ é un modulo ciclico tale che $0 : m = (0)$ oppure $0 : m = (p^r)$ con p elemento primo di A, allora due qualunque sottomoduli non nulli di M hanno intersezione non nulla.*

Proof. Se $0 : m = (0)$, allora $M \simeq A$ e i suoi sottomoduli sono gli ideali. É chiaro che essendo A integro il prodotto di un elemento non nullo del primo e di uno non nullo del secondo é un elemento non nullo della intersezione.

Se invece $0 : m = (p^r)$ con p primo, ed N un sottomodulo di M, sia $am \in N$ un elemento non nullo. Allora $a \notin (p^r)$ e possiamo quindi scrivere $a = p^s u$ con $u \notin (p)$ e $0 \leq s \leq r - 1$. Poiché u e p^r non hanno fattori a comune, si ha $(u, p^r) = (1)$ e quindi

$$1 = uv + p^r q$$

con v e q opportuni elementi di A. Ne segue

$$amv = p^s uvm = p^s m$$

e quindi $p^s m \in N$. Poiché $s \leq r - 1$, si ha $p^{r-1} m \in N$ con $p^{r-1} m \neq 0$. Ció prova che l'elemento non nullo $p^{r-1} m$ stá in tutti i sottomoduli di M. □

Terminiamo questo paragrafo con un risultato che ci servirá nel seguito e che e', in un certo senso, duale del risultato precedente. E' un teorema che si puó definire di ricomposizione invece che di decomposizione.

Lemma 8.5. *Sia A un dominio euclideo e $M =< m_1 > \oplus < m_2 >$ un A-modulo. Se $0 : m_1 = (a)$, $0 : m_2 = (b)$ e $(a, b) = 1$, allora*

$$M =< m_1 + m_2 >$$

con $0 : (m_1 + m_2) = (ab)$.

Proof. Si ha $ax+by = 1$ e quindi $m_1 = by(m_1+m_2)$ e $m_2 = ax(m_1+m_2)$. Ció prova $M \subseteq< m_1 + m_2 >$ e quindi $M =< m_1 + m_2 >$. Inoltre $c(m_1 + m_2) = 0$ se e solo se $cm_1 = cm_2 = 0$, se e solo se $c \in (a) \cap (b)$, se e solo se $c \in (ab)$, dove abbiamo usato ripetutamente il fatto che A e' euclideo e che $(a, b) = 1$. □

Corollario 8.6. *Se $M =< m_1 > \oplus < m_2 > \oplus \cdots \oplus < m_t >$, con $0 : m_i = (a_i)$, e $(a_i, a_j) = 1$ per ogni $i \neq j$, allora*

$$M =< m_1 + m_2 + \cdots + m_t >$$

con $0 : M = (a_1 a_2 \cdots a_t)$.

Proof. Si ha

$$M = \oplus_i < m_i >=< m_1 + m_2 > \oplus(\oplus_{i\geq 3} < m_i >) = \cdots =< m_1 + m_2 + \cdots + m_t > .$$

□

9 Lo spazio vettoriale V come modulo su $k[X]$.

In questa sezione applichiamo i risultati precedenti alla teoria delle matrici quadrate ad elementi in un corpo k. Indichiamo con $M_n(k)$ lo spazio vettoriale delle matrici quadrate $n \times n$ ad elementi in k e sia V uno spazio vettoriale fissato di dimensione n su k.

Ricordiamo che una matrice quadrata A ad elementi in un corpo k si dice **simile** ad una matrice quadrata B, se esiste una matrice quadrata U invertibile tale che

$$B = U^{-1}AU.$$

Ció equivale a dire che A e B sono le matrici associate mediante basi diverse allo stesso endomorfismo $\varphi : V \to V$.

La matrice A si dice **semplice o diagonalizzabile** se é simile ad una matrice diagonale. Un endomorfismo $\varphi : V \to V$ dello spazio vettoriale V si dice semplice se esiste una base di V tale che la matrice associata a φ mediante tale base é semplice.

Ricordiamo che il polinomio caratteristico di una matrice A é per definizione

$$ch_A(X) = det(XI - A).$$

Il criterio di diagonalizzabilitá dice:

Teorema 9.1. *Una matrice A é semplice se e solo se tutti gli autovalori di A sono in k e per ogni autovalore la dimensione dell'autospazio corrispondente é eguale alla molteplicitá dell'autovalore come radice del polinomio caratteristico di A.*

Ad esempio la matrice $\begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$ non é semplice. Infatti si ha $ch_A(X) = (X-1)^2$ e quindi c'é un solo autovalore con molteplicitá due. L'autospazio corrispondente ha dimensione 1 e quindi A non é semplice.

Ricordiamo che se V é uno spazio vettoriale su k di dimensione n, $Hom(V,V)$ é uno spazio vettoriale con le operazioni cosí definite:

$$(\varphi + \psi)(v) = \varphi(v) + \psi(v)$$
$$(\alpha\varphi)(v) = \varphi(\alpha v).$$

É facile vedere che $Hom(V,V)$ ha dimensione n^2 su k ed é infatti isomorfo allo spazio vettoriale $M_n(k)$.

Se ora $\varphi \in Hom(V,V)$, indichiamo con

$$\varphi^i := \varphi \circ \varphi \circ \cdots \circ \varphi$$

la composizione di φ con se stessa i volte.

Dunque se $\varphi \in Hom(V,V)$ e $f(X) = a_0 + a_1 + \cdots + a_s X^s \in k[X]$ ha senso considerare l'elemento $f(\varphi)$ di $Hom(V,V)$ che opera cosí sui vettori $v \in V$:

$$f(\varphi)(v) = a_0 v + a_1\varphi(v) + a_2\varphi^2(v) + \cdots + a_s\varphi^s(v).$$

Questa notazione permette di dotare V di una struttura di $k[X]$-modulo finitamente generato.

Definizione 9.2. *Sia $\varphi \in Hom(V,V)$ un endomorfismo fissato. Allora il gruppo abeliano V assume una struttura di modulo sul dominio euclideo $k[X]$ mediante la moltiplicazione esterna*

$$k[X] \times V \to V$$

definita da

$$f(X)v := f(\varphi)(v).$$

Ad esempio $(2 + 3X - X^2)v = 2v + 3\varphi(v) - \varphi^2(v)$. Notiamo subito che se $\alpha \in k$, allora la moltiplicazione αv nella struttura di modulo su $k[X]$ coincide con la moltiplicazione αv nella struttura di k-spazio vettoriale.

Ció implica immediatamente che

Lemma 9.3. *Se $v_1, \ldots, v_n$ sono una base di V, allora sono un sistema di generatori di V come modulo su $k[X]$.*

Peró la base di V su k non é mai una base di V su $k[X]$, in quanto V non é libero su $k[X]$. Anzi si vede facilmente che V é un $k[X]$-modulo di torsione.

