PREFAZIONE

Il presente lavoro è una raccolta di appunti di un corso di dottorato di ricerca in Matematica tenuto dal secondo autore presso l'Università di Lecce nel periodo 20 ottobre-2 dicembre 2003.
Il corso ha avuto lo scopo di presentare dei risultati classici relativi alla teoria delle algebre soddisfacenti identità polinomiali. Si studiano, infatti, alcuni importanti teoremi di struttura quali il Teorema di Amitsur-Levitzki, il Teorema di Kaplansky e il Teorema di Posner.
Più in dettaglio, nel primo capitolo vengono dimostrati il Teorema della Densità di Jacobson e il Teorema di Wedderburn-Artin: sono due noti teoremi della teoria degli anelli semplici e primitivi ma sono di fondamentale importanza per poter sviluppare la teoria delle algebre con identità polinomiali.
Nel secondo capitolo vengono introdotti i concetti di algebra libera e di identità polinomiale per un'algebra. In particolare viene descritto un utile metodo di multilinearizzazione di polinomi.
Nel terzo capitolo si dà la dimostrazione del famoso Teorema di Amitsur-Levitzki alla base di numerosi risultati presentati nel seguito.
Nel quarto capitolo si studiano alcune proprietà dei sottocampi massimali al fine di dimostrare l'importante teorema di Kaplansky.
Il quinto capitolo ha per argomento i polinomi centrali e in esso si descrive anche un metodo per costruirli dovuto a Razmyslov.
Nel sesto capitolo si dà la dimostrazione di Rowen del Teorema di Posner e si studiano alcune applicazioni di tale teorema alle PI-algebre e ai T-ideali dell'algebra libera.
Infine nell'ultimo capitolo si dà la definizione di matrice generica e si presentano dei risultati riguardanti l'algebra delle matrici generiche. Inoltre si fornisce un esempio di algebra di divisione di dimensione finita.
La teoria svolta richiede come prerequisiti solo la conoscenza di alcune no-

zioni di base della teoria delle algebre e in particolare del prodotto tensoriale di algebre.

Claudia Nuccio
Onofrio Mario Di Vincenzo
Lecce, 10 giugno 2004

CAPITOLO 1

ANELLI SEMPLICI E PRIMITIVI

In questo primo capitolo vengono presentati due risultati classici sugli anelli semplici e primitivi: il Teorema della Densità di Jacobson e il Teorema di Wedderburn-Artin. Tali teoremi si riveleranno utili nel seguito per la dimostrazione di diversi risultati sugli anelli soddisfacenti identità polinomiali.

1.1 IL TEOREMA DELLA DENSITÀ DI JACOBSON

1.1 Definizione. Sia R un anello. Un R-modulo (sinistro) M si dice *irriducibile* (o *semplice*) se $RM \neq 0$ e ogni R-sottomodulo di M è banale. Un anello è *semplice* se $R^2 \neq 0$ e R non ha ideali bilateri propri.

Vale il seguente classico risultato:

1.2 Lemma. ***(Lemma di Schur)***
Siano M ed N degli R-moduli e sia $f : M \to N$ un omomorfismo non nullo di R-moduli. Valgono:

(1) Se M è irriducibile allora f è iniettiva;

(2) Se N è irriducibile allora f è suriettiva;

(3) Se M ed N sono irriducibili allora f è un isomorfismo.

1.3 Definizione. Siano R un anello e M un R-modulo (sinistro). L'insieme

$$\mathcal{A}nn_R(M) = \{r \mid r \in R, \forall m \in M \quad rm = 0\}$$

è un ideale bilatero di R detto l'*annullatore (sinistro)* di M.
Se $Ann_R(M) = \{0\}$, allora l'R-modulo M si dice *fedele*. Evidentemente ogni modulo fedele è non nullo.
Un anello R si dice *primitivo (sinistro)* se esiste un R-modulo (sinistro) fedele e semplice.

1.4 Osservazione. Siano R un anello, M un R-modulo (sinistro) e sia $D := End_R(M)$. Definiamo sul gruppo abeliano $(M, +)$ la seguente operazione esterna:

$$\forall\, y \in M, \beta \in D \qquad \beta \cdot y := \beta(y)$$

Allora M è un D-modulo sinistro. Indichiamo con $End_D(M)$ l'anello degli endomorfismi di M come D-modulo sinistro e consideriamo l'omomorfismo:

$$\varphi : R \to End_D(M), \qquad r \mapsto L_r$$

dove L_r è definito nel seguente modo:

$$\forall\, y \in M \qquad L_r(y) = ry.$$

Per ogni $r \in R$, se $L_r = 0$ allora $rM = 0$ e quindi $ker\varphi = Ann_R(M)$.
Pertanto M è fedele se e solo se φ è un monomorfismo.

1.5 Esempio. Sia V uno spazio vettoriale (anche di dimensione infinita) su un corpo D e sia $R := End_D(V)$. Allora R è un anello primitivo e V è l'R-modulo fedele irriducibile.
Infatti, se $u \in V - \{0\}$ e $v \in V$ allora esiste $f \in End_D(V)$ tale che $f(u) = v$.
Pertanto, per ogni elemento non nullo $u \in V$, si ha $Ru = V$ e quindi V non ha R-sottomoduli propri.
Inoltre, per ogni $\theta \in R$, $\theta(V) = 0$ se e solo se $\theta = 0$, cioè $Ann_R(V) = 0$.
Pertanto V è un R-modulo fedele.

Per i moduli irriducibili vale la seguente proprietà:

1.6 Proposizione. *Siano R un anello ed M un R-modulo irriducibile. Se $v \in M - \{0\}$ allora $Rv = M$ e M si dice modulo ciclico.*

Dimostrazione. Dalla semplicità di M segue $Rv = 0$ oppure $Rv = M$.
Supponiamo che $Rv = 0$. Allora, posto

$$N := \{x \mid x \in M,\ Rx = 0\},$$

risulta $N \neq 0$ e quindi, essendo N un sottomodulo di M, $N = M$, cioè $RM = 0$. Ma ciò è impossibile perché M è un R-modulo irriducibile e così $Rv \neq 0$. Pertanto $Rv = M$.

□

1.7 Osservazione. Se R è un anello unitario e M un R-modulo irriducibile, allora M è un R-modulo unitario.

Diamo, ora, la definizione di anello denso:

1.8 Definizione. Sia M uno spazio vettoriale (sinistro) su un corpo D e sia R un sottoanello di $End_D(M)$. R si dice *denso* in $End_D(M)$ se, per ogni $n \in \mathbb{N}$, per ogni sottoinsieme D-indipendente $\{z_1, \ldots, z_n\}$ di M e per ogni arbitrario sottoinsieme $\{y_1, \ldots, y_n\}$ di M, esiste $\vartheta \in R$ tale che, per ogni $i \in \underline{n}\rfloor$, vale $\vartheta z_i = y_i$.

In particolare, nel caso di dimensione finita, $End_D(M)$ è l'unico sottoanello denso in quanto vale la seguente:

1.9 Proposizione. *Siano M uno spazio vettoriale su un corpo D, $n \in \mathbb{N}$ tale che $dim_D M = n$ e R un sottoanello di $End_D(M)$. Se R è denso in $End_D(M)$ allora $R = End_D(M)$.*

Dimostrazione. Siano $\{v_1, \ldots, v_n\}$ una base di M su D e $f \in End_D(M)$. Siano inoltre $w_1, \ldots, w_n \in M$ tali che

$$\forall\, i \in \underline{n}\rfloor \qquad w_i = f(v_i).$$

Poiché R è denso in $End_D(M)$, esiste $\theta \in R$ tale che, per ogni $i \in \underline{n}\rfloor$, $\theta v_i = w_i$. Poichè θ e f coincidono sugli elementi della base, segue che $\theta = f$. Pertanto $End_D(M) \subseteq R$, cioè $End_D(M) = R$.

□

Enunciamo infine il seguente lemma:

1.10 Lemma. *Siano R un anello, V un R-modulo irriducibile e poniamo $D := End_R(V)$. Se W è un D-sottospazio di V di dimensione finita su D e $u \in V - W$, allora esiste $r \in R$ tale che $rW = 0$ e $ru \neq 0$.*

1.11 Teorema. ***(Teorema della densità di Jacobson [8])***
Siano R un anello primitivo, M un R-modulo fedele e irriducibile e poniamo $D := End_R(M)$. Allora R è isomorfo ad un sottoanello denso di $End_D(M)$.

Dimostrazione. Considerato l'omomorfismo

$$\varphi : R \rightarrow End_D(M), \qquad r \mapsto L_r,$$

dall'osservazione (**1.4**) e dall'irriducibilità di M, segue subito che $R \cong \varphi(R)$ e quindi resta solo da provare che $\varphi(R)$ è un sottoanello denso in $End_D(M)$. Siano $n \in \mathbb{N}$, $v_1, \ldots, v_n \in M$ elementi linearmente indipendenti su D e $w_1, \ldots, w_n \in M$. Posto, per ogni $i \in \underline{m}\rfloor$, $W_i := \langle v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n \rangle$, dalla lineare indipendenza di $v_1, \ldots, v_n$ segue subito che $v_i \notin W_i$. Per il lemma (**1.10**), esiste $r_i \in R$ tale che $r_i w_i = 0$ e $r_i v_i \neq 0$. Poiché $r_i v_i \in M$ e $r_i v_i \neq 0$, da (**1.6**) segue che

$$\forall\, i \in \underline{n}\rfloor \qquad R r_i v_i = M$$

e quindi esistono $t_1, \ldots, t_n \in R$ tali che

$$\forall\, i \in \underline{n}\rfloor \qquad t_i r_i v_i = w_i.$$

Posto $r := \sum_{i=1}^{n} t_i r_i \in R$ e osservato che

$$\forall\, i \neq j \qquad t_j r_j v_i \in t_j(r_j W_j) = t_j \cdot 0 = 0,$$

si ha

$$\forall\, i \in \underline{n}\rfloor \qquad r v_i = w_i.$$

Pertanto

$$\forall\, i \in \underline{n}\rfloor \qquad L_r(v_i) = r v_i = w_i.$$

e, poiché $L_r \in \varphi(R)$, $\varphi(R)$ è denso in $End_D(M)$.

□

E' noto che se F è un campo e V uno spazio vettoriale su F di dimensione finita $n \in \mathbb{N}$ allora $End_F(V) \cong M_n(F)$. Ciò però non vale se F è un corpo.

1.12 Definizione. Sia R un anello. Si dice *anello opposto* di R e si denota con R^{op} l'anello che ha R come sostegno, come addizione quella definita in R e la seguente moltiplicazione $\circ$:

$$\forall\, a, b \in R^{op} \qquad a \circ b := b \cdot a$$

dove $\cdot$ è il prodotto definito in R.
L'applicazione

$$\theta : R \to R^{op}, \qquad r \mapsto r$$

è un *anti-isomorfismo*, cioè è un isomorfismo di gruppi additivi tale che

$$\forall\, r_1, r_2 \in R \qquad \theta(r_1 r_2) = \theta(r_2)\theta(r_1)$$

1.13 Osservazione. Se D è un corpo allora anche D^{op} è un corpo.

1.14 Proposizione. *Siano D un corpo, V uno spazio vettoriale su D e $n \in \mathbb{N}$ tale che $dim_D V = n$. Allora $End_D(V) \cong M_n(D^{op})$.*

Possiamo enunciare, ora, il seguente corollario del Teorema della Densità di Jacobson:

1.15 Corollario. *Siano R un anello primitivo, M un R-modulo fedele e irriducibile e $D := End_R(M)$. Allora esiste $n \in \mathbb{N}$ tale che $R \cong M_n(D^{op})$ oppure, per ogni $n \in \mathbb{N}$, esistono un sottoanello S_n di R ed un epimorfismo φ_n da S_n su $M_n(D^{op})$.*

1.2 Il Teorema di Wedderburn-Artin

1.16 Definizione. Siano R un anello e M un R-modulo sinistro. Si dice che M è *Artiniano sinistro* se e solo se ogni insieme non vuoto di R-sottomoduli di M ha un elemento minimale.
Un anello R è *Artiniano a sinistra* se è un R-modulo Artiniano sinistro.

Analogamente si definiscono i moduli e gli anelli *Artiniani destri.*
Dalla definizione segue subito che un R-modulo M è Artiniano (sinistro) se e solo se soddisfa la *condizione delle catene discendenti (DCC)*, cioè se e solo se per ogni catena

$$A_1 \supseteq A_2 \supseteq A_3 \supseteq \ldots A_m \supseteq \ldots$$

di R-sottomoduli di M esiste $n \in \mathbb{N}$ tale che, per ogni $i \geq n$, $A_i = A_n$.

1.17 Osservazioni. Sia R un anello.

(1) Siano M un R-modulo ed N un R-sottomodulo di M. Allora M è Artiniano (sinistro) se e solo se N e M/N sono Artiniani (sinistri).

(2) Siano $k \in \mathbb{N}$ e $M_1, \ldots, M_k$ R-moduli. Allora la somma diretta

$$\bigoplus_{i=1}^{k} M_i$$

è Artiniana (sinistra) se e solo se, per ogni $i \in \underline{k}\rfloor$, M_i è Artiniano (sinistro).

1.18 Esempio. Siano D un corpo e $n \in \mathbb{N}$. Allora $M_n(D)$ è un anello Artiniano a destra e a sinistra ed è semplice e primitivo.
Dimostriamo dapprima che $M_n(D)$ è Artiniano a sinistra e a destra.
Per ogni $i, j \in \underline{n}\rfloor$, denotiamo con $e_{ij} \in M_n(D)$ la *matrice elementare* avente l'unità di D nella posizione (i,j) e 0 in tutte le altre. Tali matrici godono della seguente proprietà:

$$\forall i, j, p, q \in \underline{n}\rfloor \qquad e_{ij}e_{pq} = \delta_{jp}e_{iq}$$

dove δ_{jp} è il simbolo di Kronecker. Ne segue che, per ogni $i \in \underline{n}\rfloor$, l'insieme

$$L_i := M_n(D)e_{ii} = \{(a_{kj}) \in M_n(D) \,|\, \forall j \neq i \quad a_{kj} = 0\}$$

è un ideale sinistro minimale di $M_n(D)$ e quindi è un modulo su $M_n(D)$ irriducibile. Pertanto L_i è Artiniano sinistro e, per **(1.17(1))**, anche $M_n(D)$ è Artiniano sinistro.
Inoltre si dimostra che, per ogni $i \in \underline{n}\rfloor$, L_i è fedele e quindi $M_n(D)$ è primitivo sinistro.

