CAPITOLO 7

L'ALGEBRA DELLE MATRICI GENERICHE

In quest'ultimo capitolo viene introdotto il concetto di matrice generica e si studiano alcuni risultati sull'algebra delle matrici generiche. Inoltre viene dato un esempio di algebra di divisione di dimensione finita.

7.1 Definizione. Siano K un campo, $n \in \mathbb{N}$ e $Y := \left\{ u_{ij}^{(k)} \mid ij \in \underline{n}], k \in \mathbb{N} \right\}$ un insieme di indeterminate su K commutative e indipendenti. Indichiamo con $K\left[u_{ij}^{(k)}\right]$ l'anello dei polinomi nelle indeterminate appartenenti a Y e poniamo

$$\forall k \in \mathbb{N} \qquad U^{(k)} := \left(u_{ij}^{(k)}\right)_{i,j=1,\ldots,n} \in M_n\left(K\left[u_{ij}^{(k)}\right]\right).$$

Per ogni $k \in \mathbb{N}$, $U^{(k)}$ si dice *matrice generica* $n \times n$ *su* K.
La K-sottoalgebra di $M_n\left(K\left[u_{ij}^{(k)}\right]\right)$ generata da $\{U^{(k)}\}_{k\in\mathbb{N}}$ si denota con $K_n\langle U\rangle$ e si dice *algebra delle matrici generiche* $n \times n$ *su* K.

7.2 Teorema. *Siano K un campo infinito e $n \in \mathbb{N}$. Allora*

$$K_n\langle U\rangle \cong K\langle X\rangle / T(M_n(K)).$$

Dimostrazione. Consideriamo l'omomorfismo

$$\varphi : K\langle X\rangle \to K_n\langle U\rangle, \qquad x_k \mapsto U^{(k)}$$

e dimostriamo che $ker\,\varphi = T(M_n(K))$.
Siano $t \in \mathbb{N}$ e $f(x_1, \ldots, x_t) \in T(M_n(K))$. Poiché

$$M_n\left(K\left[u_{ij}^{(k)}\right]\right) \cong K\left[u_{ij}^{(k)}\right] \bigotimes_K M_n(K),$$

da **(2.18)** e **(3.2)** segue che $f \in T\left(M_n\left(K\left[u_{ij}^{(k)}\right]\right)\right)$. Allora f è un'identità polinomiale per $K_n\langle U\rangle$ essendo $K_n\langle U\rangle$ sottoalgebra di $M_n\left(K\left[u_{ij}^{(k)}\right]\right)$.
Segue

$$\forall\, i_1,\ldots,i_t \in \mathbb{N} \qquad f\left(U^{(i_1)},\ldots,U^{(i_t)}\right) = 0,$$

cioè $f \in ker\,\varphi$.
Viceversa siano $t \in \mathbb{N}$ e $f(x_1,\ldots,x_t) \in ker\,\varphi$. Allora

$$\forall\, i_1,\ldots,i_t \in \mathbb{N} \qquad f\left(U^{(i_1)},\ldots,U^{(i_t)}\right) = 0.$$

Siano $r_1,\ldots,r_t \in M_n(K)$ e, per ogni $k \in \underline{t}\rfloor$, $i,j \in \underline{n}\rfloor$, sia $a_{ij}^{(k)} \in K$ tale che $r_k = \left(a_{ij}^{(k)}\right)$. Consideriamo l'applicazione $\psi : K\left[u_{ij}^{(k)}\right] \to K$ tale che

$$\psi\left(u_{ij}^{(k)}\right) = \begin{cases} a_{ij}^{(k)} & \forall\, k \in \underline{t}\rfloor \\ 0 & \forall\, k \in \mathbb{N} - \underline{t}\rfloor \end{cases}$$