Notiamo che un polinomio $f(X)$ stá nell'annullatore di V se e solo se $f(\varphi)$ e' l'omomorfismo nullo. Infatti si ha

$$f(X)v = 0, \forall v \in V \Leftrightarrow f(\varphi)(v) = 0, \forall v \in V \Leftrightarrow f(\varphi) = 0 \in Hom(V, V).$$

Lemma 9.4. *L'annullatore di V su $k[X]$ é un ideale non nullo di $k[X]$.*

Proof. Infatti $id, \varphi, \varphi^2, \ldots, \varphi^{n^2}$ sono $n^2 + 1$ vettori di $Hom(V, V)$, che é uno spazio vettoriale di dimensione n^2. Ció implica che tali vettori sono linearmente dipendenti e questo é esattamente quello che dobbiamo dimostrare. □

Definizione 9.5. *L'ideale $0 :_{k[X]} V$ é un ideale non nullo di un dominio ad ideali principali e quindi é un ideale principale. L'unico generatore monico di tale ideale, si chiamerá il* **polinomio minimo** *di φ e si indicherá con $m_\varphi(X)$.*

Si ha

$$m_\varphi(X)v = m_\varphi(\varphi)(v) = 0$$

per ogni $v \in V$, e quindi

$$m_\varphi(\varphi) = 0 \in Hom(V, V).$$

Inoltre se $f(X) \in k[X]$ é un polinomio tale che $f(\varphi) = 0$, allora $f(\varphi)(v) = 0$ per ogni $v \in V$ e quindi $f(X) \in 0 :_{k[X]} V = (m_\varphi(X))$. Quindi $f(X)$ deve essere un multiplo di $m_\varphi(X)$. Ne segue che

Lemma 9.6. *Il polinomio $m_\varphi(X)$ é il polinomio monico di grado minimo che si annulla in φ.*

Analogamente se $A \in M_n(k)$ e $f(X) = a_0 + a_1 + \cdots + a_s X^s \in k[X]$, allora indichiamo con $f(A)$ la matrice di $M_n(k)$ cosí definita

$$f(A) := a_0 I + a_1 A + a_2 A^2 + \cdots + a_s A^s.$$

Ció ci permette di definire una applicazione

$$\rho : k[X] \to M_n(k)$$

ponendo $\rho(f(X)) = f(A)$. É facile vedere che ρ é un omomorfismo di anelli il cui nucleo é dunque un ideale di $k[X]$ che si dimostra essere non nullo.

Definizione 9.7. *L'unico generatore monico di $Ker(\rho)$ si chiama il* **polinomio minimo** *di A e si indica con $m_A(X)$.*

Se $\underline{v} = v_1, \ldots, v_n$ é una base di V su k, e $f(X) \in k[X]$, é facile vedere che

$$f(M_{\underline{v},\varphi}) = M_{\underline{v},f(\varphi)}$$

ossia la matrice associata a $f(\varphi)$ mediante $\underline{v}$ coincide con la trasformata mediante $f(X)$ della matrice associata a φ mediante la stessa base. Allora, se si pone $A = M_{\underline{v},\varphi}$, e $f(X) \in k[X]$, si ottiene:

$$f(A) = 0 \Longleftrightarrow f(M_{\underline{v},\varphi}) = 0 \Longleftrightarrow M_{\underline{v},f(\varphi)} = 0 \Longleftrightarrow f(\varphi) = 0.$$

Ne segue

Lemma 9.8. *Se $A = M_{\underline{v},\varphi}$, il polinomio minimo di A e quello di φ coincidono.*

Ad esempio se $A = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}$, si ha $(A - 2I)^2 = 0$ e quindi $m_A(X) = (X-2)^2$ oppure $m_A(X) = (X-2)$. Poiché $A \neq 2I$, si ha $m_A(X) = (X-2)^2$.

10 I sottomoduli di V su $k[X]$.

Siccome vogliamo applicare il teorema di struttura dei moduli finitamente generati su un dominio euclideo al $k[X]$-modulo V, siamo interessati a capire prima di tutto quali siano i sottomoduli di V su $k[X]$. Come sempre in questo paragrafo, V é uno spazio vettoriale di dimensione n e $\varphi : V \to V$ é un endomorfismo di spazi vettoriali.

Lemma 10.1. *Se $W \subseteq V$ e' un sottomodulo di V su $k[X]$, allora W e' anche un sottospazio vettoriale su k ed e' φ-invariante nel senso che $\varphi(W) \subseteq W$.*

Proof. W e' un sottogruppo del gruppo abeliano di V e se $\alpha \in k$ e $w \in W$, abbiamo giá visto che αw ha lo stesso significato su k e su $k[X]$, quindi W e' sottospazio vettoriale di V. Poi se $w \in W$, si ha

$$Xw = \varphi(w) \in W$$

e quindi W e' φ-invariante. □

E' chiaro che se $V = W \oplus T$ come moduli su $k[X]$, allora $V = W \oplus T$ anche come spazi vettoriali: infatti l'essere $W \cap T = \{0\}$ non dipende dagli scalari.

Prima di applicare il teorema di struttura dei moduli finitamente generati su un dominio euclideo al modulo V, ci serve studiare i sottomoduli ciclici di V. Nel seguito useremo la notazione $< v >$ per indicare il sottomodulo ciclico generato dal vettore v su $k[X]$. Da non confondere con il sottospazio vettoriale generato dal vettore v su k. Il primo e' costituito dai vettori $f(X)v$ al variare di $f(X) \in k[X]$, il secondo dai vettori αv al variare di α in k. Naturalmente $< v >$ e' anche uno spazio vettoriale su k e il calcolo della sua dimensione e' il problema risolto nel seguente teorema, ove scriveremo $0 :_{k[X]} v$ invece che $0 :_{k[X]} < v >$.

Teorema 10.2. *Sia $v \in V$ e d il grado di un generatore $g(X)$ dell'ideale $0 :_{k[X]} v$ di $k[X]$. Allora $v, \varphi(v), \varphi^2(v), \ldots, \varphi^{d-1}(v)$ sono una base di $< v >$ su k. In particolare* $\dim_k < v >= d$.

Proof. Un elemento w del $k[X]$-modulo generato da v e' del tipo $w = f(X)v$; si ha $f(X) = q(X)g(X) + r(X)$ ove $r(X) = \sum_{i=0}^{j} a_i X^i$ con $j \leq d-1$. Ne segue

$$w = f(X)v = r(X)v = a_0 v + a_1 \varphi(v) + \cdots + a_j \varphi^j(v)$$

e quindi $v, \varphi(v), \varphi^2(v), \ldots, \varphi^{d-1}(v)$ generano $< v >$ su k.

Se poi $\sum_{i=0}^{d-1} a_i \varphi^i(v) = 0$, posto $f(X) := \sum_{i=0}^{d-1} a_i X^i$, si ha $0 = f(X)v$ e quindi $f(X) \in 0 :_{k[X]} V = (g(X))$. Per motivi di gradi deve essere $f(X) = 0$ e quindi $a_0 = a_1 = \cdots = a_{d-1} = 0$. Ció prova che i vettori $v, \varphi(v), \varphi^2(v), \ldots, \varphi^{d-1}(v)$ sono anche linearmente indipendenti. □

Abbiamo anche provato che

Corollario 10.3. *Se V é ciclico su $k[X]$, allora il grado del polinomio minimo di φ é eguale alla dimensione di V su k.*

Osserviamo che vale anche il viceversa di questo enunciato. Proveremo nel seguito che se il grado del polinomio minimo di φ é eguale alla dimensione di V su k, allora V é un modulo ciclico su $k[X]$..

11 La forma canonica razionale di una matrice quadrata

Applicando il teorema di struttura dei moduli finitamente generati su un dominio euclideo al $k[X]$-modulo V, sappiamo che e' possibile decomporre V nella somma diretta di moduli ciclici:

$$V =< v_1 > \oplus < v_2 > \oplus \cdots \oplus < v_s >$$

con

$$0 : v_i = (f_i(X))$$

per ogni $i = 1, \ldots, s$. E' chiaro che i polinomi $f_i(X)$ sono non nulli, perche' ogni vettore di V ha torsione su $k[X]$, e sono non invertibili, perché chiaramente i v_i non sono nulli. Si puó operare in modo che i polinomi $f_i(X)$ siano anche monici.