Procedendo in modo analogo si dimostra che, per ogni $i \in \underline{n}\rfloor$, l'insieme $W_i := e_{ii}M_n(D)$ è un ideale destro minimale fedele e che $M_n(D)$ è Artiniano destro e primitivo destro.
Dimostriamo infine che $M_n(D)$ è semplice. Sia I un ideale bilatero non nullo di $M_n(D)$ e sia $x \in I - \{0\}$. Allora, per ogni $i, j \in \underline{n}\rfloor$, esistono $a_{ij} \in D$ tali che $x = \sum_{i,j=1}^{n} a_{ij}e_{ij}$. Poiché I è bilatero, per ogni $p, q, i_0, j_0 \in \underline{n}\rfloor$, $e_{p\,i_0}\, x\, e_{j_0\,q} \in I$. Ma

$$e_{p\,i_0}\, x\, e_{j_0\,q} = \sum_{i,j=1}^{n} a_{ij}e_{p\,i_0}e_{ij}e_{j_0\,q} = a_{i_0\,j_0}e_{pq}$$

e quindi, per ogni $p, q \in \underline{n}\rfloor$, $e_{pq} \in I$, cioè $M_n(D) \subseteq I$. Pertanto $I = M_n(D)$.

1.19 Teorema. ***(Teorema di Wedderburn-Artin)***
Sia R un anello. Sono equivalenti:

(i) R è semplice Artiniano a sinistra;

(ii) R è primitivo Artiniano a sinistra;

(iii) Esistono un corpo D ed uno spazio vettoriale V su D di dimensione finita $n \in \mathbb{N}$ tali che $R \cong End_D(V)$;

(iv) Esistono $n \in \mathbb{N}$ ed un corpo Δ tali che $R \cong M_n(\Delta)$.

Dimostrazione. **"(i)⇒(ii)"** Poichè R è Artiniano a sinistra, l'insieme di tutti gli ideali sinistri non nulli di R contiene un ideale sinistro minimale L. Segue che L è irriducibile come R-modulo in quanto gli R-sottomoduli di un ideale sono tutti e soli gli ideali sinistri di R contenuti nell'ideale stesso.
Essendo R un anello semplice e $Ann_R(L)$ un ideale bilatero, si ha che $Ann_R(L) = 0$ oppure $Ann_R(L) = R$. Se fosse $Ann_R(L) = R$ allora $RL = 0$ e quindi, posto

$$I := Ann_R(R) = \{x \,|\, x \in R,\ Rx = 0\},$$

si avrebbe $I \neq 0$. Ma I è un ideale bilatero di R e così, sempre per la semplicità di R, $I = 0$ oppure $I = R$. Poiché $I \neq 0$ si ha $I = R$ da cui segue $R^2 = 0$. Ciò è impossibile in quanto R è semplice e quindi $Ann_R(L) = 0$. Pertanto L è un R-modulo fedele irriducibile e perciò R è un anello primitivo.
"(ii)⇒(iii)" Poichè R è primitivo, esiste un R-modulo V fedele e irriducibile e sia $D := End_R(V)$. Proviamo che $dim_D V$ è finita.
Supponiamo che tale dimensione sia infinita e quindi che, per ogni $n \in \mathbb{N}$, esistano $v_1, \dots, v_n \in V$ linearmente indipendenti su D. Per il Teorema della Densità di Jacobson, R è isomorfo ad un sottoanello denso di $End_D(V)$ e così, posto

$$L_n := \{x \,|\, x \in R,\ xv_1 = xv_2 = \ldots = xv_n = 0\},$$

si ha $L_n \neq \emptyset$. Inoltre L_n è un ideale sinistro di R e risulta

$$L_1 \supset L_2 \supset \ldots \supset L_n \supset L_{n+1} \supset \ldots$$

con $L_n \neq L_{n+1}$ per ogni $n \in \mathbb{N}$. Infatti, se $v_1, \ldots, v_n, v_{n+1} \in V$ sono linearmente indipendenti, dalla densità di R in $End_D(V)$ segue che esiste $x \in R$ tale che $xv_1 = \ldots = xv_n = 0$ e $xv_{n+1} \neq 0$.
Pertanto R non è Artiniano sinistro e ciò contraddice l'ipotesi.
Segue che $dim_D V$ è finita e quindi, per **(1.9)**, $R \cong End_D(V)$.
"(iii)⇒(iv)" Da **(1.14)** segue che $End_D(V) \cong M_n(D^{op})$ e quindi, per avere la tesi, basta porre $\Delta := D^{op}$.
"(iv)⇒(i)" Segue da **(1.18)**.

□

Vediamo, ora, come sono fatti i moduli irriducibili su anelli di matrici.

1.20 Proposizione. *Siano D un corpo, $n \in \mathbb{N}$ e $R := M_n(D)$. Se V è un R-modulo irriducibile allora esiste $i \in \underline{n}\rfloor$ tale che $V \cong Re_{ii}$.*

Dimostrazione. Poichè R è unitario, V è un R-modulo unitario irriducibile. Se $v \in V - \{0\}$ allora esiste $i \in \underline{n}\rfloor$ tale che $e_{ii}v \in V - \{0\}$. Per **(1.6)**, $Re_{ii}v = V$ e quindi il seguente omomorfismo di R-moduli

$$\varphi : Re_{ii} \to V, \qquad x \mapsto xv$$

è non nullo. Inoltre, dalla dimostrazione di **(1.18)** segue che Re_{ii} è un R-modulo irriducibile e così, per il lemma di Schur, φ è un isomorfismo. Pertanto $V \cong Re_{ii}$.

□

Al fine di caratterizzare i moduli irriducibili di un qualsiasi anello, introduciamo la seguente definizione:

1.21 Definizione. Siano R anello ed L un ideale sinistro di R. L è *regolare* in R se esiste $e \in R$ tale che, per ogni $x \in R$, $x - xe \in L$.
Se R è unitario e 1_R è la sua unità basta porre $e := 1_R$.

1.22 Proposizione. *Siano R un anello e M un R-modulo. Allora M è irriducibile se e solo se esiste un ideale sinistro L massimale e regolare in R tale che $M \cong R/L$.*

Dimostrazione. Se M è irriducibile allora $M \neq 0$ e sia $v \in M - \{0\}$. Per **(1.6)**, $Rv = M$ e quindi il seguente omomorfismo

$$f : R \to M, \qquad x \mapsto xv$$

è un epimorfismo non nullo. Posto $L := ker\, f$, per il teorema di omomorfismo per i moduli, si ha che L è un ideale sinistro di R e $R/L \cong M$.
Inoltre L è massimale. Infatti, sia A un ideale sinistro di R tale che $L \subseteq A$.

Allora, per il teorema di corrispondenza per anelli, A/L è un ideale sinistro di R/L e, essendo $R/L \cong M$, dall'irriducibilità di M segue che $A = L$ oppure $A = R$.
Dimostriamo, infine, che L è regolare. Poiché f è suriettiva, esiste $e \in R$ tale che $f(e) = v$, cioè $ev = v$. Allora, per ogni $x \in R$, $xev = xv$ e così $x - xe \in ker\, f = L$. Segue che L è regolare.
Supponiamo, ora, che esista un ideale sinistro L massimale e regolare in R tale che $M \cong R/L$. Dalla regolarità di L si deduce che $RM \neq 0$ e così dalla massimalità di L segue subito che M è irriducibile.

□

1.23 Osservazione. Siano R un anello e M un R-modulo irriducibile.
Per (**1.22**), esiste un ideale sinistro L massimale e regolare in R tale che $M \cong R/L$. Pertanto

$$\begin{aligned} Ann_R(M) &= Ann_R(R/L) = \{x \mid x \in R,\, r \cdot R/L = 0\} \\ &= \{x \mid x \in R,\, xR \subseteq L\} \end{aligned}$$

Osserviamo che $Ann_R(R/L)$ è un ideale bilatero di R contenuto in L. Infatti, poiché L è regolare, esiste $e \in R$ tale che, per ogni $x \in R$, $x - xe \in L$ e quindi, se $a \in Ann_R(R/L)$, $a - ae \in L$. Ma $ae \in aR \subseteq L$ e quindi $a \in L$, cioè $Ann_R(R/L) \subseteq L$. Inoltre si dimostra che $Ann_R(R/L)$ è il più grande ideale di R contenuto in L.

CAPITOLO 2

ALGEBRE SODDISFACENTI IDENTITÀ POLINOMIALI

In questo capitolo si introducono i concetti di algebra libera e di identità polinomiale per un'algebra. Inoltre si danno diverse definizioni e caratterizzazioni riguardanti i polinomi di un'algebra libera e si descrive un metodo di multilinearizzazione.

D'ora in poi C denoterà sempre un anello commutativo unitario.

2.1 Definizione. Sia X un insieme. Un monoide M si dice *libero su X* se

(1) $X \subseteq M$

(2) per ogni monoide M' e per ogni applicazione $\varphi : X \to M'$ esiste un unico omomorfismo (di monoidi) $\widetilde{\varphi} : M \to M'$ tale che $\widetilde{\varphi}_{|X} = \varphi$.

Si dimostra che se X è un insieme allora, a meno di isomorfismi, esiste un unico monoide libero su X e lo si denota con X^*. Inoltre si dimostra che se $w \in X^*$ allora esiste un unico $n \in \mathbb{N}_0$ e un'unica n-upla $(x_1, x_2 \ldots, x_n) \in X^n$ tale che $w = x_1 x_2 \ldots x_n$.
Usando la terminologia classica, X si dice *alfabeto*, i suoi elementi sono le *lettere* e gli elementi di X^* le *parole* su X. L'elemento neutro di X^* si dice *parola vuota* e si indica con 1.
Consideriamo l'applicazione:

$$\varphi : X \to \mathbb{N}_0, \qquad x \mapsto 1.$$

Allora, per **(2.1)**, esiste un unico omomorfismo di monoidi

$$|\ \ | : X^* \to (\mathbb{N}_0, +), \qquad x \mapsto |x|$$

tale che, per ogni $x \in X, |x| = 1$. Se $w \in X^*$, chiamiamo $|w|$ *lunghezza* di w.
Se $x_1, \dots, x_k \in X$ e $w := x_1 \dots x_k$ allora:

$$|w| = |x_1 \dots x_k| = |x_1| + \dots + |x_k| = \underbrace{1 + \dots + 1}_{k-volte} = k.$$

Posto, per ogni $n \in \mathbb{N}$, $X^{(n)} := \{w \in X^* \mid |w| = n\}$ si ha $X^0 = \{1\}$, $X^1 = X$ e $X^* = \dot{\bigcup}_{n \in \mathbb{N}_0} X^{(n)}$.

2.2 Definizione. Sia $X = \{x_1, x_2, \dots\}$ un insieme numerabile. Allora, per ogni $i \in \mathbb{N}$ e per ogni $w \in X^*$, indichiamo con $|w|_{x_i}$ il numero di volte in cui la lettera x_i compare nell'espressione di w e diciamo che $|w|_{x_i}$ è la *lunghezza di w relativa ad x_i*. Ovviamente risulta che $|w| = \sum_{i \in \mathbb{N}} |w|_{x_i}$.

2.3 Definizione. Sia X un insieme e A una C-algebra unitaria. A si dice *algebra libera* su X se:

(1) $X \subseteq A$

(2) per ogni C-algebra B e per ogni applicazione φ da X in B esiste un unico omomorfismo (di C-algebre) $\widetilde{\varphi}$ da A in B tale che $\widetilde{\varphi}_{|X} = \varphi$.

Si dimostra che se X è un insieme allora, a meno di isomorfismi, esiste un'unica C-algebra libera su X e la si denota con $C\langle X \rangle$.
In particolare, d'ora in poi l'insieme X sarà sempre numerabile e se $n \in \mathbb{N}$ e $X = \{x_1, x_2, \dots, x_n\}$, allora $C\langle X \rangle$ si indicherà col simbolo $C\langle x_1, x_2, \dots, x_n \rangle$.
Gli elementi di $C\langle X \rangle$ si dicono usualmente *polinomi(non commutativi) in X su C*. L'espressione "non commutativi" sta ad indicare la differenza con i classici polinomi in X su C che dovremmo chiamare "polinomi commutativi in X su C".
Si dimostra che l'algebra semigruppale $C[X^*]$ di X^* su C è un'algebra libera su X e quindi ogni elemento $P \in C\langle X \rangle$ è combinazione lineare, a coefficienti in C, di elementi di X^*, cioè di parole su X.