ψ è un omomorfismo di K-algebre e induce un omomorfismo di K-algebre di matrici $\overline{\psi} : M_n\left(K\left[u_{ij}^{(k)}\right]\right) \to M_n(K)$ tale che

$$\overline{\psi}\left(U^{(k)}\right) = \begin{cases} r_k & \forall\, k \in \underline{t}\rfloor \\ 0 & \forall\, k \in \mathbb{N} - \underline{t}\rfloor \end{cases}$$

Allora

$$f(r_1,\ldots,r_t) = \overline{\psi}\left(f\left(U^{(1)},\ldots,U^{(t)}\right)\right) = \overline{\psi}(0) = 0$$

Dall'arbitrarietà di $r_1,\ldots,r_t$ in $M_n(K)$ segue che $f \in T(M_n(K))$ e quindi $ker\,\varphi = T(M_n(K))$.
Per il Teorema di omomorfismo per anelli si ha

$$K_n\langle U\rangle \cong K\langle X\rangle / T(M_n(K)).$$

□

7.3 Corollario. *Siano K un campo infinito e $n \in \mathbb{N}$. Allora $K_n\langle U\rangle$ e $M_n(K)$ sono PI-equivalenti.*

Vogliamo presentare, ora, un importante risultato dovuto ad Amitsur e affermante che, per ogni $n \in \mathbb{N}$, l'algebra delle matrici generiche $K_n\langle U\rangle$ è un dominio d'integrità. La dimostrazione di tale teorema si basa sul Teorema di Posner e sull'esistenza di K-algebre di divisione di dimensione finita n^2 sul proprio centro. Pertanto premettiamo nel seguente esempio la costruzione di un tale tipo di algebre:

7.4 Esempio. (Algebre di divisione di dimensione finita)
Siano K un campo, $n \in \mathbb{N}$ e sia L il campo dei quozienti dell'anello dei polinomi $K[x_1, \ldots, x_n]$, cioè $L := K(x_1, \ldots, x_n)$.
Sia $\sigma \in Aut_K(L)$ tale che $\sigma(x_n) = x_1$ e, per ogni $i \in \underline{n-1}\rfloor$, $\sigma(x_i) = x_{i+1}$.
Allora $o(\sigma) = n$.
Poniamo

$$L[x, \sigma] := \left\{ \sum_{i=0}^{m} a_i x^i \mid m \in \mathbb{N}_0, a_i \in L \quad \forall\, i \in \underline{m}\rfloor \right\},$$

cioè sia $L[x, \sigma]$ l'insieme dei polinomi a coefficienti in L nell'indeterminata commutativa x. In $L[x, \sigma]$ definiamo l'addizione nel modo usuale, mentre la moltiplicazione viene definta imponendo che valga anche la seguente condizione:

$$\forall\, b \in L, \forall\, i \in \mathbb{N} \qquad x^i b = \sigma^i(b) x^i.$$

Con tali operazioni, $L[x, \sigma]$ risulta essere un anello non commutativo detto l'*anello sghembo dei polinomi su* L.
Vediamo com'è fatto il centro di $L[x, \sigma]$. Sia $f \in Z(L[x, \sigma])$ e siano $m \in \mathbb{N}_0$, $a_0, a_1, \ldots, a_n \in L$ tali che $f = \sum_{i=0}^{m} a_i x^i$. Allora, per ogni $k \in \mathbb{N}_0$ e $b \in L$, si ha

$$\begin{aligned} fbx^k = bx^k f \quad &\Leftrightarrow \quad \forall\, i \in \underline{m}\rfloor \qquad a_i x^i b x^k = b x^k a_i x^i \Leftrightarrow \\ &\Leftrightarrow \quad \forall\, i \in \underline{m}\rfloor \qquad a_i \sigma^i(b) x^i x^k = b \sigma^k(a_i) x^k x^i \Leftrightarrow \\ &\Leftrightarrow \quad \forall\, i \in \underline{m}\rfloor \qquad a_i \sigma^i(b) = b \sigma^k(a_i) \qquad (\triangle) \end{aligned}$$