Per ogni $i = 1, \ldots, s$ poniamo $d_i = deg(f_i(X))$ e, in accordo con il Teorema 10.2, scegliamo come base di $< v_i >$ su k i vettori

$$v_i, \varphi(v_i), \varphi^2(v_i), \ldots, \varphi^{d_i - 1}(v_i).$$

Poiché V é la somma diretta su k dei sottospazi $< v_1 >, < v_2 >, \cdots < v_s >$, i vettori

$$v_1, \varphi(v_1), \ldots, \varphi^{d_1-1}(v_1), v_2, \varphi(v_2), \ldots, \varphi^{d_2-1}(v_2), \ldots, v_r, \varphi(v_r), \ldots, \varphi^{d_r-1}(v_r)$$

sono una base di V su k.

Se scriviamo $f_i(X) = \sum_{j=0}^{d_i-1} a_{ji} X^j + X^{d_i}$, notiamo che si ha

$$0 = f_i(X)v_i = \sum_{j=0}^{d_i-1} a_{ji}\varphi^j(v_i) + \varphi^{d_i}(v_i)$$

e quindi

$$\varphi\left(\varphi^{d_i-1}(v_i)\right) = \varphi^{d_i}(v_i) = -\sum_{j=0}^{d_i-1} a_{ji}\varphi^j(v_i).$$

Ne segue che la matrice associata a φ rispetto a questa base é la seguente matrice a blocchi:

$$\begin{pmatrix}
0 & 0 & \ldots & 0 & -a_{01} & & & & & & & & & & \\
1 & 0 & \ldots & 0 & -a_{11} & & & & & & & & & & \\
0 & 1 & \vdots & 0 & -a_{21} & & & 0 & & \ldots & & & 0 & & \\
\vdots & \vdots & \ddots & \vdots & \vdots & & & & & & & & & & \\
0 & 0 & \ldots & 1 & -a_{d_1-1\ 1} & & & & & & & & & & \\
 & & & & & 0 & 0 & \ldots & 0 & -a_{02} & & & & & \\
 & & & & & 1 & 0 & \ldots & 0 & -a_{12} & & & & & \\
 & & 0 & & & 0 & 1 & \vdots & 0 & -a_{22} & \ldots & & & 0 & \\
 & & & & & \vdots & \vdots & \ddots & \vdots & \vdots & & & & & \\
 & & & & & 0 & 0 & \ldots & 1 & -a_{d_2-1\ 2} & & & & & \\
 & & \ldots & & & & & \ldots & & & \ddots & & & \ldots & \\
 & & & & & & & & & & & 0 & 0 & \ldots & 0 & -a_{0r} \\
 & & & & & & & & & & & 1 & 0 & \ldots & 0 & -a_{1r} \\
 & & 0 & & & & & 0 & & \ldots & 0 & 1 & \vdots & 0 & -a_{2r} \\
 & & & & & & & & & & & \vdots & \vdots & \ddots & \vdots & \vdots \\
 & & & & & & & & & & & 0 & 0 & \ldots & 1 & -a_{d_r-1\ r}
\end{pmatrix}$$

Definizione 11.1. *Diremo che la matrice precedente e' una* **forma canonica razionale di una qualunque matrice associata a** φ.

Data la matrice

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

corrispondente all'omomorfismo

$$\varphi : k^3 \to k^3$$

definito su una base v_1, v_2, v_3 di k^3 mediante le assegnazioni

$$\varphi(v_1) = v_2 + v_3, \quad \varphi(v_2) = v_2, \quad \varphi(v_3) = -v_1 + v_2 + v_3,$$

si osservi che

$$v - 1 = v_2 + (2 - X)v_3 \in < v_2 > + < v_3 > .$$

Inoltre si puó provare che

$$V = < v_2 > \oplus < v_3 >$$

con $0 :_{k[X]} v_2 = (X - 1)$, e $0 :_{k[X]} v_3 = ((X - 1)^2)$. Se scegliamo come base di V i vettori v_2 per il primo modulo ciclico, e $v_3, \varphi(v_3)$ per il secondo, una forma canonica razionale della matrice A é

$$\left(\begin{array}{c|cc} 1 & 0 & 0 \\ - & - & - \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{array}\right)$$

Data la matrice

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

si puó provare che

$$V = < v_2 - v_3 > \oplus < v_4 - v_1 >$$

con

$$0 : (v_2 - v_3) = (X - 1), \quad 0 : (v_4 - v_1) = ((X - 1)^2(X - 2)).$$

Scegliamo come base per V i vettori

$$v_2 - v_3, v_4 - v_1, \varphi(v_4 - v_1) = -2v_1 + v_2 - v_3 + v_4, \varphi^2(v_4 - v_1) = -4v_1 + 3v_2 - 2v_3.$$

Una forma canonica razionale della matrice A é quindi

$$\left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ - & - & - & - \\ 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & -5 \\ 0 & 0 & 1 & 4 \end{array}\right)$$

Notiamo che un aforma canonica razionale di una data matrice A si puó determinare su un campo qualunque k ed é detrminata dalla decomposizione di V in somma diretta di moduli ciclici. Non é particolarmente espressiva, ma é la forma migliore che si puó ottenere senza restrizioni sul corpo di base.

12 La forma canonica di Jordan di una matrice quadrata complessa

In questo paragrafo determiniamo la forma canonica di Jordan di una matrice quadrata sui complessi. Questa non é una forma razionale perché la sua definizione dipende dal essere capaci di risolvere equazioni polinomiali, cosa che in generale non si puó fare con operazioni razionali. Sicuramente si puó fare su un corpo algebricamente chiuso, ad esempio sul corpo complesso $\mathbf{C}$. Quindi, in questo paragrafo, il corpo di base sará sempre il corpo complesso $\mathbf{C}$.

Si giungerá alla forma canonica di Jordan partendo dalla decomposizione giá acquisita di V come somma diretta di moduli ciclici e decomponendo ulteriormente tali moduli secondo il Teorema 8.3.

Partendo dalla decomposizione di V come somma diretta di moduli ciclici,

$$V =< w_1 > \oplus < w_2 > \oplus \cdots \oplus < w_r >$$

con $0 : w_i = (f_i(X))$, per ogni $i = 1, \ldots, r$, possiamo decomporre ciascun $f_i(X)$ nel prodotto di potenze di fattori distinti irriducibili e quindi lineari in $\mathbf{C}[X]$:

$$f_i(X) = \prod_{j=1}^{t} (X - \lambda_j)^{p_j}.$$

Per ogni $j = 1, \ldots, t$, poniamo, come nel citato Teorema 8.3,

$$h_j := \prod_{k \neq j} (X - \lambda_k)^{p_k} = \frac{f_i(X)}{(X - \lambda_j)^{p_j}}.$$

Allora si ha

$$< w_i >=< h_1(X)w_i > \oplus < h_2(X)w_i > \oplus \cdots \oplus < h_t(X)w_i >$$

con

$$0 : h_j(X)w_i = ((X - \lambda_j)^{p_j}).$$

Allora si ottiene una decomposizione di V come somma diretta di moduli ciclici primari

$$V =< v_1 > \oplus < v_2 > \oplus \cdots \oplus < v_s >$$

con $0 : v_i = ((X - \lambda_i)^{t_i})$. Notiamo che puó aversi con $i \neq j$, $\lambda_i = \lambda_j$.