2.4 Definizione. Sia $X = \{x_1, x_2, \dots\}$ un insieme numerabile e sia

$$P = \sum_{u \in X^*} (P, u)u \in C\langle X \rangle.$$

Se $(P, u) \neq 0$, allora $(P, u)u$ si dice un *monomio* di P e (P, u) un *coefficiente* di P.
Se $P \neq 0$ chiamiamo *grado* di P il seguente numero intero:

$$deg(P) := max\{\, |u| \mid u \in X^*, (P, u) \neq 0\}$$

e poniamo $deg(0) := -\infty$.
Definiamo inoltre, per ogni $i \in \mathbb{N}$,

$$deg^i(P) := max\{\, |u|_{x_i} \mid u \in X^*, (P,u) \neq 0\}$$

$$deg_i(P) := min\{\, |u|_{x_i} \mid u \in X^*, (P,u) \neq 0\}.$$

Segue che, per ogni $u \in X^*$ e per ogni $i \in \mathbb{N}$, $deg(u) = |u|$ e

$$deg_i(u) = |u|_{x_i} = deg^i(u).$$

2.5 Definizione. Siano $f \in C\langle X\rangle$ e R un'algebra su C. Denotiamo con $f(R)$ l'insieme delle immagini di f tramite gli omomorfismi da $C\langle X\rangle$ in R (come C-algebre), cioè:

$$f(R) := \{\psi(f) \mid \psi \in Hom_C(C\langle X\rangle, R)\}.$$

Siano $d \in \mathbb{N}$, $f = f(x_1, \dots, x_d) \in C\langle X\rangle$ e R una C-algebra. Consideriamo $\psi \in Hom_C(C\langle X\rangle, R)$ e sia, per ogni $i \in \mathbb{N}$, $r_i \in R$ tale che $\psi(x_i) = r_i$. Allora poniamo $f(r_1, \dots, r_d) := \psi(f)$.
Ovviamente $f(R) = \{f(r_1, \dots, r_d) \mid \forall i \in \underline{d}\rfloor \quad r_i \in R\}$ essendo $C\langle X\rangle$ algebra libera su X. In particolare, se $R = C\langle X\rangle$, allora

$$f(C\langle X\rangle) = \{f(f_1, \dots, f_d) \mid \forall i \in \underline{d}\rfloor \quad f_i \in C\langle X\rangle\}$$

e, se $g \in C\langle X\rangle$, per ogni $i \in \underline{d}\rfloor$, definiamo

$$f(x_i \mapsto g) := f(x_1, \dots, x_{i-1}, g, x_{i+1}, \dots, x_d) \in f(C\langle X\rangle).$$

2.6 Definizione. Siano A una C-algebra, $f \in C\langle X\rangle$ e $m \in \mathbb{N}$ tale che $f = f(x_1, \dots, x_m)$. Si dice che f è un'*identità polinomiale* per l'algebra A se

$$\forall\, a_1, \dots, a_m \in A \qquad f(a_1, \dots, a_m) = 0.$$

Inoltre, f è un'identità polinomiale *propria* se esiste un coefficiente $\alpha \in C$ di f tale che $\alpha A \neq 0$.
Si dice che A è *un'algebra con identità polinomiale*, o, più brevemente, una *PI-algebra* se e solo se esiste $f \in C\langle X\rangle$ tale che f è un'identità polinomiale per A e uno dei monomi di f di grado più alto ha coefficiente 1.
Analogamente, si dice *PI-anello* un anello che è una PI-algebra su $\mathbb{Z}$.

2.7 Osservazione. La classe delle algebre che soddisfano identità polinomiali è un'estensione della classe delle algebre commutative, infatti ogni algebra commutativa soddisfa l'identità

$$f = [\,x_1, x_2\,] = x_1x_2 - x_2x_1.$$

2.8 Osservazione. Siano $f \in C\langle X\rangle$ e R una C-algebra. Allora f è un'identità di R se e solo se $f \in \bigcap ker\psi$ al variare di $\psi \in Hom_C(C\langle X\rangle, R)$.

2.9 Definizione. Siano $m \in \mathbb{N}$ e $f(x_1, \dots, x_m) \in C\langle X\rangle$. Se $i \in \underline{m}\rfloor$, si dice che f è *mescolato in* x_i se, per ogni $u \in X^*$ tale che $(f, u) \neq 0$, $|u|_{x_i} > 0$. f si dice *polinomio mescolato* nelle lettere $x_{i_1}, \dots, x_{i_k}$ se, per ogni $i \in \underline{k}\rfloor$, f è mescolato in x_{i_k}.

2.10 Proposizione. *Ogni polinomio è somma finita di polinomi mescolati.*

2.11 Proposizione. *Siano $f \in C\langle X\rangle$ e A una C-algebra. f è identità polinomiale per A se e solo se ogni sua componente mescolata è identità polinomiale per A.*

Dimostrazione. Sia $m \in \mathbb{N}$ tale che $f = f(x_1, \dots, x_m)$ e, per ogni $S \in \mathcal{P} := \mathcal{P}(\{x_1, \dots, x_m\})$, denotiamo con f_S la componente di f mescolata nelle lettere appartenenti ad S. Allora

$$f = \sum_{S \in P} f_S.$$

$\Rightarrow$) Sia $S \in \mathcal{P}$ tale che se $T \in \mathcal{P}$ e $T \subsetneq S$ allora $f_T = 0$. Si consideri l'applicazione $\sigma : X \to A$ così definita:

$$\forall i \in \mathbb{N} \qquad \sigma(x_i) := \begin{cases} 0 & x_i \notin S \\ a_i & x_i \in S \end{cases}$$

con $a_i \in A$. Sia $\widetilde{\sigma}$ l'unico omomorfismo di C-algebre da $C\langle X\rangle$ in A tale che $\widetilde{\sigma}_{|X} = \sigma$. Allora, se $T \in \mathcal{P}$ e $T \nsubseteq S$, si ha $\widetilde{\sigma}(f_T) = 0$ e quindi, per **(2.8)**,

$$\begin{aligned} 0 &= \widetilde{\sigma}(f) = \widetilde{\sigma}\left(\sum_{T \in \mathcal{P}} f_T\right) = \sum_{T \in \mathcal{P}} \widetilde{\sigma}(f_T) = \\ &= \sum_{T \subseteq S} \widetilde{\sigma}(f_T) = \widetilde{\sigma}(f_S). \end{aligned}$$

Dall'arbitrarietà di σ segue che

$$f_S \in \bigcap ker\psi \qquad \text{al variare di } \psi \text{ in } Hom_C(C\langle X\rangle, A)$$

e quindi, per **(2.8)**, f_S è un'identità polinomiale per A.
Procedendo in modo analogo per ogni $S \in \mathcal{P}$, si dimostra la tesi in un numero finito di passi.

$\Leftarrow$) Banale.

□

2.12 Definizione. Sia $t \in \mathbb{N}$ e sia $f(x_1, \dots, x_t) \in C\langle X\rangle$. f si dice *omogeneo* in x_i se $deg_i(f) = deg^i(f)$.
f è *multiomogeneo* se, per ogni $i \in \underline{t}\rfloor$, f è omogeneo in x_i. Più precisamente,

se $n_1, \ldots, n_t \in \mathbb{N}$, si dice che f è multiomogeneo di *multigrado* $(n_1, \ldots, n_t)$ se, per ogni $i \in \underline{t}\rfloor$, $deg_i(f) = n_i = deg^i(f)$.
Per ogni $i \in \underline{t}\rfloor$, f è *lineare* in x_i se $deg_i(f) = deg^i(f) = 1$ ed è *multilineare* se è lineare in ogni lettera x_i.

Quindi un polinomio multilineare è un polinomio multiomogeneo di multigrado $(1, 1, \ldots, 1)$.

2.13 Osservazione. I polinomi multilineari sono collegati in modo naturale con i gruppi simmetrici. Infatti, se $t \in \mathbb{N}$ e se $f \in C\langle X\rangle$ è un polinomio multilineare di grado t, allora, per ogni $\pi \in \mathcal{S}_t$, esiste $\alpha_\pi \in C$ tale che :

$$f = f(x_1, \ldots, x_t) = \sum_{\pi \in \mathcal{S}_t} \alpha_\pi x_{\pi(1)} \ldots x_{\pi(t)}.$$

2.14 Definizione. Se $I \subseteq C\langle X\rangle$, I si dice *T-ideale* se è un ideale bilatero di $C\langle X\rangle$ ed è invariante sotto l'azione di $End_C(C\langle X\rangle)$, cioè

$$\forall\, \varphi \in End_C(C\langle X\rangle) \qquad \varphi(I) \subseteq I.$$

2.15 Proposizione. *Sia A una C-algebra e sia*

$$T(A) := \{f \in C\langle X\rangle \mid f \text{ è identità polinomiale per } A\}.$$

Allora $T(A)$ è un T-ideale di $C\langle X\rangle$.

Dimostrazione. Siano $\pi \in End_C(C\langle X\rangle)$ e $f \in T(A)$. Allora, per ogni $\sigma \in Hom_C(C\langle X\rangle, A)$, da **(2.8)** segue che:

$$\sigma(\pi(f)) = (\sigma\pi)(f) = 0$$

e quindi $\pi(f) \in \bigcap ker\sigma$, al variare di σ in $Hom_C(C\langle X\rangle, A)$. Sempre per **(2.8)** si ha che $\pi(f) \in T(A)$.

□

Vale anche il viceversa.

2.16 Proposizione. *Se I è un ideale bilatero in $C\langle X\rangle$, allora $T(C\langle X\rangle/I)$ è il più grande T-ideale di $C\langle X\rangle$ contenuto in I.*

Dimostrazione. Poniamo $\overline{R} := C\langle X\rangle/I$. Ovviamente $T(\overline{R}) \subseteq I$. Infatti, sia $f \in T(\overline{R})$ e sia $k \in \mathbb{N}$ tale che $f = f(x_1, \ldots, x_k)$. Allora, per ogni $g_1, \ldots, g_k \in C\langle X\rangle$, vale:

$$0 = f(g_1 + I, \ldots, g_k + I) = f(g_1, \ldots, g_k) + I$$

e quindi $f(g_1, \ldots, g_k) \in I$. In particolare, se poniamo $g_i := x_i$ per ogni $i \in \underline{k}\rfloor$, si ha $f(x_1, \ldots, x_k) \in I$.

Quindi, basta dimostrare che se T un è un T-ideale in $C\langle X\rangle$ contenuto in I allora si ha anche $T \subseteq T(\overline{R})$.
Siano $k \in \mathbb{N}$, $p(x_1, \ldots, x_k) \in T$ e $r_1, \ldots, r_k \in \overline{R}$. Siano, inoltre, $q_1, \ldots, q_k$ polinomi di $C\langle X\rangle$ tali che, per ogni $i \in \underline{k}\rfloor$, $r_i = q_i + I$. Allora

$$\begin{aligned} p(r_1, \ldots, r_k) &= p(q_1 + I, \ldots, q_k + I) = \\ &= p(q_1, \ldots, q_k) + I = 0 \end{aligned}$$

perché $p \in T \subseteq I$ e, per ipotesi, T è invariante per endomorfismi in $C\langle X\rangle$. Pertanto $p \in T(\overline{R})$ e quindi $T \subseteq T(\overline{R})$.

□

2.17 Definizione. Siano R e $\overline{R}$ due C-algebre. R e $\overline{R}$ sono *PI-equivalenti* se $T(R) = T(\overline{R})$.

2.18 Teorema. *Se F è un campo infinito e A è una F-algebra, allora $T(A)$ è multiomogeneo.*

Per la dimostrazione di tale teorema si sfrutta la seguente proposizione:

2.19 Proposizione. ***(Argomento di Vandermonde)***
Sia V uno C-modulo tale che

$$\forall\, \alpha \in C, \forall\, v \in V \qquad \alpha v = 0 \Rightarrow \alpha = 0 \text{ o } v = 0.$$

Siano $n \in \mathbb{N}, v_0, v_1, \ldots, v_n \in V$ e $t_0, t_1, \ldots, t_n \in C$ $n+1$ elementi distinti tali che

$$\forall\, i \in \underline{n}\rfloor \cup \{0\} \qquad v_0 + t_i v_1 + \ldots t_i^n v_n = 0.$$

Allora $v_i = 0$ per ogni $i \in \underline{n}\rfloor \cup \{0\}$.

Dimostrazione. Osserviamo innanzitutto che C è un dominio d'integrità. Infatti siano $\alpha, \beta \in C$ tali che $\alpha\beta = 0$ e sia $\beta \neq 0$. Allora

$$\forall\, v \in V \qquad \alpha\beta v = 0.$$

In particolare, se $v \in V - \{0\}$, $\beta v \neq 0$ e quindi $\alpha(\beta v) = 0$ implica che $\alpha = 0$. Posti

$$\underline{v} := (v_0 \quad v_1 \ldots v_n)^T, \qquad \underline{0} := (0 \quad 0 \ldots 0)^T$$

$$\forall\, i,j \in \underline{n+1}\rfloor \qquad \alpha_{ij} := t_{i-1}^{j-1}, \qquad A := (\alpha_{ij})_{i,j=1,\ldots,n+1}$$

dalle ipotesi segue che $A\underline{v} = \underline{0}$. Poiché A è una matrice di Vandermonde, si ha

$$det(A) = \prod_{i>j} (t_i - t_j)$$

e quindi $det(A) \neq 0$ perché C è un dominio d'integrità e $t_0, t_1, \ldots, t_n$ sono elementi a due a due distinti.

Per ogni $i, j \in \underline{n+1}|$ indichiamo con A_{ij} la matrice $n \times n$ ottenuta da A eliminando la i-esima riga e la j-esima colonna e poniamo

$$\beta_{ij} := (-1)^{i+j} det(A_{ij})$$

Se $B := (\beta_{ij})_{i,j=1,\dots,n+1}$ allora $BA = det(A)I_{n+1}$, dove I_{n+1} è la matrice identità di $M_{n+1}(C)$. Pertanto, moltiplicando ambo i membri di $A\underline{v} = \underline{0}$ per B, si ottiene:

$$\underline{0} = B\underline{0} = B(A\underline{v}) = (BA)\underline{v} = det(A)I_{n+1}\,\underline{v}$$

Segue

$$\forall\, i \in \underline{n}| \cup \{0\} \qquad det(A)v_i = 0$$

ed essendo $det(A) \neq 0$, si ha che

$$\forall\, i \in \underline{n}| \cup \{0\} \qquad v_i = 0.$$

□

Dimostrazione del teorema (2.18).

Sia $f \in T(A)$. Per **(2.11)** possiamo supporre, senza perdere di generalità, che f sia mescolato.