In particolare, se $b = 1$, allora

$$\forall\, k \in \mathbb{N}_0, \forall\, i \in \underline{m}\rfloor \qquad a_i = \sigma^k(a_i) \qquad (\nabla)$$

e quindi i coefficienti di f devono essere fissati da tutte le potenze di σ.
Pertanto, se L' è il sottocampo di L costituito da tutti gli elementi di L che vengono fissati da σ, si ha che $a_i \in L'$ per ogni $i \in \underline{m}\rfloor$.
Inoltre da $(\triangle)$ e (∇) segue che

$$\forall\, i \in \underline{m}\rfloor, \forall\, b \in L \qquad a_i \sigma^i(b) = b a_i.$$

Allora, per ogni $i \in \underline{m}\rfloor$ tale che $a_i \neq 0$, vale:

$$\forall\, b \in L \qquad \sigma^i(b) = a_i^{-1} b a_i = b$$

e quindi $\sigma^i = id_L$, cioè $i \equiv 0 (\mathrm{mod}\ n)$.
Siano $r \in \underline{m}\rfloor \cup \{0\}$ e $b_0, b_1, \ldots, b_r \in L$ tali che

$$\{b_0, b_1, \ldots, b_r\} := \{a_i \mid i \in \underline{m}\rfloor \text{ e } a_i \neq 0\}.$$

Segue che

$$f = \sum_{\substack{i=0 \\ i \equiv 0 (\mathrm{mod}\ n)}}^{m} a_i x^i = \sum_{q=0}^{r} b_q (x^n)^q,$$

cioè $Z(L[x,\sigma]) \subseteq L'[x^n]$. In realtà vale anche l'altra inclusione in quanto, per ogni $m, q \in \mathbb{N}$ e $c \in L, b \in L'$, vale:

$$\begin{aligned} cx^m bx^{nq} &= c\sigma^m(b)x^m x^{nq} = cbx^m x^{nq} = bcx^{m+nq} = \\ &= b\sigma^{nq}(c)x^{nq}x^m = bx^{nq}cx^m. \end{aligned}$$

Dimostriamo, ora, che $L[x,\sigma]$ è un modulo libero sul proprio centro $L'[x^n]$ avente n^2 generatori.
Osserviamo innanzitutto che L è un'estensione di Galois di L' con gruppo di Galois $\langle\sigma\rangle$ e quindi la dimensione di L su L' è uguale all'ordine n del gruppo di Galois.
Siano $v_1, v_2, \ldots, v_n$ una base di L su L' e proviamo che il seguente insieme

$$\{v_i x^j \mid i \in \underline{n}\rfloor, j \in \underline{n-1}\rfloor \cup \{0\}\}$$

genera $L[x,\sigma]$ su $L'[x^n]$.
Sia $f \in L[x,\sigma]$ e siano $m \in \mathbb{N}_0$, $a_0, a_1, \ldots, a_m \in L$ tali che $f = \sum_{k=0}^{m} a_k x^k$.
Per ogni $k \in \underline{m}\rfloor \cup \{0\}$, siano $\alpha_{k1}, \ldots, \alpha_{kn} \in L'$ tali che $a_k = \sum_{i=1}^{n} \alpha_{ki} v_i$.
Segue che

$$\begin{aligned} f &= \sum_{k=0}^{m}\left(\sum_{i=1}^{n}\alpha_{ki}v_i\right)x^k = \sum_{\substack{k=0\\ k\equiv 0(\mathrm{mod}\ n)}}^{m}\left(\sum_{i=1}^{n}\alpha_{ki}v_i\right)x^k + \\ &+ \sum_{\substack{k=0\\ k\equiv 1(\mathrm{mod}\ n)}}^{m}\left(\sum_{i=1}^{n}\alpha_{ki}v_i\right)x^k + \ldots + \sum_{\substack{k=0\\ k\equiv (n-1)(\mathrm{mod}\ n)}}^{m}\left(\sum_{i=1}^{n}\alpha_{ki}v_i\right)x^k = \\ &= \sum_{i=1}^{n}\left(\sum_{\substack{k=0\\ k\equiv 0(\mathrm{mod}\ n)}}^{m}\alpha_{ki}v_i x^k\right) + \sum_{i=1}^{n}\left(\sum_{\substack{k=0\\ k\equiv 1(\mathrm{mod}\ n)}}^{m}\alpha_{ki}v_i x^k\right) + \ldots + \\ &+ \sum_{i=1}^{n}\left(\sum_{\substack{k=0\\ k\equiv (n-1)(\mathrm{mod}\ n)}}^{m}\alpha_{ki}v_i x^k\right) \end{aligned}$$