Ora, se $< v >$ é ciclico primario con $0 : v = ((X - \lambda)^t)$, poniamo $\psi := \varphi - \lambda\ id$. Per il Teorema 10.2, i vettori $v, \varphi(v), \cdots, \varphi^{t-1}(v)$ sono una base su k per $< v >$, e inoltre si ha

$$\varphi^i(v) = (\psi + \lambda\ id)^i(v) \in < v, \psi(v), \cdots, \psi^{t-1}(v) > .$$

Ció prova che anche $v, \psi(v), \cdots, \psi^{t-1}(v)$ sono una base su k per $< v >$.

In questo caso si ha: se $i \leq t-2$

$$\varphi(\psi^i(v)) = (\psi + \lambda\ id)(\psi^i(v)) = \lambda\psi^i(v) + \psi^{i+1}(v) \tag{1}$$

mentre

$$\varphi(\psi^{t-1}(v)) = (\psi + \lambda\ id)(\psi^{t-1}(v)) = \lambda\psi^{t-1}(v) + \psi^t(v) = \lambda\psi^{t-1}(v) \tag{2}$$

in quanto

$$\psi^t(v) = (\varphi - \lambda\ id)^t(v) = (X - \lambda)^t v = 0.$$

Torniamo quindi alla decomposizione $V =< v_1 > \oplus < v_2 > \oplus \cdots \oplus < v_s >$ con $0 : v_i = ((X - \lambda_i)^{t_i})$ e scegliamo come base di $< v_i >$ su k i vettori

$$v_i, \psi_i(v_i), \psi_i^2(v_i), \ldots, \psi_i^{t_i-1}(v_i)$$

ove, per ogni $i = 1, \cdots, s$, si ponga $\psi_i := \varphi - \lambda_i\ id$.

Poiché V é la somma diretta su k dei sottospazi $< v_1 >, < v_2 >, \cdots < v_s >$, i vettori

$$v_1, \psi_1(v_1), \ldots, \psi_1^{t_1-1}(v_1), v_2, \psi_2(v_2), \ldots, \psi_2^{t_2-1}(v_2), \ldots, v_s, \psi_s(v_s), \ldots, \psi_s^{t_s-1}(v_s)$$

sono una base di V su k. Tale base si dice una base di Jordan di V.

Allora usando (1) e (2), é immediato vedere che la matrice associata a φ, rispetto a questa base di Jordan, é la seguente matrice a blocchi:

$$\begin{pmatrix}
\lambda_1 & 0 & 0 & \ldots & 0 & 0 & & & & & & & & & & & & \\
1 & \lambda_1 & 0 & \ldots & 0 & 0 & & & & & & & & & & & & \\
0 & 1 & \lambda_1 & \ldots & 0 & 0 & & & & & & & & & & & & \\
\vdots & \vdots & \ddots & \ddots & \vdots & \vdots & & & 0 & & & \ldots & & & 0 & & & \\
\vdots & \vdots & \vdots & \ddots & \ddots & \vdots & & & & & & & & & & & & \\
0 & 0 & 0 & \ldots & 1 & \lambda_1 & & & & & & & & & & & & \\
& & & & & & \lambda_2 & 0 & 0 & \ldots & 0 & 0 & & & & & & \\
& & & & & & 1 & \lambda_2 & 0 & \ldots & 0 & 0 & & & & & & \\
& & & & & & 0 & 1 & \lambda_2 & \ldots & 0 & 0 & & & & & & \\
& & 0 & & & & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \cdots & & & 0 & & \\
& & & & & & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & & & & & & \\
& & & & & & 0 & 0 & 0 & \ldots & 1 & \lambda_2 & & & & & & \\
& & \ldots & & & & & & \ldots & & & \ddots & & & \ldots & & & \\
& & & & & & & & & & & & \lambda_t & 0 & 0 & \ldots & 0 & 0 \\
& & & & & & & & & & & & 1 & \lambda_t & 0 & \ldots & 0 & 0 \\
& & & & & & & & & & & & 0 & 1 & \lambda_t & \ldots & 0 & 0 \\
& & 0 & & & & & & 0 & & & \cdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
& & & & & & & & & & & & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\
& & & & & & & & & & & & 0 & 0 & 0 & \ldots & 1 & \lambda_t
\end{pmatrix}$$

ove, magari dopo permutazione degli elementi della base di Jordan, i blocchi corrispondenti ad uno stesso autovalore λ sono messi vicini, uno dopo l'altro, in ordine crescente di dimensione.

Abbiamo cosí provato che ogni matrice A quadrata sui complessi é equivalente ad una matrice di Jordan, ossia ad una matrice a blocchi tali che

a) sulla diagonale principale c'e' uno stesso numero complesso,

b) sulla sottodiagonale principale ci sono tutti 1

c) nelle altre posizioni ci sono degli 0.

In realtá e' chiaro che non e' necessario avere matrici complesse; dal procedimento descritto si capisce che ció che e' essenziale e' il fatto che i polinomi $f_i(X)$, che generano gli annullatori dei moduli ciclici nella decomposizione di V, si possano decomporre nel prodotto di fattori lineari.

Determiniamo ad esempio una matrice di Jordan simile alla matrice

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

Si era trovato che $f_1(X) = X - 1,\ f_2(X) = (X-1)^2$ e si era giunti alla decomposizione

$$V =< v_2 > \oplus < v_3 >$$

con $0 : v_2 = (X-1)$, $0 : v_3 = (X-1)^2$. Se scegliamo allora come base per V i vettori $v_2, v_3, \psi(v_3)$, la matrice associata φ rispetto a tale base é la matrice

$$J(\varphi) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Infatti si aveva

$$\varphi(v_1) = v_2 + v_3,\ \varphi(v_2) = v_2,\ \varphi(v_3) = -v_1 + v_2 + 2v_3$$

e quindi $\psi(v_3) = -v_1 + v_2 + v_3$ e la base scelta é $v_2, v_3, -v_1 + v_2 + v_3$. Si ha

$$\varphi(v_2) = v_2,\ \varphi(v_3) = (-v_1 + v_2 + v_3) + v_3,\ \varphi(-v_1 + v_2 + v_3) = -v_1 + v_2 + v_3.$$

Se invece

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

si era trovato

$$f_1(X) = X - 1, \quad f_2(X) = (X-1)^2(X-2)$$

e si era giunti alla decomposizione

$$V =< v_2 - v_3 > \oplus < v_4 - v_1 >$$

con

$$0 : (v_2 - v_3) = (X - 1), \quad 0 : (v_4 - v_1) = ((X - 1)^2(X - 2)).$$

Il primo sottomodulo non si puó ulteriormente spezzare. Il secondo invece si spezza cosí:

$$< v_4 - v_1 >=< (X - 1)^2(v_4 - v_1) > \oplus < (X - 2)(v_4 - v_1) >=$$

$$=< -v_1 + v_2 - v_4 > \oplus < v_2 - v_3 - v_4 >$$

con $0 : (-v_1 + v_2 - v_4) = ((X - 2))$, e $0 : (v_2 - v_3 - v_4) = ((X - 1)^2)$.