Sia $m \in \mathbb{N}$ tale che $f = f(x_1, \dots, x_m)$ e sia $n := deg^1(f)$. Per ogni $i \in \underline{n}|$, denotiamo con f_i la somma dei monomi di f di grado i in x_1. Allora

$$f(x_1, \dots, x_m) = \sum_{i=0}^{n} f_i(x_1, \dots, x_m).$$

Poiché f è un'identità polinomiale,

$$\forall\, a_1, \dots, a_m \in A, \forall\, t \in C \qquad f(ta_1, a_2, \dots, a_m) = 0$$

e quindi

$$\begin{aligned} 0 &= f(ta_1, a_2, \dots, a_m) = \sum_{i=0}^{n} f_i(ta_1, a_2, \dots, a_m) = \\ &= \sum_{i=0}^{n} t^i f_i(a_1, a_2, \dots, a_m) \end{aligned}$$

Dall'arbitrarietà di $t \in C$ e da **(2.19)** segue che

$$\forall i \in \underline{n}| \cup \{0\} \qquad f_i(a_1, a_2, \dots, a_m) = 0.$$

Iterando il procedimento per ogni $j \in \underline{m}| - \{1\}$ si ha la tesi.

□

Il concetto di polinomio multilineare svolge un ruolo molto importante nella teoria delle PI-algebre. Per tale motivo introduciamo, ora, un metodo di multilinearizzazione che, applicato ad un qualsiasi polinomio mescolato, permette di ottenerne un altro multilineare.

2.20 Definizione. Siano A una C-algebra, $m \in \mathbb{N}$ e $f(x_1, \ldots, x_m) \in C\langle X \rangle$ un'identità polinomiale per A mescolata. Si definisce *altezza* di f la seguente quantità:

$$ht(f) := deg(f) - m \geq 0.$$

2.21 Proposizione. *Sia $f \in C\langle X \rangle$. f è un polinomio multilineare se e solo se $ht(f) = 0$.*

2.22 Definizione. Siano $m \in \mathbb{N}$ e $f(x_1, \ldots, x_m) \in C\langle X \rangle$. Per ogni $i \in \underline{m}\rfloor$ e $k \in \mathbb{N} - \underline{m}\rfloor$ definiamo l'*operatore differenza* $\Delta_{i,k}$:

$$\Delta_{i,k}(f) := f(x_i \mapsto x_i + x_k) - f(x_i \mapsto x_k) - f.$$

2.23 Esempio. Sia $f(x_1, x_2) := x_1^2 x_2 \in \mathbb{Z}\langle X \rangle$. Allora
$\Delta_{1,3}(f) = (x_1 + x_3)^2 x_2 - x_1^2 x_2 - x_3^2 x_2 = x_1 x_3 x_2 + x_3 x_1 x_2$
$\Delta_{2,3}(f) = x_1^2(x_2 + x_3) - x_1^2 x_3 - x_1^2 x_2 = 0$

Il metodo di multilinearizzazione consiste nell'applicare l'operatore differenza ad un dato polinomio f un opportuno numero di volte. Infatti si dimostra che in tal modo si ottiene proprio un polinomio multilineare di grado minore o uguale a $deg(f)$.

2.24 Proposizione. *Siano $m \in \mathbb{N}$, $f(x_1, \ldots, x_m) \in C\langle X \rangle$ un polinomio mescolato, $i \in \underline{m}\rfloor$ e supponiamo che $deg^i(f) > 1$. Se $j \in \mathbb{N} - \underline{m}\rfloor$, posto $g(x_1, \ldots, x_j) := \Delta_{i,j}(f)$ valgono:*
(1) $deg^i(g) = deg^i(f) - 1$
(2) Tutti i coefficienti di g sono coefficienti di f.
(3) Se $deg^i(f) = deg_i(f) =: u$, allora $g(x_j \mapsto x_i) = (2^u - 2)f$

2.25 Proposizione. *Siano A una C-algebra, $m \in \mathbb{N}$ e $f(x_1, \ldots, x_m) \in C\langle X \rangle$ un'identià multilineare per A. Allora, per ogni $i \in \underline{m}\rfloor$ e $k \in \mathbb{N} - \underline{m}\rfloor$, valgono:*
(1)$\Delta_{i,k}(f) \in T(A)$;
(2)$deg(\Delta_{i,k}(f)) \leq deg(f)$;
(3)$ht(\Delta_{i,k}(f)) \leq ht(f)$.

2.26 Proposizione. *Siano A una C-algebra e $d \in \mathbb{N}$. Se A soddisfa un'identità polinomiale propria di grado d allora A soddisfa un'identità polinomiale multilineare propria di grado minore o uguale a d.*

Dimostrazione. Sia $m \in \mathbb{N}$ e sia $f(x_1, \ldots, x_m) \in C\langle X \rangle$ un'identià polinomiale per A. Dimostriamo la tesi per induzione su $ht(f)$.
Se $ht(f) = 0$ allora la tesi è banalmente verificata perché f è multilineare.
Supponiamo che $ht(f) > 0$ e che la tesi sia vera per ogni identità polinomiale avente altezza minore di $ht(f)$.

Poiché $ht(f) > 0$, esiste $i \in \underline{m}\rfloor$ tale che $deg^i(f) > 1$. Se $k \in \mathbb{N} - \underline{m}\rfloor$, per **(2.25)**, $\Delta_{i,k}(f) \in T(A)$ e $ht(\Delta_{i,k}(f)) < ht(f)$. Dall'ipotesi induttiva segue subito la tesi.

□

La proposizione seguente evidenzia l'importanza rivestita dai polinomi multilineari nelle PI-algebre:

2.27 Proposizione. *Se F è un campo tale che $char(F) = 0$ e A è una F-algebra allora $T(A)$ è generato come T-ideale di $F\langle X\rangle$ dai polinomi multilineari che vi appartengono.*

Più in generale vale il seguente profondo risultato, dovuto a Kemer [11]:

2.28 Teorema. *Se F è un campo e $char(F) = 0$ allora ogni T-ideale di $F\langle X\rangle$ è finitamente generato.*

2.29 Definizione. Se $S \subseteq C\langle X\rangle$, si indica con $(S)^T$ il T-ideale di $C\langle X\rangle$ generato da S:

$$(S)^T := \bigcap I \qquad \text{al variare di } I \text{ tra i T-ideali di } C\langle X\rangle\,,\ S \subseteq I.$$

Se $S_1, S_2 \subseteq C\langle X\rangle$, S_1 e S_2 si dicono *equivalenti* se $(S_1)^T = (S_2)^T$.

2.30 Proposizione. *Sia F un campo.*

(1) *Se F è infinito allora ogni polinomio in $F\langle X\rangle$ è equivalente alle sue componenti multiomogenee.*

(2) *Se $char(F) = 0$, ogni polinomio di $F\langle X\rangle$ è equivalente ad un insieme di polinomi multilineari.*

Dimostrazione. **(1)** Siano $m \in \mathbb{N}$ e $f(x_1, \dots, x_m) \in F\langle X\rangle$ (anche non mescolato). Posto $n := deg^1(f)$, per ogni $i \in \underline{n}\rfloor$ indichiamo con f_i la componente omogenea di f di grado i rispetto a x_1. Allora $f = \sum_{i=0}^{n} f_i$.
Vogliamo dimostrare che, per ogni $i \in \underline{n}\rfloor$, $f_i \in (f)^T$. Ovviamente vale:

$$\forall\, t \in F \qquad f(tx_1, x_2, \dots, x_m) \in (f)^T$$

e quindi

$$\forall\, t \in F \qquad \sum_{i=0}^{n} t^i f_i(x_1, x_2, \dots, x_m) \in (f)^T.$$

Allora, posti $\overline{0} := (f)^T$ e

$$\forall\, i \in \underline{n}\rfloor \qquad \overline{f}_i = f_i + (f)^T \in F\langle X\rangle / (f)^T$$

si ha

$$\forall\, t \in F \qquad \sum_{i=0}^{n} t^i \overline{f}_i = \overline{0}.$$

Da **(2.19)** segue

$$\forall\, i \in \underline{n}] \qquad \overline{f}_i = \overline{0}$$

e quindi

$$\forall\, i \in \underline{n}] \qquad f_i \in (f)^T.$$

Poichè $f = \sum_{i=0}^{n} f_i$ è vero anche il viceversa, cioè $f \in (f_0, f_1, \ldots, f_n)^T$.
Pertanto $(f)^T = (f_0, f_1, \ldots, f_n)^T$.
Iterando tale procedimento per ogni $i \in \underline{m}] - \{1\}$ si ottiene la tesi.
(2) Siano $m \in \mathbb{N}$ e $f(x_1, \ldots, x_m) \in F\langle X\rangle$ un polinomio mescolato e non multilineare. Applicando il metodo di multilinearizzazione, si ottiene un'identità multilineare g di grado minore o uguale a $deg(f)$. Dalla definizione di operatore differenza segue subito che $g \in (f)^T$ e per **(2.24(3))**, grazie all'ipotesi $char(F) = 0$, si ha che $f \in (g)^T$. Pertanto $(f)^T = (g)^T$, cioè f e g sono equivalenti.

□

2.31 Esempio. Siano $p \in \mathbb{P}$, $m \in \mathbb{N}$ e F un campo finito tale che $|F| = p^m$. Allora il seguente polinomio:

$$f(x_1, \ldots, x_{p^m}) := \sum_{\pi \in \mathcal{S}_{p^m}} x_{\pi(1)} \ldots x_{\pi(p^m)} \in \mathbb{Z}\langle X\rangle$$

è un'identità di F detta *identità simmetrica*.
Infatti $F - \{0\}$ è un gruppo moltiplicativo di ordine $p^m - 1$ e quindi, per ogni $x \in F - \{0\}$, si ha $x^{p^m - 1} = 1_F$ cioè $x^{p^m} - x = 0$. Pertanto $x_1^{p^m} - x_1 \in \mathbb{Z}\langle X\rangle$ è un'identità di F e, multilinearizzandola, si ottiene proprio il polinomio f.
Da **(2.25(1))** segue che f è un'identità di F, e quindi

$$\forall\, a_1, \ldots, a_{p^m} \in F \qquad \sum_{\pi \in \mathcal{S}_{p^m}} a_{\pi(1)} \ldots a_{\pi(p^m)} = 0.$$

Accenniamo, ora, brevemente ad un altro metodo di multilinearizzazione che risulta più veloce di quello già visto.
Siano $m \in \mathbb{N}$, $f(x_1, \ldots, x_m) \in C\langle X\rangle$, $i \in \underline{m}]$ e $n \in \mathbb{N}$ tali che $deg^i(f) = n$. Allora, per ottenere un polinomio multilineare a partire da f, si determina il polinomio $g := f(x \mapsto y_1 + y_2 + \ldots + y_n)$ e di tale polinomio si considera la componente di multigrado $(1, 1, \ldots, 1)$ in $y_1, y_2, \ldots, y_n$.

2.32 Proposizione. *Siano A una C-algebra, $t \in \mathbb{N}$, $f \in C\langle X\rangle$ un polinomio multilineare e sia $\mathcal{B}$ un insieme di generatori di A come C-modulo. Allora f è un'identità polinomiale per A se e solo se f si annulla per ogni valutazione delle sue lettere sugli elementi di $\mathcal{B}$.*

Dimostrazione. Ovviamente se f è un'identità polinomiale per A allora f si annulla per ogni valutazione delle sue indeterminate sugli elementi di $\mathcal{B}$.
Dimostriamo che vale il viceversa. Sia $n \in \mathbb{N}$ tale che $f = f(x_1, \ldots, x_n)$ e supponiamo dapprima che $\mathcal{B}$ sia un insieme finito.

Siano $t \in \mathbb{N}$ e $a_1, \ldots, a_t \in A$ tali che $\mathcal{B} = \{a_1, \ldots, a_t\}$.
Siano $b_1, \ldots, b_n \in A$ e, per ogni $i \in \underline{n}\rfloor$ e $j_i \in \underline{t}\rfloor$, sia $c_{ij_i} \in C$ tale che

$$\forall\, i \in \underline{n}\rfloor \qquad b_i = \sum_{j_i=1}^{t} c_{ij_i} a_{j_i}.$$

Dalla multilinearità di f segue che:

$$\begin{aligned} f(b_1, \ldots, b_n) &= f\left(\sum_{j_1=1}^{t} c_{1j_1} a_{j_1}, \ldots, \sum_{j_n=1}^{t} c_{nj_n} a_{j_n} \right) = \\ &= \sum_{j_1, \ldots, j_n = 1}^{t} c_{1j_1} \ldots c_{nj_n} f(a_{j_1}, \ldots, a_{j_n}) = 0. \end{aligned}$$

Se $\mathcal{B}$ è infinito si procede in modo analogo in quanto ogni elemento di A si scrive come combinazione lineare finita di elementi di $\mathcal{B}$.

□

2.33 Definizione. Per ogni $n \in \mathbb{N}$, il seguente polinomio

$$S_n(x_1, \ldots, x_n) := \sum_{\pi \in \mathcal{S}_n} (-1)^{\pi} x_{\pi(1)} x_{\pi(2)} \ldots x_{\pi(n-1)} x_{\pi(n)}$$

si dice il *polinomio standard di grado* n ($(-1)^{\pi}$ è la segnatura della permutazione π).

2.34 Definizione. Siano $m \in \mathbb{N}$ e $f = f(x_1, \ldots, x_m) \in C\langle X \rangle$. f si dice *alternante* se

$$\forall\, \pi \in \mathcal{S}_m \qquad f(x_{\pi(1)}, \ldots, x_{\pi(m)}) = (-1)^{\pi} f(x_1, \ldots, x_m).$$

Si dimostra che, per ogni $m \in \mathbb{N}$, S_m è alternante e da ciò e da **(2.32)** segue:

2.35 Corollario. *Siano A una C-algebra e $m \in \mathbb{N}$. Se A è generata come C-modulo da un insieme costituito da meno di t elementi allora il polinomio standard $S_{t+1}(x_1, \ldots, x_{t+1})$ è un'identità polinomiale per A.*

2.36 Corollario. *Ogni algebra di dimensione finita è una PI-algebra.*

Pertanto le PI-algebre possono essere riguardate come una generalizzazione non solo delle algebre commutative ma anche delle algebre di dimensione finita.