e quindi

$$\begin{aligned} f &= \sum_{i=1}^{n}\left(\sum_{\substack{k=0\\ k\equiv 0(\mathrm{mod}\ n)}}^{m}\alpha_{ki}x^k\right)v_i + \sum_{i=1}^{n}\left(\sum_{\substack{k=0\\ k\equiv 1(\mathrm{mod}\ n)}}^{m}\alpha_{ki}x^{k-1}\right)v_i x + \ldots + \\ &+ \sum_{i=1}^{n}\left(\sum_{\substack{k=0\\ k\equiv (n-1)(\mathrm{mod}\ n)}}^{m}\alpha_{ki}x^{k-n+1}\right)v_i x^{n-1}. \end{aligned}$$

Segue che $\{v_i x^j \mid i \in \underline{n}\rfloor, j \in \underline{n-1}\rfloor \cup \{0\}\}$ è un sistema di generatori per $L[x,\sigma]$ su $L'[x^n]$ e si dimostra che tali generatori sono anche linearmente indipendenti.

Quindi $L[x,\sigma]$ è un'algebra generata come modulo sul proprio centro da n^2 elementi, e per **(2.35)** il polinomio standard $S_{n^2+1}(x_1,\ldots,x_{n^2+1})$ è un'identità polinomiale (propria) per $L[x,\sigma]$, cioè $L[x,\sigma]$ è una PI-algebra. Inoltre $L[x,\sigma]$ è un dominio d'integrità non commutativo e quindi è un'algebra prima.
Dal Teorema di Posner segue che l'anello dei quozienti centrali $Q(L[x,\sigma])$ è un'algebra centrale semplice di dimensione finita sul suo centro F e che $F = Q(L'[x^n])$. In particolare si deduce che

$$dim_F Q(L[x,\sigma]) = n^2$$

e che $Q(L[x,\sigma])$ è un dominio d'integrità perché lo è $L[x,\sigma]$.
Pertanto $Q(L[x,\sigma])$ è un'algebra di divisione di dimensione n^2 sul suo centro che è un'estensione di K.

7.5 Lemma. *Siano K un campo, $n \in \mathbb{N}$, $Y := \left\{u_{ij}^{(k)} \,|\, ij \in \underline{n}\rfloor, k \in \mathbb{N}\right\}$ un insieme di indeterminate su K commutative e indipendenti e F il campo dei quozienti di $K\left[u_{ij}^{(k)}\right]$, cioè $F := K\left(u_{ij}^{(k)}\right)$. Allora $M_n(F)$ è generato da $K_n\langle U\rangle$ come spazio vettoriale su F.*

Dimostrazione. Sia $M := \{e_{ij} \,|\, i,j \in \underline{n}\rfloor\}$ l'insieme delle matrici elementari $n \times n$ su F. Allora

$$\forall\, k \in \mathbb{N} \qquad U^{(k)} = \sum_{i,j=1}^{n} u_{ij}^{(k)} e_{ij}.$$

Ordiniamo M lessicograficamente:

$$e_{11} < e_{12} < e_{13} < \ldots < e_{1n} < e_{21} < e_{22} < \ldots < e_{2n} < e_{31} < \ldots < e_{nn}$$

e, per ogni $k \in \underline{n^2}\rfloor$, dènotiamo con v_k la k-sima matrice della catena. Segue che, per ogni $k \in \mathbb{N}$ e $i \in \underline{n^2}\rfloor$, esiste $\alpha_{ki} \in Y$ tale che

$$\forall\, k \in \mathbb{N} \qquad U^{(k)} = \sum_{i=1}^{n^2} \alpha_{ki} v_i.$$