Si sceglie come base di V quella formata dai vettori:

$$v_2 - v_3,\ v_2 - v_3 - v_4,\ \psi(v_2 - v_3 - v_4) = v_3 - v_4,\ -v_1 + v_2 - v_4.$$

Allora una matrice di Jordan simile ad A é la matrice:

$$\left(\begin{array}{c|cc|c} 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 2 \end{array}\right)$$

Il problema cruciale e' ora quello che potrebbero esserci diverse matrici di Jordan simili ad una data matrice A. In realtá, nel seguente teorema, si prova che, sui complessi, una matrice di Jordan simile ad A e' univocamente determinata.

Teorema 12.1. *Se V e' uno spazio vettoriale su $\mathbb{C}$ e $\varphi \in Hom(V, V)$, una matrice di Jordan per φ e' univocamente determinata dalle dimensioni delle immagini dei morfismi $(\varphi - \lambda\ id)^j$, per ogni autovalore λ e per ogni $j \geq 1$.*

Proof. Dimostriamo per semplicitá il teorema nel caso di un solo autovalore λ. Supponiamo che la matrice di Jordan sia costituita da t blocchi di misura $r_1, \cdots, r_t$ rispettivamente; allora $r_1 + \cdots + r_t = n$ se n e' la dimensione di V.

Se $v_{1,1}, \cdots, v_{1,r_1}, v_{2,1}, \cdots, v_{2,r_2}, \cdots, v_{t,1}, \cdots, v_{t,r_t}$ e' la base di V rispetto a cui la matrice di Jordan rappresenta φ, e' chiaro che si ha $\varphi(v_{1,1}) = \lambda v_{1,1} + v_{1,2}$ e quindi $v_{1,2} = \psi(v_{1,1})$, ove si ponga

$$\psi := \varphi - \lambda\ id.$$

Similmente per gli altri elementi della base, che quindi si puó riscrivere piú semplicemente

$$v_1, \psi(v_1), \cdots, \psi^{r_1-1}(v_1), v_2, \psi(v_2), \cdots, \psi^{r_2-1}(v_2), \cdots, v_t, \psi(v_t), \cdots, \psi^{r_t-1}(v_t).$$

Indicheremo con $\rho(\psi^j)$ la dimensione di $Im(\psi^j)$. I trasformati mediante ψ degli elementi della base sono i vettori

$$\psi(v_1), \psi^2(v_1), \cdots, \psi^{r_1-1}(v_1), 0, \psi(v_2), \cdots, \psi^{r_2-1}(v_2), 0, \cdots, \psi(v_t), \cdots, \psi^{r_t-1}(v_t), 0.$$

Ció prova che

$$\rho(\psi) = (r_1 - 1) + (r_2 - 1) + \cdots + (r_t - 1) = n - t$$

e quindi $t = n - \rho(\psi)$. Procedendo a calcolare ψ^2 sugli elementi della base di Jordan si vede che

$$\rho(\psi^2) = (r_1 - 2) + (r_2 - 2) + \cdots + (r_t - 2) + \sharp\{j \mid r_j = 1\}.$$

Ne segue

$$\sharp\{j \mid r_j = 1\} = \rho(\psi^2) - n + 2t = \rho(\psi^2) + n - 2\rho(\psi).$$

Ma si ha anche

$$\rho(\psi^3) = n - 3t + \sharp\{j \mid r_j \leq 2\}$$

e quindi

$$\begin{aligned}\sharp\{j \mid r_j = 2\} &= \rho(\psi^3) - n + 3t - \sharp\{j \mid r_j = 1\} \\ &= \rho(\psi^3) - n + 3t - \rho(\psi^2) + n - 2t \\ &= \rho(\psi^3) - \rho(\psi^2) + t \\ &= \rho(\psi^3) - \rho(\psi^2) + n - \rho(\psi).\end{aligned}$$

Procedendo cosí determiniamo gli interi r_i univocamente mediante gli interi $\rho(\psi^j)$ come richiesto. □

Avendo dimostrato la unicitá della matrice di Jordan simile ad una matrice data A, possiamo indicare tale matrice di Jordan con $J(A)$.

Corollario 12.2. *Due matrici complesse A e B sono equivalenti se e solo $J(A) = J(B)$.*

Proof. Essendo A simile a $J(A)$ e B simile a $J(B)$, e' chiaro che se $J(A) = J(B)$ allora A e' simile a B. Se poi A e' simile a B, allora $J(A)$ e $J(B)$ sono matrici di Jordan dello stesso omomorfismo e quindi coincidono. □

Vediamo nel caso delle matrici 2×2 come gli interi $\rho(\psi^j)$ determinino i possibili blocchi di Jordan.

Abbiamo due possibili matrici di Jordan corrispondenti ai valori $\{2\}$ o $\{1, 1\}$

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

Nel primo caso si ha

$$\varphi(v_1) = \lambda v_1, \quad \varphi(v_2) = \lambda v_2,$$

e quindi

$$\psi(v_1) = \psi(v_2) = 0$$

e $\rho(\psi) = 0$.

Nel secondo caso si ha

$$\varphi(v_1) = \lambda v_1 + v_2, \quad \varphi(v_2) = \lambda v_2,$$

e quindi

$$\psi(v_1) = v_2, \quad \psi(v_2) = 0$$

e $\rho(\psi) = 1$.

Nel caso delle matrici 3×3, si hanno tre possibili forme di Jordan corrispondenti ai valori $\{3\}$, $\{1, 2\}$ o $\{1, 1, 1\}$

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

Nel primo caso si ha $\rho(\psi) = 1$, nel secondo $\rho(\psi) = 2$ e nel terzo $\rho(\psi) = 3$.

Per le matrici 4×4, si hanno 5 possibili forme di Jordan corrispondenti ai valori $\{1, 1, 1, 1\}$, $\{4\}$, $\{1, 3\}$, $\{2, 2\}$ e $\{1, 1, 2\}$

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

I valori di $\rho(\psi)$ sono rispettivamente $\{0, 3, 2, 2, 1\}$, quelli di $\rho(\psi^2)$ nel terzo e quarto caso sono rispettivamente $\{1, 0\}$. Quindi i valori di $\rho(\psi)$ in questo caso non sono sufficienti a distinguere le diverse forme di Jordan: servono anche i valori di $\rho(\psi^2)$.

13 La decomposizione di V come somma diretta di moduli ciclici

Studiamo in questo paragrafo un algoritmo per la determinazione dei moduli ciclici su $k[X]$ in cui V si decompone. Procediamo esattamente come nella dimostrazione del Teorema 8.1.

Dobbiamo presentare V come quoziente di un modulo libero. Consideriamo una base $\underline{v} = v_1, \ldots, v_n$ di V su k e sia $A = M_{\underline{v},\varphi}$. Ció significa che

$$(v_1, \ldots, v_n)A = (\varphi(v_1), \ldots, \varphi(v_n)).$$

Siccome $\underline{v}$ é un sistema di generatori di V su $k[X]$, una presentazione é data dall'epimorfismo

$$\sigma : k[X]^n \to V$$

definito sulla base canonica $e_1, \ldots, e_n$ di $k[X]^n$ cosí:

$$\sigma(e_i) = v_i.$$

Dunque se $(f_1(X), \ldots, f_n(X)) \in k[X]^n$ si ha:

$$\sigma(f_1(X), \ldots, f_n(X)) = \sum f_i(X)v_i = (f_1(X), \ldots, f_n(X))^t(v_1, \ldots, v_n).$$

Per il primo teorema di omomorfismo si ha un isomorfismo

$$k[X]^n/Ker(\sigma) \to V$$

che manda l'elemento $\overline{\alpha}$ in $\sigma(\alpha)$.