2.37 Corollario. *Siano F un campo e $n \in \mathbb{N}$. Allora $S_{n^2+1}(x_1, \ldots, x_{n^2+1})$ è un'identità polinomiale per $M_n(F)$.*

2.38 Proposizione. *Sia $n \in \mathbb{N}$. Per ogni $t \in \underline{n}\rfloor$, $M_t(C)$ soddisfa tutte le identità polinomiali di $M_n(C)$.*

Dimostrazione. Siano $t \in \underline{n}\rfloor$ e $E = \{E_{ij} \mid i, j \in \underline{n}\rfloor\}$ l'insieme delle matrici elementari. La seguente applicazione:

$$\varphi : M_t(C) \to M_n(C), \qquad A = \sum_{i,j=1}^{t} a_{ij}E_{ij} \;\mapsto\; A' = \sum_{i,j=1}^{t} a_{ij}E_{ij} + \\ + \sum_{i=1}^{n}\sum_{j=t+1}^{n} 0 \cdot (E_{ij} + E_{ji})$$

è un monomorfismo di C-algebre e quindi possiamo riguardare $M_t(C)$ come una C-sottoalgebra di $M_n(C)$. Pertanto ogni identità di $M_n(C)$ è identità di $M_t(C)$.

□

CAPITOLO 3

IL TEOREMA DI AMITSUR-LEVITZKI

Il Teorema di Amitsur-Levitzki è uno dei più importanti risultati riguardanti le identità di algebre di matrici e di esso sono state date quattro diverse dimostrazioni. L'originale del 1950, dovuta ad S. A. Amitsur e J. Levitzki, è di tipo combinatorio ed è stata successivamente modificata da Swann utilizzando la teoria dei grafi.
Nel 1958, B. Kostant [12] ha dato una dimostrazione basata sulla teoria delle *identità traccia* e sulla teoria di Frobenius riguardante le rappresentazioni dei gruppi simmetrici e alternanti.
La dimostrazione di Y. P. Razmyslov [18] del 1974 è basata, invece, sulla multilinearizzazione del Teorema di Hamilton-Caley.
La dimostrazione che noi presenteremo è quella del 1976 di S. Rosset [19]: è la più breve ed ingegnosa e fa uso del concetto di *algebra esterna*.

3.1 Teorema. *(Teorema di Amitsur-Levitzki [4])*
Sia $n \in \mathbb{N}$.

(1) Il grado minimo delle identità polinomiali proprie di $M_n(C)$ è $2n$.

(2) Il polinomio standard $S_{2n}(x_1, \ldots, x_{2n})$ è un'identità polinomiale per $M_n(C)$.

Vediamo subito la dimostrazione della prima parte del teorema:

Dimostrazione. (di **(3.1(1))**)
Siano $t \in \mathbb{N}$ e $f \in C\langle X\rangle$ un'identità polinomiale per $M_n(C)$ che possiamo supporre propria e multilineare di grado $t \leq 2n-1$. Allora, per ogni $\pi \in \mathcal{S}_t$,

esiste $\alpha_\pi \in C$ tale che:

$$f = \sum_{\pi \in \mathcal{S}_t} \alpha_\pi x_{\pi(1)} \dots x_{\pi(t)}$$

e supponiamo che $\alpha_{id_{\underline{t}|}} M_n(C) \neq 0$.
Consideriamo l'insieme delle matrici elementari $E = \{E_{ij} \mid i, j \in \underline{n}|\}$ e, per ogni $k \in \underline{n}|$, definiamo:

$$T_k := \begin{cases} E_{\frac{k+1}{2}\,\frac{k+1}{2}} & \text{se } k \text{ è dispari} \\ E_{\frac{k}{2}\,\frac{k+2}{2}} & \text{se } k \text{ è pari} \end{cases}$$

cioè $T_1 := E_{11}$, $T_2 := E_{12}$, $T_3 := E_{22}$, $T_4 := E_{23}$, ecc.. Osserviamo che l'insieme $\{T_k \mid k \in \underline{n}|\}$ ha cardinalità $2n - 1$.
Per ogni $\pi \in \mathcal{S}_t$, poniamo $T_\pi := T_{\pi(1)} T_{\pi(2)} \dots T_{\pi(t)}$ e sia $\pi \in \mathcal{S}_t$ tale che $T_\pi \neq 0$. Per ogni $k \in \underline{t}|$, poniamo $E_{i_k j_k} := T_{\pi(k)}$ e sia $k \in \underline{t}|$ tale che $T_{\pi(k)} = E_{11} = T_1$. Allora:

$$\begin{aligned} T_\pi &= T_{\pi(1)} T_{\pi(2)} \dots T_{\pi(k-1)} T_{\pi(k)} T_{\pi(k+1)} \dots T_{\pi(t)} = \\ &= T_{\pi(1)} T_{\pi(2)} \dots E_{i_{k-1}\,j_{k-1}} E_{11} E_{i_{k+1}\,j_{k+1}} \dots T_{\pi(t)}. \end{aligned}$$

Ma $E_{i_{k-1}\,j_{k-1}} E_{11} E_{i_{k+1}\,j_{k+1}} \neq 0$ se e solo se $j_{k-1} = 1$ e $i_{k+1} = 1$, cioè se e solo se

$$T_{\pi(k+1)} = E_{i_{k+1}\,j_{k+1}} = E_{12} = T_2$$

e

$$T_{\pi(k-1)} = E_{i_{k-1}\,j_{k-1}} = E_{11} = T_1 = T_{\pi(k)}.$$

Pertanto, poiché $T_\pi \neq 0$, si deve avere $T_1 = T_{\pi(1)}$ e $T_2 = T_{\pi(2)}$, cioè $\pi(1) = 1$ e $\pi(2) = 2$.
Sia, ora, $z \in \underline{t}|$ tale che $T_{\pi(z)} = E_{22} = T_3$. Essendo $T_\pi \neq 0$, deve risultare:

$$0 \neq T_{\pi(z-1)} T_{\pi(z)} T_{\pi(z+1)} = E_{i_{z-1}\,j_{z-1}} E_{22} E_{i_{z+1}\,j_{z+1}}$$

e ciò si verifica se e solo se $j_{z-1} = 2$ e $i_{z+1} = 2$, cioè se e solo se

$$T_{\pi(z-1)} = E_{i_{z-1}\,j_{z-1}} = E_{22} = T_2$$

e

$$T_{\pi(z+1)} = E_{i_{z+1}\,j_{z+1}} = E_{23} = T_4.$$

Segue che $\pi(z-1) = 2 = \pi(2)$ e quindi $z = 3$. Pertanto $\pi(3) = 3$ e $\pi(4) = 4$.
Procedendo in questo modo, è evidente che $T_\pi \neq 0$ se e solo se $\pi = id_{\underline{t}|}$ e quindi:

$$f(T_1, T_2, \dots, T_t) = \alpha_{id_{\underline{t}|}} T_1 \dots T_t = \begin{cases} \alpha_{id_{\underline{t}|}} E_{1\,\frac{t+1}{2}} & \text{se } t \text{ è dispari} \\ \alpha_{id_{\underline{t}|}} E_{1\,\frac{t+2}{2}} & \text{se } t \text{ è pari} \end{cases}$$

In entrambi i casi risulta $f(T_1, T_2, \dots, T_t) \neq 0$ che è impossibile perchè avevamo supposto che f fosse è un'identità di $M_n(C)$. Pertanto f non può essere un'identità di $M_n(C)$.

□

Per la dimostrazione della seconda parte del teorema abbiamo bisogno di fare alcune premesse.

3.2 Lemma. *Siano $n \in \mathbb{N}$ e $f(x_1,\dots,x_n) \in C\langle X\rangle$ un'identità polinomiale multilineare per una C-algebra A. Se B è una C-algebra commutativa, allora f è un'identità polinomiale del prodotto tensoriale $A \bigotimes_C B$.*

Dimostrazione. Da **(2.13)** segue che, per ogni $\pi \in \mathcal{S}_n$, esiste $\alpha_\pi \in C$ tale che

$$f = f(x_1,\dots,x_n) = \sum_{\pi\in\mathcal{S}_n} \alpha_\pi x_{\pi(1)} \dots x_{\pi(n)}.$$

Se $\mathcal{B}, \mathcal{B}'$ sono insiemi di generatori rispettivamente per A e B come C-moduli, allora $\mathcal{B}'' := \{a \otimes b \,|\, a \in \mathcal{B}, b \in \mathcal{B}'\}$ è un insieme di generatori per $A \bigotimes_C B$ come C-modulo.
Da **(2.32)** segue che, per dimostrare che f è un'identità polinomiale per $A \bigotimes_C B$, basta verificare che f si annulla per ogni valutazione delle sue indeterminate sugli elementi di $\mathcal{B}''$. Pertanto, dalla commutatività di B, segue che, per ogni $a_1,\dots,a_n \in \mathcal{B}, b_1,\dots,b_n \in \mathcal{B}'$,

$$\begin{aligned} f(a_1 \otimes b_1,\dots,a_n \otimes b_n) &= \sum_{\pi\in\mathcal{S}_n} \alpha_\pi (a_{\pi(1)} \dots a_{\pi(n)} \otimes b_{\pi(1)} \dots b_{\pi(n)}) = \\ &= \left(\sum_{\pi\in\mathcal{S}_n} \alpha_\pi a_{\pi(1)} \dots a_{\pi(n)}\right) \otimes b_1 \dots b_n = \\ &= f(a_1,\dots,a_n) \otimes b_1 \dots b_n = 0 \otimes b_1 \dots b_n = 0 \end{aligned}$$

□

Pertanto le identità polinomiali multilineari si trasportano per tensorizzazione con algebre commutative.

3.3 Definizione. Siano K un campo, $n \in \mathbb{N}$ e sia $K[x_1,\dots,x_n]$ l'anello dei polinomi commutativi su K nelle indeterminate indipendenti $x_1,\dots,x_n$. Una funzione $f(x_1,\dots,x_n)$ si dice *funzione simmetrica* se

$$\forall\, \sigma \in \mathcal{S}_n \qquad f(x_{\sigma(1)},\dots,x_{\sigma(n)}) = f(x_1,\dots,x_n).$$

Per ogni $j \in \underline{n}|$ la *k-sima funzione elementare simmetrica* di $x_1,\dots,x_n$ è:

$$e_k(x_1,\dots,x_n) = \sum_{1\le i_1<i_2<\dots<i_k\le n} x_{i_1} x_{i_2} \dots x_{i_k}$$

mentre la k-sima *funzione simmetrica potenza* di $x_1,\dots,x_n$ è

$$p_k(x_1,\dots,x_n) = x_1^k + x_2^k + \dots + x_n^k.$$

Le *formule di Newton* forniscono un legame fra le funzioni simmetriche elementari e le funzioni simmetriche potenza:

3.4 Lemma. ***(Formule di Newton)*** *Sia* $n \in \mathbb{N}$.
(1) $\forall\, k \in \underline{n}\rfloor \qquad p_k - p_{k-1}e_1 + p_{k-2}e_2 + \ldots + (-1)^k k e_k = 0$
(2) $\forall\, k \in \mathbb{N} - \underline{n}\rfloor \qquad p_k - p_{k-1}e_1 + p_{k-2}e_2 + \ldots + (-1)^n p_{k-n}e_n = 0$

Per dimostrare tali formule è utile introdurre la seguente notazione: se $n, h_1, \ldots, h_n \in \mathbb{N}_0$ e $x_1^{h_1} \ldots x_n^{h_n} \in K[x_1, \ldots, x_n]$, allora $S(x_1^{h_1} \ldots x_n^{h_n})$ indica la somma di tutti i monomi di $K[x_1, \ldots, x_n]$ ottenuti a partire da $x_1^{h_1} \ldots x_n^{h_n}$ sotto l'azione naturale del gruppo simmetrico $\mathcal{S}_n$ sulle indeterminate $x_1, \ldots x_n$.

Dimostrazione. **(1)** In riferimento alla notazione introdotta, si ha:
$p_{k-1}e_1 = p_k + S(x_1^{k-1}x_2)$
$p_{k-2}e_2 = S(x_1^{k-1}x_2) + S(x_1^{k-2}x_2x_3)$
$\vdots$
$p_{k-i}e_i = S(x_1^{k-i+1}x_2 \ldots x_i) + S(x_1^{k-i}x_2 \ldots x_{i+1}) \qquad \forall\, i \in \underline{k-2}\rfloor$
$\vdots$
$p_1 e_{k-1} = S(x_1^2 x_2 \ldots x_{k-1}) + k e_k$.
Pertanto, facendo la somma membro a membro a segni alterni, si ottiene la prima formula.
(2) Si considerano le seguenti uguaglianze:
$p_{k-1}e_1 = p_k + S(x_1^{k-1}x_2)$
$p_{k-2}e_2 = S(x_1^{k-1}x_2) + S(x_1^{k-2}x_2x_3)$
$\vdots$
$p_{k-i}e_i = S(x_1^{k-i+1}x_2 \ldots x_i) + S(x_1^{k-i}x_2 \ldots x_{i+1}) \qquad \forall\, i \in \underline{k-2}\rfloor$
$\vdots$
$p_{k-n}e_n = S(x_1^{k-n+1}x_2 \ldots x_n)$
e facendo, come prima, la somma membro a membro a segni alterni si ottiene la seconda formula.