Allora, posti

$$u := \left(U^{(1)}\ U^{(2)} \ldots U^{(n^2)}\right)^T \qquad v := (v_1\ \ v_2 \ldots v_{n^2})^T,$$

esiste $A \in M_{n^2}(F)$ tale che $u = Av$. Dimostriamo che $det(A) \neq 0$.
Se $k \in \underline{n^2}\rfloor$, la k-sima riga di A è

$$\left(u_{11}^{(k)}\ \ u_{12}^{(k)} \ldots u_{1n}^{(k)}\ \ u_{21}^{(k)} \ldots u_{2n}^{(k)} u_{31}^{(k)} \ldots u_{n1}^{(k)} \ldots u_{nn}^{(k)}\right)$$

e quindi il $det(A)$ è un polinomio nelle variabili indipendenti $u_{ij}^{(k)}$.
Per ogni $k \in \underline{n^2}\rfloor$ e $i, j \in \underline{n}\rfloor$, sia $b_{ij}^{(k)} \in K$ e sia $\overline{A}$ la matrice ottenuta da A sostituendo $b_{ij}^{(k)}$ a $u_{ij}^{(k)}$. Se $det(A) = 0$, allora anche $det(\overline{A}) = 0$ e, per l'arbitrarietà di $b_{ij}^{(k)}$ in K, dovrebbe annullarsi il determinante di tutte le matrici $n^2 \times n^2$ su K. Ciò è impossibile e quindi $det(A) \neq 0$.
Pertanto esiste $A^{-1} \in M_{n^2}(F)$ tale che $v = A^{-1}u$ e così l'insieme di generatori $\{e_{ij} \mid i, j \in \underline{n}\rfloor\}$ di $M_n(F)$ è contenuto nell'F-sottospazio generato da $K_n\langle U\rangle$. Segue che tale sottospazio coincide proprio con $M_n(F)$, cioè $M_n(F)$ è generato da $K_n\langle U\rangle$ come spazio vettoriale su F.

□

7.6 Teorema. ***(Amitsur [3])***
Siano K un campo infinito e $n \in \mathbb{N}$. Allora $K_n\langle U\rangle$ è un dominio d'integrità.

Dimostrazione. Proviamo innanzitutto che $K_n\langle U\rangle$ è un anello primo.
Siano $\alpha, \beta \in K_n\langle U\rangle$ tali che $\alpha K_n\langle U\rangle \beta = 0$, cioè tali che

$$\forall\, r \in K_n\langle U\rangle \qquad \alpha r \beta = 0.$$

Poiché per **(7.5)** $M_n(F)$ è generato da $K_n\langle U\rangle$ come spazio vettoriale su F, $\alpha M_n(F)\beta = 0$. Ma $M_n(F)$ è un anello unitario semplice e quindi è primitivo. Da **(6.5)** segue che $M_n(F)$ è primo e, per **(6.2)**, si ha $\alpha = 0$ oppure $\beta = 0$. Allora, sempre per **(6.2)**, $K_n\langle U\rangle$ è primo.
Supponiamo, ora, che $K_n\langle U\rangle$ non sia un dominio d'integrità. Per **(6.3)**, esiste $r \in K_n\langle U\rangle$ tale che $r \neq 0$ e $r^2 = 0$. Ma, per **(7.2)**,