Abbiamo giá visto che il $k[X]$-modulo V é di torsione e quindi, per il teorema 7.6, il sottomodulo $Ker(\sigma)$ é libero di rango n. Dobbiamo ora trovare una base di $Ker(\sigma)$.

Osserviamo che si ha

$$(v_1, \ldots, v_n)XI = (Xv_1, \ldots, Xv_n) = (\varphi(v_1), \ldots, \varphi(v_n)) = (v_1, \ldots, v_n)A.$$

Dunque otteniamo

$$(v_1, \ldots, v_n)(XI - A) = 0.$$

Questo ci dice che gli n vettori di $k[X]^n$ determinati dalle colonne della matrice $XI - A$ sono in $Ker(\sigma)$.

Proviamo allora che tali vettori sono un sistema di generatori per $Ker(\sigma)$. Ció proverá che sono infatti una base.

Teorema 13.1. *I vettori di $k[X]^n$ costituiti dalle colonne della matrice $XI - A$ sono un sistema di generatori per $Ker(\sigma)$ e quindi ne sono un base.*

Proof. Osserviamo che il sottomodulo N di $k[X]^n$ generato dai vettori colonna della matrice $XI - A$ é costituito dai vettori

$$(g_1, \ldots, g_n)^t(XI - A) = (g_1, \ldots, g_n)(XI - {}^tA)$$

al variare di $(g_1, \ldots, g_n)$ in $k[X]^n$.

Se ora $\alpha = (f_1, \ldots, f_n) \in k[X]^n$, possiamo scrivere per ogni $i = 1, \ldots, n$

$$f_i = c_i + Xg_i$$

ove $c_i \in k$ e $g_i = 0$ oppure ha grado minore di quello di f_i. Dunque si ottiene

$$\alpha = (f_1, \ldots, f_n) = (c_1, \ldots, c_n) + (g_1, \ldots, g_n)(XI - {}^tA) + (g_1, \ldots, g_n){}^tA.$$

Applicando lo stesso ragionamento al vettore $(g_1, \ldots, g_n)A$, dopo un numero finito di passi (finito perché ad ogni passo i gradi dei polinomi diminuiscono), potremo scrivere per ogni $\alpha \in k[X]^n$

$$\alpha = \beta + (c_1, \ldots, c_n)$$

con $\beta \in N$ e $c_i \in k$. Se ora $\alpha \in Ker(\sigma)$ avremo

$$0 = \sigma(\alpha) = \sigma(c_1, \ldots, c_n) = \sum c_i v_i$$

e quindi $c_1 = c_2 = \cdots = c_n = 0$. Ció prova che $Ker(\sigma) \subseteq N$ e quindi la tesi. $\square$

Se indichiamo con $g_1, \ldots, g_n$ la base di $Ker(\sigma)$ appena trovata, é chiaro che si ha

$$(g_1, \ldots, g_n) = (e_1, \ldots, e_n)(XI - A).$$

In accordo con il Teorema 7.5, dobbiamo ora operare con matrici elementari sulla matrice $XI - A$ e determinare cosí due matrici invertibili U e Z di tipo $n \times n$ ad elementi in $k[X]$, tali che

$$\Delta := U(XI - A)Z = \begin{pmatrix} f_1(X) & 0 & \ldots & 0 \\ 0 & f_2(X) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & f_n(X) \end{pmatrix}$$

con $f_i(X) \in k[X]$.

Si ottiene dunque

$$(g_1, \ldots, g_n)Z = (e_1, \ldots, e_n)(XI - A)Z = (e_1, \ldots, e_n)U^{-1}\Delta.$$

Poiche' U^{-1} e' invertibile, ponendo

$$(\epsilon_1, \cdots, \epsilon_n) := (e_1, \ldots, e_n)U^{-1},$$

si ha che $\{\epsilon_1, \cdots, \epsilon_n\}$ e' una base di $k[X]^n$ e $\{\epsilon_1 f_1, \cdots, \epsilon_n f_n\}$ e' una base di $Ker(\sigma)$.

Inoltre si ottiene

$$k[X]^n / Ker(\sigma) =< \overline{\epsilon_1} > \oplus \cdots \oplus < \overline{\epsilon_n} >$$

con $0 : \overline{\epsilon_i} = (f_i(X))$ e infine

$$V =< \sigma(\epsilon_1) > \oplus, \cdots, \oplus < \sigma(\epsilon_n) >$$

con $0 : \sigma(\epsilon_i) = (f_i(X))$.

Poiché il rango di $Ker(\phi)$ é n, giá sappiamo che i polinomi $f_1(X), \ldots, f_n(X)$ sono diversi da zero; inoltre possiamo operare in modo che tali polinomi siano anche

monici. É chiaro che se $f_i(X)$ é invertibile in $k[X]$, allora $\sigma(\epsilon_i) = 0$ e l'addendo corrispondente e' nullo.

Ricapitoliamo il procedimento per giungere alla decomposizione di V come somma diretta di moduli ciclici.

Tenendo conto delle operazioni sulle righe compiute nel processo di diagonalizzazione della matrice $XI - A$,

a) si determina U^{-1},

b) si calcola la base $(\epsilon_1, \ldots, \epsilon_n) := (e_1, \ldots, e_n)U^{-1}$

c) e infine si calcolano i vettori $w_1, \ldots, w_r$ con le formule:

$$w_1 = \sigma(\epsilon_1), w_2 = \sigma(\epsilon_2), \ldots, w_r = \sigma(\epsilon_n).$$

Sviluppiamo un esempio concreto.

Esempio 13.2. *Sia data la matrice*

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

Con operazioni elementari sulle righe si trasforma $XI - A$ cosí:

$$XI - A = \begin{pmatrix} X & 0 & 1 \\ -1 & X-1 & -1 \\ -1 & 0 & X-2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & X \\ -1 & X-1 & -1 \\ X-2 & 0 & -1 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ -1 & X-1 & X-1 \\ X-2 & 0 & -(X-1)^2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-1 & X-1 \\ X-2 & 0 & -(X-1)^2 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-1 & X-1 \\ 0 & 0 & -(X-1)^2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-1 & 0 \\ 0 & 0 & -(X-1)^2 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-1 & 0 \\ 0 & 0 & (X-1)^2 \end{pmatrix}$$

Quindi

$$f_1(X) = X - 1, \ f_2(X) = (X-1)^2$$

e

$$U^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ X-2 & 0 & 1 \end{pmatrix}$$

Allora

$$\epsilon_1 = e_1 - e_2 + (X-2)e_3, \quad \epsilon_2 = e_2, \quad \epsilon_3 = e_3,$$

e infine

$$w_1 = \sigma(\epsilon_2) = \sigma(e_2) = v_2, \quad w_2 = \sigma(\epsilon_3) = \sigma(e_3) = v_3.$$

La decomposizione ottenuta é quindi

$$V =< v_2 > \oplus < v_3 >$$

con $0 : v_2 = (X-1)$, $0 : v_3 = (X-1)^2$.