$\square$

3.5 Proposizione. *Siano* $n \in \mathbb{N}$ *e* $A \in M_n(\mathbb{Q})$. *Siano* $\beta_1, \ldots, \beta_n \in \mathbb{C}$ *gli autovalori (senza molteplicità) di* A *e siano* $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}$ *tali che il seguente polinomio*

$$p_A(t) := t^n + \sum_{i=1}^{n} (-1)^i \alpha_i t^{n-i} \in \mathbb{Q}[t]$$

sia il polinomio caratteristico di A. *Allora, per ogni* $k \in \underline{n}\rfloor$, α_k *è un polinomio razionale in* $tr(A^i)$ *per ogni* $i \in \mathbb{N}$ *e soddisfa la seguente formula:*

$$k\alpha_k = \sum_{i=1}^{k} (-1)^{i-1} \alpha_{k-i} tr(A^i).$$

Dimostrazione. In generale vale:

$$\forall\, k \in \underline{n}\rfloor \qquad \alpha_k = e_k(\beta_1, \ldots, \beta_n).$$

A è simile in $\mathbb{C}$ ad una matrice triangolare superiore $B \in M_n(\mathbb{C})$ avente sulla diagonale principale gli autovalori di A e quindi, se I_n è la matrice identità di $M_n(\mathbb{Q})$, si ha

$$p_A(t) = -det(-B + tI_n) = \prod_{i=1}^{n}(t - \beta_i).$$

Poiché la traccia è un invariante per matrici simili, segue

$$tr(A^k) = \beta_1^k + \ldots + \beta_n^k = p_k(\beta_1, \ldots, \beta_n).$$

Da **(3.4(1))** segue subito che

$$k\alpha_k = \sum_{i=1}^{k}(-1)^{i-1}\alpha_{k-i}tr(A^i).$$

□

3.6 Proposizione. *Siano A una $\mathbb{Q}$-algebra commutativa unitaria e $n \in \mathbb{N}$. Se $X \in M_n(A)$ è tale che $tr(X^i) = 0$ per ogni $i \in \mathbb{N}$, allora $X^n = 0$.*

Dimostrazione. Sia $X = (x_{ij})_{i,j=1,\ldots,n} \in M_n(A)$ e, per ogni $i, j \in \underline{n}|$, sia t_{ij} una indeterminata commutativa. L'anello dei polinomi

$$T := \mathbb{Q}[t_{11}, \ldots, t_{1n}, t_{21}, \ldots, t_{2n}, \ldots, t_{nn}]$$

è un dominio d'integrità contenuto nel suo campo dei quozienti

$$K := \mathbb{Q}(t_{11}, \ldots, t_{1n}, t_{21}, \ldots, t_{2n}, \ldots, t_{nn}).$$

Sia $U \in M_n(K)$ la *matrice generica*, cioè sia $U := (t_{ij})_{i,j=1,\ldots,n}$. Poiché T è un'algebra libera, per definire un omomorfismo basta definire le immagini delle indeterminate t_{ij}. Consideriamo, allora, il seguente omomorfismo:

$$g : T \to A, \qquad t_{ij} \mapsto x_{ij}.$$

Esso si estende in modo unico agli anelli di matrici in questo modo:

$$\widetilde{g} : M_n(T) \to M_n(A), \qquad U \mapsto X.$$

Siano $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}$ tali che il seguente polinomio

$$p_U(t) = t^n + \sum_{i=1}^{t}(-1)^i\alpha_i t^{n-i} \in K[t]$$

sia il polinomio caratteristico di U. Allora per il teorema di Hamilton-Caley, $p_U(U) = 0$, cioè

$$U^n - \alpha_1 U^{n-1} + \alpha_2 U^{n-2} + \ldots + (-1)^{n-1}\alpha_{n-1}U + (-1)^n\alpha_n = 0.$$

Per (3.5), per ogni $k \in \underline{n}\rfloor$, α_k è un polinomio a coefficienti razionali nelle tracce di U^i con $i \in \mathbb{N}$ e, poiché

$$\forall i \in \mathbb{N} \qquad g(tr(U^i)) = tr(X^i),$$

dalle ipotesi su X segue che $g(\alpha_k) = 0$. Pertanto

$$\begin{aligned} 0 &= \widetilde{g}(U^n - \alpha_1 U^{n-1} + \alpha_2 U^{n-2} + \ldots + (-1)^{n-1}\alpha_{n-1}U + (-1)^n \alpha_n) = \\ &= \widetilde{g}(U^n) - g(\alpha_1)\widetilde{g}(U^{n-1}) + g(\alpha_2)\widetilde{g}(U^{n-2}) + \ldots + \\ &\quad +(-1)^{n-1} g(\alpha_{n-1})\widetilde{g}(U) + (-1)^n g(\alpha_n) = X^n + 0 = X^n. \end{aligned}$$

□

Fondamentale per la dimostrazione del teorema di Levitzki è il concetto di algebra esterna:

3.7 Definizione. Siano $X = \{x_1, x_2, \ldots\}$ un insieme di indeterminate non commutative, F un campo tale che $char(F) \neq 2$ e sia I l'ideale di $F\langle X \rangle$ generato da tutti i polinomi del tipo $x_i x_j + x_j x_i \in F\langle X \rangle$ con $i, j \in \mathbb{N}$. Allora il quoziente $E := F\langle X \rangle / I$ si dice *algebra esterna su F generata da X* (o *algebra di Grassmann*).

Segue subito che una base di $F\langle X \rangle / I$ è costituita dalla parola vuota 1 e da tutti i possibili monomi del tipo $x_{i_1} x_{i_2} \ldots x_{i_n}$ con $n, i_1, i_2, \ldots, i_n \in \mathbb{N}$ tali che $i_1 < i_2 < \ldots < i_n$.
Vediamo, ora, un altro modo in cui si può definire l'algebra esterna.

3.8 Definizione. Sia V un C-bimodulo. Per ogni $n \in \mathbb{N}$ si definisce la *potenza tensoriale* $V^{\otimes n}$ induttivamente nel seguente modo:

$$V^{\otimes 0} := C$$

$$V^{\otimes 1} := V$$

$$\forall n \in \mathbb{N} \qquad V^{\otimes (n+1)} = V \bigotimes_C V^{\otimes n}.$$

Allora, per ogni $n \in \mathbb{N}$, $V^{\otimes n}$ è un C-bimodulo.
Posto

$$T_C(V) := \bigoplus_{n \in \mathbb{N}_0} V^{\otimes n},$$

si dice che $T_C(V)$ è l'*algebra tensoriale* di V e in essa il prodotto è definito per giustapposizione.

Si dimostra che se X è un insieme, F un campo tale che $char(F) \neq 2$ e V è uno spazio vettoriale su F con base $\mathcal{B} = \{v_i \mid i \in \mathbb{N}\}$, allora

$$T_F(V) \cong F\langle X \rangle,$$

dove X è equipotente a V (l'isomorfismo è quello che, per ogni $i \in \mathbb{N}$, ad x_i associa v_i). Pertanto l'algebra esterna E si può ottenere come quoziente di $T_F(V)$ con l'ideale I di $T_F(V)$ generato da tutti gli elementi del tipo $v \otimes w + w \otimes v$ al variare di $v, w \in V$.
L'algebra esterna è un esempio di algebra $\mathbb{Z}_2$-graduata. Più in generale si ha la seguente:

3.9 Definizione. Sia S un monoide. Una C-algebra R è *graduata sopra* S se, per ogni $s \in S$, esiste un C-sottomodulo R_s di R tale che

$$R = \bigoplus_{s \in S} R_s$$

e

$$\forall\, s_1, s_2 \in S \qquad R_{s_1} R_{s_2} \subseteq R_{s_1 s_2}.$$

Come detto in precedenza, l'algebra esterna E è una *superalgebra*, cioè è un'algebra graduata sopra $\mathbb{Z}_2$. Infatti, posti

$$\forall\, i \in \mathbb{N} \qquad e_i := x_i$$

$$E_0 := span_F \langle 1, e_{i_1} \dots e_{i_{2m}} \,|\, m \in \mathbb{N} \rangle$$

$$E_1 := span_F \left\langle e_{i_1} \dots e_{i_{2m+1}} \,|\, m \in \mathbb{N} \right\rangle$$

si ha che $E_0 E_1 \subseteq E_1$, $E_1 E_0 \subseteq E_1$ e $E = E_0 \bigoplus E_1$.

L'importanza dell'algebra esterna nella teoria delle PI-algebre è rivelata dal seguente:

3.10 Teorema. ***(Teorema di Kemer [11])***
Sia F un campo algebricamente chiuso e di caratteristica 0. Se A è una PI-algebra su F, allora esiste una superalgebra $B = B_0 \bigoplus B_1$ di dimensione finita su F tale che, posto $G(B) := (B_0 \bigotimes_F E_0) \bigoplus (B_1 \bigotimes_F E_1)$, si ha

$$T(A) = T(G(B)).$$

Ritorniamo alla dimostrazione del teorema di Amitsur-Levitzki:

3.11 Lemma. *Sia F un campo tale che $char(F) = 0$ e sia A una F-algebra. Allora, per ogni $n, r \in \mathbb{N}$ e per ogni $a_1, \dots, a_{2r} \in M_n(A)$, si ha*

$$tr(S_{2r}(a_1, \dots, a_{2r})) = 0.$$

Dimostrazione. Se A_{2r} è il gruppo alterno di grado $2r$ allora, per ogni permutazione dispari $\sigma \in \mathcal{S}_{2r}$, risulta

$$\mathcal{S}_{2r} = A_{2r} \cup A_{2r}\sigma = A_{2r} \cup A_{2r}\sigma^{-1}.$$

In particolare se $\sigma := (1 \quad 2 \ldots 2r-1 \quad 2r) \in \mathcal{S}_{2r} - A_{2r}$ allora, per ogni $\pi \in \mathcal{S}_{2r}$, vale:

$$\begin{aligned} tr(a_{\pi(1)} \ldots a_{\pi(2r-1)} a_{\pi(2r)}) &= tr(a_{\pi(2r)} a_{\pi(1)} \ldots a_{\pi(2r-1)}) = \\ &= tr(a_{\pi\sigma^{-1}(1)} a_{\pi\sigma^{-1}(2)} \ldots a_{\pi\sigma^{-1}(2r)}) \end{aligned}$$

e quindi

$$\begin{aligned} tr \quad & (S_{2r}(a_1, \ldots, a_{2r})) = tr\left(\sum_{\pi \in \mathcal{S}_{2r}} (-1)^{\pi} a_{\pi(1)} \ldots a_{\pi(2r)} \right) = \\ = \quad & tr\left(\sum_{\pi \in A_{2r}} a_{\pi(1)} \ldots a_{\pi(2r)} + \sum_{\pi \in A_{2r}} (-1) a_{\pi\sigma^{-1}(1)} \ldots a_{\pi\sigma^{-1}(2r)} \right) = \\ = \quad & \sum_{\pi \in A_{2r}} tr(a_{\pi(1)} \ldots a_{\pi(2r)}) - \sum_{\pi \in A_{2r}} tr(a_{\pi\sigma^{-1}(1)} \ldots a_{\pi\sigma^{-1}(2r)}) = 0. \end{aligned}$$

□

Dimostrazione di (3.1(2)).

Se proviamo che il polinomio standard $S_{2n}(x_1, \ldots, x_{2n})$ è un'identità polinomiale per $M_n(\mathbb{Q})$, poiché $M_n(\mathbb{Z}) \subseteq M_n(\mathbb{Q})$, esso sarà un'identità polinomiale anche per $M_n(\mathbb{Z})$. Inoltre, essendo

$$M_n(C) \cong M_n(\mathbb{Z}) \bigotimes_{\mathbb{Z}} C,$$

per **(3.2)** si avrà che $S_{2n}(x_1, \ldots, x_{2n})$ è un'identità polinomiale per $M_n(C)$. Proviamo, pertanto, che $S_{2n}(x_1, \ldots, x_{2n})$ è identità polinomiale per $M_n(\mathbb{Q})$ e sia E l'algebra esterna su $\mathbb{Q}$. Allora

$$M_n(E) \cong M_n(\mathbb{Q}) \bigotimes_{\mathbb{Q}} E.$$

Siano $a_1, \ldots, a_{2n} \in M_n(\mathbb{Q})$ e siano $e_1, \ldots, e_{2n} \in E$ i generatori di E. Posto $a := a_1 e_1 + \ldots + a_{2n} e_{2n}$, si ha che $a \in M_n(E)$ e

$$a^2 = \sum_{\substack{i,j=1 \\ i \neq j}}^{n} a_i e_i a_j e_j = \sum_{1 \leq i < j \leq 2n} (a_i a_j - a_j a_i) e_i e_j.$$

Allora, posto $b := a^2$, segue che $b \in M_n(E_0)$ e, per ogni $r \in \mathbb{N}$, vale:

$$\begin{aligned} b^r \quad &= \quad a^{2r} = \sum_{\substack{i_1, \ldots, i_{2r}=1 \\ i_j \neq i_k \ \forall j \neq k}}^{n} a_{i_1} \ldots a_{i_{2r}} e_{i_1} \ldots e_{i_{2r}} = \\ &= \sum_{1 \leq j_1 < \ldots < j_{2r} \leq n} S_{2r}(a_{j_1}, \ldots, a_{j_{2r}}) e_{j_1} \ldots e_{j_{2r}}. \end{aligned}$$

Per **(3.11)** si ha:

$$tr(b^r) = \sum_{1 \leq j_1 < \ldots < j_{2r} \leq n} tr(S_{2r}(a_{j_1}, \ldots, a_{j_{2r}})e_{j_1} \ldots e_{j_{2r}}) = 0.$$

Dalla commutatività di E_0 e da **(3.6)** segue che $b^n = 0$ e quindi

$$0 = b^n = S_{2n}(a_1, \ldots, a_{2n})e_1 \ldots e_{2n}.$$

Poiché $M_n(E) \cong M_n(\mathbb{Q}) \bigotimes_{\mathbb{Q}} E$, $M_n(E)$ è un $M_n(\mathbb{Q})$-modulo libero con base $\{\prod e_{j_1} \ldots e_{j_{2r}} \,|\, 1 \leq j_1 < \ldots < j_{2r} \leq n\}$ e quindi $S_{2n}(a_1, \ldots, a_{2n}) = 0$.
Dall'arbitrarietà di $a_1, \ldots, a_{2n} \in M_n(\mathbb{Q})$ segue che $S_{2n}(x_1, \ldots, x_{2n})$ è una identità polinomiale per $M_n(\mathbb{Q})$.

□

CAPITOLO 4

IL TEOREMA DI KAPLANSKY

Dimostrato nel 1948, il teorema di Kaplansky è il primo significativo risultato ottenuto nell'ambito della teoria delle PI-algebre ed è sicuramente uno dei più importanti teoremi di struttura.
Per la sua dimostrazione è necessario studiare prima alcuni risultati riguardanti i sottocampi massimali di un corpo.