$$K_n\langle U\rangle \cong K\langle X\rangle / T(M_n(K))$$

e quindi esistono $m \in \mathbb{N}$ e $f(x_1, \ldots, x_m) \in K\langle X\rangle$ tale che $f \notin T(M_n(K))$ e $f^2 \in T(M_n(K))$.
In **(7.4)** abbiamo dimostrato che esiste un'algebra di divisione D che ha dimensione n^2 sul proprio centro Z. Inoltre Z è un'estensione di K e quindi, per **(6.9)**, D e $M_n(Z)$ sono PI-equivalenti.
Essendo K un campo infinito, anche $M_n(Z) \cong M_n(K) \bigotimes_K Z$ e $M_n(K)$ sono PI-equivalenti (cfr. **(3.2)**).
Segue che $f^2 \in T(D)$ ma $f \notin T(D)$ e quindi esistono $a_1, \ldots, a_m \in D$ tali che $f(a_1, \ldots, a_m) \neq 0$. Allora

$$0 = f^2(a_1, \ldots, a_m) = f(a_1, \ldots, a_m)\, f(a_1, \ldots, a_m)$$

e ciò è impossibile perché D è un'algebra di divisione.
Pertanto $K_n\langle U\rangle$ è un dominio d'integrità.

□

7.7 Proposizione. *Siano K un campo infinito e $n \in \mathbb{N}$. Allora l'algebra dei quozienti centrali di $K_n\langle U\rangle$ è un'algebra di divisione di dimensione n^2 sul suo centro.*

Dimostrazione. Da **(7.6)** segue che $K_n\langle U\rangle$ è un anello primo e da **(6.9)** che $K_n\langle U\rangle$ è un PI-anello. Allora, per il Teorema di Posner, $Q(K_n\langle U\rangle)$ è un'algebra semplice di dimensione finita sul suo centro F. Poiché per **(7.6)** $K_n\langle U\rangle$ è un dominio d'integrità, anche $Q(K_n\langle U\rangle)$ lo è e quindi $Q(K_n\langle U\rangle)$ è un'algebra di divisione di dimensione finita sul centro. Per **(4.7)**, esiste $m \in \mathbb{N}$ tale che $dim_F Q(K_n\langle U\rangle) = m^2$. Proviamo che $m = n$.
Da **(5.11)** segue che il polinomio di Capelli C_{n^2+1} è un'identità polinomiale per $M_n(K)$ e quindi per $K_n\langle U\rangle$. Allora, per il Teorema di Posner, C_{n^2+1} è identità polinomiale per $Q(K_n\langle U\rangle)$. Essendo $Q(K_n\langle U\rangle)$ un'algebra semplice di dimensione m^2 sul centro, da **(6.9)** segue che $Q(K_n\langle U\rangle)$ e $M_m(F)$ sono PI-equivalenti. Allora C_{n^2+1} è identità polinomiale anche per $M_m(F)$ e quindi, per **(5.12)**, $n^2+1 \geq m^2+1$, cioè $n \geq m$.
Sempre da **(5.11)** segue che C_{m^2+1} è un'identità polinomiale per $M_m(F)$ e quindi per $Q(K_n\langle U\rangle)$ essendo PI-equivalenti. Per il Teorema di Posner, C_{m^2+1} è identità polinomiale per $K_n\langle U\rangle$ e quindi per $M_n(K)$. Da **(5.12)** segue che $m^2+1 \geq n^2+1$, cioè $m \geq n$.
Pertanto $m = n$ e $Q(K_n\langle U\rangle)$ è un'algebra di divisione di dimensione n^2 sul centro.

□

La proposizione precedente ci fornisce un altro esempio, oltre a **(7.4)**, di costruzione di algebre di divisione di dimensione fissata sul proprio centro.

Vediamo, infine, un risultato dovuto a Procesi e riguardante l'anello delle matrici generiche 2×2:

7.8 Teorema. ***(Procesi [16])***
Siano U, V due matrici generiche 2×2. Allora il centro di $Q(K_2\langle U, V\rangle)$ è il campo delle funzioni razionali in 5 variabili $K(y_1, y_2, y_3, y_4, y_5)$, dove

$$y_1 := tr(U) \qquad y_2 := tr(V)$$

$$y_3 := det(U) \qquad y_4 := det(V)$$

$$y_5 := tr(UV)$$