Esempio 13.3. *Un altro esempio. Sia data la matrice*

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

Operando come sopra (ma in questo caso i calcoli sono piú complicati) si ottiene la matrice diagonale

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X-1 & 0 \\ 0 & 0 & 0 & (X-1)^2(X-2) \end{pmatrix}$$

Quindi

$$f_1(X) = X-1, \quad f_2(X) = (X-1)^2(X-2)$$

e

$$U^{-1} = \begin{pmatrix} X-2 & -(X-1(X-2) & -(X-2) & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & X-2 & X-1 & 1 \end{pmatrix}$$

Allora con il cambiamento di base

$$(\epsilon_1, \ldots, \epsilon_4) = (e_1, \ldots, e_4)U^{-1},$$

si ottiene in particolare

$$\epsilon_3 = -(X-2)e_1 + (X-1)e_4, \quad \epsilon_4 = -e_1 + e_4$$

e quindi

$$V =< \sigma(\epsilon_3) > \oplus < \sigma(\epsilon_4) >=< v_2 - v_3 > \oplus < v_4 - v_1 >$$

con

$$0 : (v_2 - v_3) = (X-1), \quad 0 : (v_4 - v_1) = ((X-1)^2(X-2)).$$

14 Polinomio minimo e caratteristico di una matrice. Teorema di Cayley-Hamilton

Facciamo alcune considerazioni importanti che discendono dal teorema di decomposizione di V come somma diretta di moduli ciclici. Ricordiamo che A e' la matrice associata ad un endomorfismo φ dello spazio vettoriale V di dimensione n, $det(XI - A)$ e' il polinomio caratteristico $ch_\varphi(X)$ di φ o di A. Ricordiamo inoltre che un elemento λ di k e' un autovalore per φ se esiste un vettore non nullo $v \in V$ tale che $\varphi(v) = \lambda v$. Sappiamo anche che gli autovalori sono esattamente le radici in k del polinomio caratteristico. Se ora Δ e' la matrice diagonale che di ottiene dalla diagonalizzazione della matrice $XI - A$, e se $\{f_1, \cdots, f_n\}$ sono gli elementi sulla diagonale principale, allora si ha

$$\prod_{i=1}^{n} f_i(X) = det(\Delta) = det(U)det(V)det(XI - A) = \alpha\beta\ ch_\varphi(X)$$

con $\alpha, \beta \in k^*$, in quanto le matrici U e V sono invertibili in $k[X]$ e quindi il loro determinante e' una costante non nulla. Poiche' i polinomi $f_i(X)$ sono monici e tale e' anche $ch_\varphi(X)$, si ottiene

$$\prod_{i=1}^{n} f_i(X) = ch_\varphi(X).$$

Ricordiamo che il polinomio minimo $m_\varphi(X)$ di φ o di A, e' il generatore monico dell'ideale $0 :_{k[X]} V$, o anche il polinomio monico di grado minimo che si annulla in φ (o in A). Tale polinomio ha la proprietá seguente: se $g(X) \in k[X]$ e' tale che $g(\varphi) = 0$, allora $g(X)$ e' multiplo di $m_\varphi(X)$.

Teorema 14.1. *Il polinomio minimo di φ e' il minimo comune multiplo dei polinomi $f_1(X), \cdots, f_n(X)$. Quindi*

$$m_\varphi(X) = lcm\{f_1(X), \cdots, f_n(X)\}.$$

Proof. Sia $f(X)$ un minimo comune multiplo monico dei polinomi $f_1(X), \cdots, f_n(X)$. Allora si ha

$$f(X) \in \bigcap_{i=1}^{n}(f_i(X)) = \bigcap_{i=1}^{n} 0 :_{k[X]} w_i = 0 :_{k[X]} V = (m_\varphi(X))$$

e quindi $f(X)$ e' multiplo di $m_\varphi(X)$. Ma si deduce anche che $m_\varphi(X) \in (f_i(X))$ per ogni $i = 1, \cdots, n$, e quindi che $m_\varphi(X)$ e' multiplo di $f(X)$. □

Corollario 14.2. *Il polinomio minimo di φ e' un divisore del polinomio caratteristico.*

Corollario 14.3. Teorema di Cayley-Hamilton *Se $\varphi \in Hom(V,V)$ allora si ha*

$$ch_\varphi(\varphi) = 0$$

ossia ogni endomorfismo annulla il suo polinomio caratteristico.

Proof. Si ha

$$ch_\varphi(X) \in (m_\varphi(X)) = 0 :_{k[X]} V;$$

quindi $ch_\varphi(X)v = 0$ per ogni $v \in V$. Ne segue che $ch_\varphi(\varphi) = 0 \in Hom(V,V)$. □

Notiamo che se $A = M_{\underline{v},\varphi}$ e' la matrice associata a φ mediante la base $\underline{v}$, si ha

$$ch_\varphi(A) = M_{\underline{v}}(ch_\varphi(\varphi)) = M_{\underline{v}}(0) = 0$$

e quindi il polinomio caratteristico si annulla anche in A.

Corollario 14.4. *Il polinomio minimo e il polinomio caratteristico hanno gli stessi fattori irriducibili, magari con diversa molteplicitá. In particolare ogni radice del poinomio caratteristico, ossia ogni autovalore, e' radice anche del polinomio minimo.*

Proof. Se $f(X)$ e' irriducibile in $k[X]$ e divide il polinomio caratteristico, allora $f(X)$ divide $f_i(X)$ per qualche i e quindi divide il polinomio minimo che e' multiplo di tutti gli $f_i(X)$. □

Corollario 14.5. *Se $\varphi \in Hom(V,V)$ sono equivalenti:*

a) V é ciclico su $k[X]$.

b) Il grado di $m_\varphi(X)$ é n.

c) $m_\varphi(X) = ch_\varphi(X)$.

Proof. Se $V =< v >$, allora abbiamo visto nel Corollario 10.3 che il grado di $m_\varphi(X)$ é n. Questo prova che a) implica b). Siccome e' ovvio che b) implica c), basta provare che c) implica a). Ma se $m_\varphi(X) = ch_\varphi(X)$, allora e' chiaro che i polinomi $f_i(X)$ sono a due a due coprimi, altrimenti $ch_\varphi(X) = \prod f_i(X)$ non sarebbe un minimo comune multiplo. Allora si conclude con il lemma di ricostruzione (vedi Corollario 8.6). □

Corollario 14.6. *Se $\varphi \in Hom(V,V)$ sono equivalenti:*

a) φ e' semplice.

b) $m_\varphi(X)$ non ha radici multiple.

c) La matrice di Jordan di φ e' diagonale.

Proof. Se φ e' semplice, allora possiamo trovare una base di V rispetto a cui la matrice associata A e' diagonale. Ma allora e' chiaro che $f_i(X) = X - \lambda_i$ per ogni i e quindi la matrice di Jordan e' diagonale. Ció prova che a) implica b), mentre il viceversa e' ovvio. Se poi A e' diagonale, allora $f_i(X) = X - \lambda_i$ per ogni i e quindi $m_\varphi(X)$ ha radici semplici. Se infine $m_\varphi(X)$ ha radici semplici, anche tutti gli $f_i(X)$ hanno radici semplici. Per come si determina la matrice di Jordan, segue che tale matrice e' diagonale. □

Corollario 14.7. *Se $\varphi \in Hom_{\mathbf{C}}(V, V)$ e per qualche $r \geq 1$ si ha $\varphi^r = id$, allora φ é semplice.*

Proof. Infatti $m_\varphi(X)$ divide $X^r - 1$ e quindi non puó avere radici multiple in quanto $X^r - 1$ non ha radici multiple perche' la sua derivata non si annulla in 1. □

Studiamo ora le matrici di misura piccola e ci chiediamo se la conoscenza del polinomio minimo e del polinomio caratteristico determinano la forma di Jordan.

La risposta e' positiva se $A \in M_n(\mathbf{C})$ con $n \leq 3$.