4.1 Definizione. Siano D un corpo e K un sottocampo di D. K è un *sottocampo massimale* di D se, per ogni H sottocampo di D, risulta

$$K \subseteq H \subseteq D \Rightarrow K = H.$$

4.2 Proposizione. *Siano D un corpo e K un sottocampo di D. Allora K è un sottocampo massimale di D se e solo se $C_D(K) = K$, dove $C_D(K)$ è il centralizzante in D di K.*

Dimostrazione. "$\Rightarrow$" Supponiamo che K sia un sottocampo massimale di D e sia $a \in C_D(K)$. Allora $K \subseteq K(a)$ e $K(a)$ è un sottocampo di D. Dalla massimalità di K in D segue che $a \in K$ e quindi $C_D(K) \subseteq K$. Essendo K commutativo, ovviamente $K \subseteq C_D(K)$ e quindi $C_D(K) = K$.
"$\Leftarrow$" Supponiamo che $C_D(K) = K$ e sia L un sottocampo di D tale che $K \subseteq L \subseteq D$. Allora, per ogni $a \in L$ e per ogni $k \in K$, si ha $ak = ka$ e quindi $a \in C_D(K) = K$. Pertanto $L \subseteq K$ e così $L = K$.

□

4.3 Teorema. *Siano F un campo, A una F-algebra centrale e semplice e B una F-algebra semplice. Allora $A \bigotimes_F B$ è una F-algebra semplice.*

Dimostrazione. Poniamo $R := A \bigotimes_F B$ e siano $1_A, 1_B$ le unità di A e B rispettivamente.
Sia Y una base di B su F. Allora, per ogni $r \in R - \{0\}$, esistono $n \in \mathbb{N}$,

$y_1, \dots, y_n \in Y, a_1, \dots, a_n \in A - \{0\}$ tali che r si scriva in modo unico nel seguente modo:

$$r = \sum_{i=1}^{n} a_i \otimes y_i.$$

Definiamo *lunghezza di* r il numero di addendi di quella sommatoria.
Sia I un ideale bilatero di R e sia $s \in I - \{0\}$ un elemento di lunghezza minima in I. Allora esistono $n \in \mathbb{N}, y_1, \dots, y_n \in Y, a_1, \dots, a_n \in A - \{0\}$ tali che

$$s = \sum_{i=1}^{n} a_i \otimes y_i.$$

Poiché $a_1 \neq 0$, Aa_1A è un ideale bilatero di A non nullo e quindi, dalla semplicità di A, segue che $Aa_1A = A$. Allora $1_A \in Aa_1A$ e quindi esistono $m \in \mathbb{N}, r_1, \dots, r_m, s_1, \dots, s_m \in A$ tali che

$$1_A = \sum_{j=1}^{m} r_j a_1 s_j.$$

Segue che

$$\begin{aligned}\sum_{j=1}^{m}(r_j \otimes 1_B)s(s_j \otimes 1_B) &= \sum_{i=1}^{n}\left(\sum_{j=1}^{m} r_j a_i s_j\right) \otimes y_i = \\ &= 1_A \otimes y_1 + \sum_{i=2}^{n}\left(\sum_{j=1}^{m} r_j a_i s_j\right) \otimes y_i =: w.\end{aligned}$$

Poiché $\sum_{j=1}^{m}(r_j \otimes 1_B)s(s_j \otimes 1_B) \in I$, allora $w \in I$. Inoltre $w \neq 0$ perché $y_1, \dots, y_n$ sono linearmente indipendenti e nell'espressione di w c'è almeno un elemento di A, l'unità 1_A, che è non nullo.
Sia, ora, $a \in A$. Allora, posto, per ogni $i \in \underline{n}\rfloor - \{1\}$, $\overline{a}_i := \sum_{j=1}^{m} r_j a_i s_j$, si ha

$$(a \otimes 1_B)w - w(a \otimes 1_B) = \sum_{i=2}^{n}(a\overline{a}_i - \overline{a}_i a) \otimes y_i = 0.$$

Infatti $(a \otimes 1_B)w - w(a \otimes 1_B) \in I$ perché I è bilatero e, poichè s ha lunghezza minima in I, ogni elemento di lunghezza minore deve essere nullo. Dalla lineare indipendenza di $y_2, \dots, y_n$ segue che

$$\forall i \in \underline{n}\rfloor - \{1\} \qquad a\overline{a}_i = \overline{a}_i a.$$

L'arbitrarietà di $a \in A$ implica che $\overline{a}_i \in Z(A) = F$ e quindi

$$w = 1_A \otimes y_1 + \sum_{i=2}^{n} \overline{a}_i \otimes y_i = 1_A \otimes \left(y_1 + \sum_{i=2}^{n} \overline{a}_i y_i\right).$$

Posto $b := y_1 + \sum_{i=2}^{n} \overline{a}_i y_i$ segue che $w = 1_A \otimes b$ e $b \neq 0$ essendo $w \neq 0$. Poiché B è semplice, $BbB = B$ e quindi esistono $t \in \mathbb{N}, c_1, \ldots, c_t, d_1, \ldots, d_t \in B$ tali che

$$1_B = \sum_{i=1}^{t} c_i b d_i.$$

Allora

$$\begin{aligned} \sum_{i=1}^{t} (1_A \otimes c_i) w (1_A \otimes d_i) &= \sum_{i=1}^{t} (1_A \otimes c_i)(1_A \otimes b)(1_A \otimes d_i) = \\ &= 1_A \otimes \left(\sum_{i=1}^{t} c_i b d_i \right) = 1_A \otimes 1_B = 1_R. \end{aligned}$$

Ma $w \in I$ e quindi, essendo I bilatero, $\sum_{i=1}^{t} (1_A \otimes c_i) w (1_A \otimes d_i) \in I$, cioè $1_R \in I$. Pertanto $I = R$ e quindi R è semplice.

□

4.4 Corollario. *Sia F un campo e siano A, B F-algebre centrali e semplici. Allora $A \bigotimes_F B$ è una F-algebra centrale e semplice.*

4.5 Proposizione. *Siano D un corpo, K un sottocampo massimale e poniamo $F := Z(D)$. Allora $D \bigotimes_F K$ è un anello denso di trasformazioni K-lineari su D.*

Dimostrazione. Per ogni $a \in D$ consideriamo la moltiplicazione a sinistra in D:

$$l_a : D \to D, \qquad x \mapsto ax$$

e la moltiplicazione a destra in D:

$$\sigma_a : D \to D, \qquad x \mapsto xa.$$

Allora, riguardando D come un gruppo abeliano, si ha che $l_a, \sigma_a \in End(D)$. Posto $R := D \bigotimes_F K$, possiamo costruire la seguente applicazione:

$$f : R \to End(D), \qquad a \otimes c \mapsto l_a \circ \sigma_c$$

che risulta essere ben posta per la proprietà universale dei prodotti tensoriali. Allora f è un omomorfismo di anelli e $f(1_D \otimes 1_D) = id_D$.
Poiché tutti i corpi e i campi sono semplici, D è un'algebra centrale semplice su F e K è semplice. Per **(4.3)**, R è una F-algebra semplice e così $ker f = 0$ perché $ker f$ è un ideale bilatero di R. Essendo f non nullo, segue che D è un R-modulo fedele.
Inoltre, per ogni $a, x \in D$ e per ogni $c \in K$ si ha

$$(a \otimes c)\, x = f(a \otimes c)(x) = (l_a \circ \sigma_c)(x) = axc$$

e quindi D è irriducibile come R-modulo perché se $x \neq 0$ allora, per ogni $y \in D$, esiste $d \in D$ tale che $y = dx$.
Osserviamo, infine, che la moltiplicazione è non banale in quanto

$$(1_D \otimes 1_D)\,x = x \neq 0.$$

Pertanto R è primitivo e D è l'R-modulo fedele e irriducibile.
Vediamo, ora, com'è fatto $End_R(D)$:
$End_R(D) = \{g | g : D \to D\ F - \text{lineare}, g(axb) = ag(x)b\ \forall\, a, x \in D, b \in K\}$.
Pertanto dobbiamo studiare le applicazioni che soddisfano la seguente proprietà:

$$\forall\, a, x \in D, b \in K \qquad g(axb) = ag(x)b \tag{$\star$}$$

Innanzitutto osserviamo che g è una moltiplicazione a destra, infatti basta porre $x := 1_D$ e $b := 1_D$ e si ottiene:

$$\forall\, a \in D \qquad g(a) = ag(1_D).$$

Allora, posto $c := g(1_D)$,

$$\forall\, a \in D \qquad g(a) = ac$$

e quindi dalla $(\star)$ segue:

$$\forall\, a, x \in D, b \in K \qquad axbc = axcb.$$

Se poniamo $a := 1_D$ e $x := 1_D$ allora:

$$\forall\, b \in K \qquad bc = cb,$$

cioè $c \in C_D(K)$. Poiché K è massimale, da **(4.2)** segue che $C_D(K) = K$ e così $c \in K$. Pertanto $End_R(D) = \{\sigma_c \,|\, c \in K\}$.
Per il Teorema di Densità di Jacobson (cfr.**(1.11)**), R è un anello denso di trasformazioni lineari di D su $End_R(D) = \{\sigma_c \,|\, c \in K\} \cong K$ e l'azione di K su D è proprio per moltiplicazione a destra.

□

4.6 Proposizione. *Siano D un corpo, K un sottocampo massimale di D e F il centro di D. Se $dim_F D$ è finita allora esiste $n \in \mathbb{N}$ tale che $dim_F D = n^2$.*

Dimostrazione. $D \bigotimes_F K$ è denso nell'anello delle applicazioni lineari a destra $End(D)_K$ e quindi, poiché $dim_F D$ è finita, $D \bigotimes_F K \cong End(D)_K$.
Posto $t := dim D_K$, si ha che

$$M_t(K) \cong End(D)_K \cong D \bigotimes_F K$$

e quindi $dim_F D = dim_F \Big(D \bigotimes_F K\Big) = t^2$.

□

4.7 Corollario. *Se A è un'algebra semplice di dimensione finita sul suo centro F allora esiste $m \in \mathbb{N}$ tale che $dim_F A = m^2$.*

Dimostrazione. Per il Teorema di Wedderburn-Artin esistono $n \in \mathbb{N}$ e un corpo D tali che $A \cong M_n(D)$. Allora

$$F = Z(A) \cong Z(M_n(D)) \cong Z(D).$$

Per **(4.6)**, esiste $t \in \mathbb{N}$ tale che $dim_F D = t^2$ e quindi

$$dim_F A = dim_F(M_n(D)) = dim_D(M_n(D)) dim_F D = n^2 t^2 = (nt)^2.$$

$\square$

4.8 Teorema. ***(Teorema di Kaplansky [10])***
Ogni algebra primitiva soddisfacente un'identità polinomiale propria è un'algebra semplice di dimensione finita sul suo centro e tale dimensione è un quadrato.

Dimostrazione. Sia R una C-algebra primitiva e sia $f \in C\langle X \rangle$ un'identità polinomiale propria per R. Grazie a **(2.26)** possiamo supporre, senza perdere di generalità, che f sia multilineare e sia $d \in \mathbb{N}$ tale che $deg(f) = d$. Da **(1.15)** segue che esistono $n \in \mathbb{N}$ e un corpo D tali che $R \cong M_n(D)$ oppure, per ogni $n \in \mathbb{N}$, esistono un sottoanello S_n di R ed un epimorfismo φ_n da S_n su $M_n(D)$. Se si verificasse la seconda condizione, allora, posto $F := Z(D)$, per ogni $n \in \mathbb{N}$ f sarebbe un'identità polinomiale per $M_n(F)$ e ciò è impossibile per la prima parte del Teorema di Amitsur-Levitzki. Pertanto $R \cong M_n(D)$ e quindi, essendo $Z(R) \cong F$, R è un'algebra semplice su F.
Resta da provare che la dimensione di R su F come spazio vettoriale è finita.
Ovviamente D soddisfa f in quanto D è contenuto in R a meno di isomorfismi. Se K è un sottocampo massimale di D, da **(3.2)** e dalla multilinearità di f segue che f è un'identità polinomiale per $A := D \bigotimes_F K$. Inoltre anche A è primitivo e così, in modo analogo a quanto visto sopra, da **(1.15)** segue che esistono $t \in \mathbb{N}$ e un corpo Δ tali che $A \cong M_t(\Delta)$. In particolare, $\Delta^{op} = End_A(M)$, dove M è un A-modulo fedele e irriducibile. Ma in **(4.5)** abbiamo dimostrato che D è un A-modulo fedele irriducibile e che $End_A(D) \cong K$. Allora $\Delta^{op} \cong K$ e quindi $\Delta \cong K$ essendo K un campo. Pertanto $A \cong M_t(K)$.

Poiché $R \cong M_n(D)$ e $M_n(D) \cong M_n(F) \otimes_F D$ segue:

$$\begin{aligned} R \bigotimes_F K &\cong M_n(D) \bigotimes_F K \cong \\ &\cong \left(M_n(F) \bigotimes_F D \right) \bigotimes_F K \cong \\ &\cong M_n(F) \bigotimes_F \left(D \bigotimes_F K \right) \cong \\ &\cong M_n(F) \bigotimes_F M_t(K) \cong M_{nt}(K). \end{aligned}$$

Allora

$$dim_F R = dim_K R \bigotimes_F K = (nt)^2.$$

Inoltre, da (**3.2**) segue che f è un'identità polinomiale per $R \otimes_F K$ e quindi per $M_{nt}(K)$. Allora, per il teorema di Amitsur-Levitzki, $2(nt) \leq d$ e così $dim_F R \leq [d/2]^2$.

$\square$

CAPITOLO 5

POLINOMI CENTRALI PER ALGEBRE DI MATRICI

Il concetto di polinomio centrale ha svolto un ruolo cruciale nello sviluppo della teoria delle PI-algebre. Inizialmente l'interesse verso questi polinomi era dettato esclusivamente dalla curiosità in quanto si cercava una risposta al seguente problema posto da Kaplansky nel 1956: esistono polinomi centrali per $M_n(C)$ per ogni $n \in \mathbb{N}$? La risposta affermativa a tale quesito fu data nel 1972 da Formanek e nel 1973 da Razmyslov che costruirono i primi polinomi centrali usando due differenti metodi.
Ben presto fu chiaro che l'uso dei polinomi centrali permetteva una diretta applicazione delle tecniche standard della teoria degli anelli commutativi. Allora l'intera esposizione della teoria delle PI-algebre fu rivoluzionata e i polinomi centrali rivestirono in essa un ruolo dominante.