Facciamo infatti una tabella in cui mettiamo i possibili polinomi minimi, quelli caratteristici e infine la corrispondente matrice di Jordan. Incominciamo con le matrici 2×2.

$$ch_\varphi(X) = (X - \lambda_1)(X - \lambda_2) = m_\varphi(X) \quad J = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

$$ch_\varphi(X) = (X - \lambda)^2 = m_\varphi(X), \quad J = \begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix}$$

$$ch_\varphi(X) = (X - \lambda)^2, \quad m_\varphi(X) = (X - \lambda), \quad J = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

Vediamo le matrici 3×3.

$$ch_\varphi(X) = (X - \lambda_1)(X - \lambda_2)(X - \lambda_3) = m_\varphi(X), \quad J = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}$$

$$ch_\varphi(X) = (X - \lambda_1)^2(X - \lambda_2) = m_\varphi(X), \quad J = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 1 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}$$

$$ch_\varphi(X) = (X - \lambda_1)^2(X - \lambda_2) \quad m_\varphi(X) = (X - \lambda_1)(X - \lambda_2), \quad J = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}$$

$$ch_\varphi(X) = (X-\lambda)^3 = m_\varphi(X), \quad J = \begin{pmatrix} \lambda & 0 & 0 \\ 1 & \lambda & 0 \\ 0 & 1 & \lambda \end{pmatrix}$$

$$ch_\varphi(X) = (X-\lambda)^3 \;\; m_\varphi(X) = (X-\lambda)^2, \quad J = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 1 & \lambda \end{pmatrix}$$

$$ch_\varphi(X) = (X-\lambda)^3 \;\; m_\varphi(X) = (X-\lambda), \quad J = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$$

Osserviamo che nel caso $n = 4$ il risultato non é piú vero. Consideriamo le matrici di Jordan

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

Queste matrici sono diverse ma hanno entrambe

$$ch_\varphi(X) = (X-\lambda)^4, \;\; m_\varphi(X) = (X-\lambda)^2.$$

Possiamo usare questa descrizione per determinare la forma di Jordan della matrice

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

Si ha $ch_A(X) = (X-2)(X-1)^2$, e quindi per il polinomio minimo abbiamo due scelte: $(X-2)(X-1)^2$ o $(X-2)(X-1)$. Ma $(A-2I)(A-I) \neq 0$ e quindi $ch_A(X) = m_A(X)$. Ne segue che

$$J(A) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Corollario 14.8. *Se $A \in M_n(\mathbf{C})$ si ha*

$$ch_A(X) = X^n - Tr(A)X^{n-1} + \cdots + (-1)^n det(A).$$

Proof. Se $\lambda_1, \ldots, \lambda_n$ sono gli autovalori di A ripetuti con la loro molteplicitá di radici del polinomio caratteristico, si ha

$$det(A) = det(J(A)) = \prod_{i=1}^n \lambda_i, \quad Tr(J(A)) = \sum_{i=1}^n \lambda_i = Tr(A).$$

Avendosi

$$ch_A(X) = ch_{J(A)}(X) = X^n - (\sum_{i=1}^{n} \lambda_i)X^{n-1} + \cdots + (-1)^n \prod_{i=1}^{n} \lambda_i$$

la conclusione segue. □

Corollario 14.9. *Se $\varphi \in Hom_{\mathbf{C}}(V,V)$, allora $\varphi = \psi + \eta$ ove $\psi, \eta \in Hom_{\mathbf{C}}(V,V)$, ψ é diagonalizzabile e η é nilpotente.*

Proof. Sia $A := M_{\underline{v},\varphi}$ la matrice asociata a φ mediante la base $\underline{v}$. Allora $J(A) = M_{\underline{w},\varphi}$ con $\underline{w}$ base di Jordan di V.

É chiaro che $J(A) = \Delta + N$ ove Δ é diagonale e N é nilpotente. Se $\psi, \eta \in Hom_{\mathbf{C}}(V,V)$ sono tali che $M_{\underline{w},\psi} = \Delta$, e $M_{\underline{w},\eta} = N$, la conclusione segue. □

Determiniamo la decomposizione in *diagonale piú nilpotente* del seguente endomorfismo

$$\varphi : \mathbf{C}^3 \to \mathbf{C}^3$$

associato mediante le basi canoniche alla matrice

$$A = \begin{pmatrix} 3 & -2 & 0 \\ -1 & 0 & -1 \\ -1 & 3 & 2 \end{pmatrix}$$

Facendo i conti si ottiene

$$U(XI - A)V = \Delta := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (X-3)(X-1)^2 \end{pmatrix}$$

con

$$U^{-1} = \begin{pmatrix} X-3 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & (X-1)^2/2 - 1 & 1 \end{pmatrix}$$

Si ottiene

$$V = < (X-1)^2 v_3 > \oplus < (X-3)v_3 > = < 2v_1 - 2v_3 > \oplus < -v_2 - v_3 > .$$

La forma di Jordan di A é dunque

$$J(A) = \left(\begin{array}{c|cc} 3 & 0 & 0 \\ - & - & - \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{array}\right)$$

mentre la base di Jordan é

$$w_1 = 2v_1 - 2v_3, w_2 - v_2 - v_3, w_3 = (\varphi - id)(-v_2 - v_3) = 2v_1 + 2v_2 - 4v_3.$$

Si ha

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Quindi se si definisce

$$\begin{cases} \psi(w_1) = 3w_1 \\ \psi(w_2) = w_2 \\ \psi(w_3) = w_3 \end{cases} \qquad \begin{cases} \eta(w_1) = 0 \\ \eta(w_2) = w_3 \\ \eta(w_3) = 0 \end{cases}$$

si ha $\varphi = \psi + \eta$ con ψ diagonale e η nilpotente.

Avevamo visto che se $A \in M_n(k)$ possiamo definire una applicazione

$$\rho : k[X] \to M_n(k)$$

ponendo $\rho(f(X)) = f(A)$. Tale applicazione é un omomorfismo di anelli il cui nucleo é dunque un ideale di $k[X]$ che é generato da $m_A(X)$.

Osserviamo ora che pur essendo $M_n(k)$ un anello non commutativo, il suo sottoanello $Im(\rho)$ é un anello commutativo.

Si ha chiaramente

$$Im(\rho) = \{a_0 + a_1A + \cdots + a_sA^s \mid a_i \in k\}$$

e quindi é naturale indicare $Im(\rho)$ con $k[A]$. Per il primo teorema di omomorfismo, si ha un isomorfismo

$$k[X]/(m_A(X)) \simeq k[A].$$

Questo isomorfismo permette di leggere proprietá algebriche di A mediante la struttura di $k[X]/(m_A(X))$, nel caso in cui si conosca $m_A(X)$.

Ad esempio per calcolare la potenza t-ma di un matrice quadrata A, possiamo procedere cosí: facciamo la divisione euclidea

$$X^t = m_A(X)q(X) + r(X)$$

ove $r(X)$ o é nullo oppure ha grado minore del grado di $m_A(X)$, ed allora si ha

$$A^t = m_A(A)q(A) + r(A) = r(A).$$

Osserviamo anche che possiamo calcolare le potenze di A usando la forma di Jordan di A. Infatti si ha $A = XJX^{-1}$ e quindi

$$A^t = XJ^tX^{-1}.$$

Siccome il calcolo delle potenze di una matrice di Jordan é piú semplice del calcolo delle potenze di una matrice qualunque, la formula precedente fornisce una reale semplificazione del calcolo.