D'ora in poi denoteremo con F un campo.

5.1 Definizione. Siano $n \in \mathbb{N}$ e $f \in F\langle X\rangle$. f si dice *polinomio centrale* per $M_n(F)$ se e solo se
(1) $f(M_n(F)) \subseteq Z(M_n(F))$;
(2) f non è un'identità polinomiale per $M_n(F)$;
(3) f ha termine noto nullo.

La condizione (3) serve per escludere i casi banali.

5.2 Esempio. Il seguente polinomio:

$$g := [x_1, x_2]^2 \in F\langle x_1, x_2\rangle$$

è centrale per $M_2(F)$. Infatti, siano $A_1, A_2 \in M_2(F)$ e sia

$$f(\lambda) := \lambda^2 - tr([A_1, A_2])\lambda + det([A_1, A_2])$$

il polinomio caratteristico di $[A_1, A_2]$. Poiché $tr([A_1, A_2]) = 0$ si ha che $f(\lambda) = \lambda^2 + det([A_1, A_2])$. Dal teorema di Hamilton-Cayley segue che:

$$0 = f([A_1, A_2]) = [A_1, A_2]^2 + det([A_1, A_2])I_2$$

e quindi:

$$[A_1, A_2]^2 = -det([A_1, A_2])I_2 \in Z(M_2(F)).$$

Pertanto $g(M_2(F)) \subseteq Z(M_2(F))$.
Inoltre g non è un'identità polinomiale perché, se consideriamo le matrici elementari e_{11}, e_{12}, e_{21}, vale:

$$\begin{aligned} g(e_{11}, e_{12} + e_{21}) &= [e_{11}, e_{12} + e_{21}]^2 = \\ &= (e_{11}e_{12} + e_{11}e_{21} - e_{12}e_{11} - e_{21}e_{11})^2 = \\ &= (e_{12} - e_{21})^2 \neq 0. \end{aligned}$$

Vale la seguente caratterizzazione:

5.3 Proposizione. *Siano $m \in \mathbb{N}$ e $f(x_1, \ldots, x_m) \in F\langle X\rangle$. f è centrale per $M_n(F)$ se e solo se f non è un'identità polinomiale per $M_n(F)$ ma $[x_{m+1}, f]$ è un'identità polinomiale per $M_n(F)$.*

5.4 Proposizione. *Siano $f \in C\langle X\rangle$, $n \in \mathbb{N}$ e $t \in \underline{n-1}]$. Se f è un polinomio centrale per $M_n(C)$, allora f è un'identità per $M_t(C)$.*

Dimostrazione. Per ipotesi vale:

$$0 \neq f(M_n(C)) \subseteq Z(M_n(C)) = \{\alpha I_n \mid \alpha \in C\}.$$

Sia $m \in \mathbb{N}$ tale che $f = f(x_1, \ldots, x_m)$. Se φ è il monomorfismo definito nella dimostrazione di **(2.38)**, allora, per ogni $A_1, \ldots, A_m \in M_t(C)$, esiste $\alpha \in C$ tale che

$$f(\varphi(A_1), \ldots, \varphi(A_m)) = \alpha I_n.$$

Per come abbiamo definito la φ, per ogni $i \in \underline{m}]$, si ha $(\varphi(A_i))E_{nn} = 0$ e quindi:

$$\alpha E_{nn} = \alpha I_n E_{nn} = f(\varphi(A_1), \ldots, \varphi(A_m))E_{nn} = 0.$$

Segue che $\alpha = 0$ e pertanto

$$0 = f(\varphi(A_1), \ldots, \varphi(A_m)) = \varphi(f(A_1, \ldots, A_m)).$$

Ma φ è iniettiva e quindi $f(A_1, \ldots, A_m) = 0$, cioè f è un'identità di $M_t(C)$.

□

Vediamo, ora, la costruzione di polinomio centrale dovuta a Razmyslov. Essa è legata ai concetti di identità polinomiale debole e di trasformata di Razmyslov.

5.5 Definizione. Siano $n, m \in \mathbb{N}$ e $f(x_1, \ldots, x_m) \in F\langle X \rangle$. f è un'*identità polinomiale debole* per $M_n(F)$ se, per ogni $a_1, \ldots, a_m \in M_n(F)$ tali che $tr(a_1) = \ldots = tr(a_m) = 0$ si ha $f(a_1, \ldots, a_m) = 0$.
Se $t \in \underline{m}\rfloor$, f si dice *identità polinomiale debole nelle lettere* $x_1, \ldots, x_t$ se per ogni $a_1, \ldots, a_m \in M_n(F)$ tali che $tr(a_1) = \ldots = tr(a_t) = 0$ si ha $f(a_1, \ldots, a_m) = 0$.
f è un'*identità polinomiale debole in senso stretto* per $M_n(F)$ se f è una identità polinomiale debole per $M_n(F)$ ma non è un'identità polinomiale per $M_n(F)$.

5.6 Esempio. Il seguente polinomio:

$$f := [x_1^2, x_2] \in F\langle X \rangle$$

è un'identità polinomiale debole in senso stretto in x_1 per $M_2(F)$.

Ovviamente ogni identità polinomiale è un'identità polinomiale debole.

5.7 Definizione. Sia $j \in \mathbb{N}$ e sia $f \in F\langle X \rangle$ un polinomio lineare nella lettera x_j. Allora esistono $m \in \mathbb{N}$ e, per ogni $i \in \underline{m}\rfloor$, esistono $g_i, h_i \in F\langle X \rangle$ tali che $deg^j(g_i) = deg^j(h_i) = 0$ e

$$f = \sum_{i=1}^{m} g_i x_j h_i.$$

Si dice *trasformata di Razmyslov* di f rispetto a x_j il seguente polinomio:

$$f^* = \sum_{i=1}^{m} h_i x_j g_i.$$

Ovviamente $(f^*)^* = f$.

5.8 Proposizione. *Siano $n, j, t \in \mathbb{N}$ e sia $f(x_1, \ldots, x_t) \in F\langle X \rangle$ un polinomio lineare nella lettera x_j. Allora f è un'identità polinomiale per $M_n(F)$ se e solo se la trasformata di Razmyslov f^* di f è un'identità polinomiale per $M_n(F)$.*

Dimostrazione. La seguente applicazione

$$\varphi : M_n(F) \times M_n(F) \to F, \qquad (a, b) \mapsto tr(ab)$$

è simmetrica, bilineare e non degenere, cioé se $a \in M_n(F)$ allora

$$tr(ab) = 0 \qquad \forall\, b \in M_n(F) \quad \Leftrightarrow a = 0.$$

Sia $m \in \mathbb{N}$ e, per ogni $i \in \underline{m}\rfloor$, siano $g_i, h_i \in F\langle X \rangle$ tali che $deg^j(g_i) = 0$, $deg^j(h_i) = 0$ e $f = \sum_{i=1}^{m} g_i x_j h_i$.
Per ogni $u_1, \ldots, u_t \in M_n(F)$ poniamo

$$\overline{f} := f(u_1, \ldots, u_t)$$

$$\forall i \in \underline{m}\rfloor \qquad \overline{g}_i := g_i(u_1, \ldots, u_t),\ \overline{h}_i := h_i(u_1, \ldots, u_t).$$

Segue che f è un'identità polinomiale per $M_n(F)$ se e solo se, per ogni $u_1, \ldots, u_t \in M_n(F)$, $\overline{f} = 0$ e quindi se e solo se

$$\begin{aligned}
\sum_{i=1}^{m} \overline{g}_i u_j \overline{h}_i = 0 \quad &\Leftrightarrow \quad \forall v \in M_n(F) \qquad tr\left(\sum_{i=1}^{m} \overline{g}_i u_j \overline{h}_i v\right) = 0 \Leftrightarrow \\
&\Leftrightarrow \quad \forall v \in M_n(F) \qquad tr\left(\sum_{i=1}^{m} \overline{h}_i v \overline{g}_i u_j\right) = 0 \Leftrightarrow \\
&\Leftrightarrow \quad \forall v \in M_n(F) \qquad \varphi\left(\left(\sum_{i=1}^{m} \overline{h}_i v \overline{g}_i\right) u_j\right) = 0 \Leftrightarrow \\
&\Leftrightarrow \quad \forall v \in M_n(F) \qquad \sum_{i=1}^{m} \overline{h}_i v \overline{g}_i = 0.
\end{aligned}$$

Pertanto f è identità polinomiale per $M_n(F)$ se e solo se $f^* = \sum_{i=1}^{m} h_i x_j g_i$ è un'identità polinomiale per $M_n(F)$.

□

5.9 Proposizione. *Siano $n, t \in \mathbb{N}$, $j \in \underline{t}\rfloor$ e sia $f(x_1, \ldots, x_t) \in F\langle X\rangle$ un polinomio lineare in x_j e omogeneo. Allora f è un'identità polinomiale debole in senso stretto in x_j per $M_n(F)$ se e solo se f^* è un polinomio centrale per $M_n(F)$.*

Dimostrazione. "$\Rightarrow$" Sia $m \in \mathbb{N}$ e, per ogni $i \in \underline{m}\rfloor$, siano $g_i, h_i \in F\langle X\rangle$ tali che $deg^j(g_i) = deg^j(h_i) = 0$ e $f = \sum_{i=1}^{m} g_i x_j h_i$.
Poniamo

$$\begin{aligned}
p(x_1, \ldots, x_t, x_{t+1}) \quad :=& \quad f(x_1, \ldots, x_{j-1}, [x_j, x_{t+1}], x_{j+1}, \ldots, x_t) = \\
=& \quad \sum_{i=1}^{m} g_i(x_1, \ldots, x_t)[x_j, x_{t+1}] h_i(x_1, \ldots, x_t) = \\
=& \quad \sum_{i=1}^{m} g_i(x_1, \ldots, x_t) x_j x_{t+1} h_i(x_1, \ldots, x_t) + \\
& \quad - \sum_{i=1}^{m} g_i(x_1, \ldots, x_t) x_{t+1} x_j h_i(x_1, \ldots, x_t).
\end{aligned}$$

Per ogni $a, b \in M_n(F)$, $[a, b]$ è una matrice a traccia nulla e quindi p è un'identità polinomiale per $M_n(F)$. Calcoliamo la trasformata di Razmyslov di p rispetto a x_j:

$$\begin{aligned} p^* &= \sum_{i=1}^{m} x_{t+1} h_i(x_1,\dots,x_t) x_j g_i(x_1,\dots,x_t) + \\ &\quad - \sum_{i=1}^{m} h_i(x_1,\dots,x_t) x_j g_i(x_1,\dots,x_t) x_{t+1} = \\ &= x_{t+1} f^* - f^* x_{t+1} = [x_{t+1}, f^*]. \end{aligned}$$

Da **(5.8)** segue che p^* è identità polinomiale per $M_n(F)$ e quindi $[x_{t+1}, f^*]$ è un'identità polinomiale per $M_n(F)$. Inoltre se f^* fosse un'identità polinomiale per $M_n(F)$, allora, per **(5.8)**, anche f lo sarebbe perchè $(f^*)^* = f$. Ma ciò è impossibile per ipotesi e quindi f^* non è un'identità polinomiale per $M_n(F)$. Da **(5.3)** segue che f^* è centrale per $M_n(F)$.
"$\Leftarrow$" Analogamente.

□

Dalla proposizione precedente si evince che per costruire polinomi centrali è sufficiente determinare delle identità polinomiali deboli in senso stretto. Per far ciò in genere si ricorre al polinomio di Capelli:

5.10 Definizione. Per ogni $m \in \mathbb{N}$, il seguente polinomio

$$C_m(x_1,\dots,x_m,y_1,\dots,y_{m+1}) := \sum_{\pi \in S_m} (-1)^\pi y_1 x_{\pi(1)} y_2 x_{\pi(2)} \cdots y_m x_{\pi(m)} y_{m+1}$$

si dice *m-esimo polinomio di Capelli.*

Ovviamente, per ogni $m \in \mathbb{N}$, $deg(C_m) = 2m + 1$ e C_m è un polinomio multilineare. Inoltre si dimostra che C_m è alternante in $x_1,\dots,x_m$ e da ciò e da **(2.32)** segue:

5.11 Proposizione. *Per ogni $n \in \mathbb{N}$, il polinomio di Capelli C_{n^2+1} è un'identità polinomiale per $M_n(F)$.*

Dimostriamo, invece, che vale il seguente risultato:

5.12 Proposizione. *Per ogni $n \in \mathbb{N}$, il polinomio di Capelli C_{n^2} non è un'identità polinomiale per $M_n(F)$.*

Dimostrazione. Sia $R := \{e_{ij} \mid i,j \in \underline{n}\rfloor\}$ l'insieme delle matrici elementari e siano $m, n \in \mathbb{N}, i, j_1, i_1, \dots, j_m, i_m \in \underline{n}\rfloor, a_1,\dots,a_m \in M_n(F)$. Allora:
$C_m(a_1,\dots,a_m, e_{ii_1}, e_{j_1 i_2}, e_{j_2 i_3}, \dots, e_{j_{m-1} i_m}, e_{j_m i}) =$

$$= \sum_{\pi \in S_m} (-1)^\pi e_{ii_1} a_{\pi(1)} e_{j_1 i_2} a_{\pi(2)} \cdots a_{\pi(m-1)} e_{j_{m-1} i_m} a_{\pi(m)} e_{j_m i}.$$

Per ogni $k \in \underline{m}\rfloor$, sia $a^{\pi(k)}_{i_k j_k}$ l'elemento di posto (i_k, j_k) della matrice $a_{\pi(k)}$.
Allora:
$C_m(a_1, \ldots, a_m, e_{ii_1}, e_{j_1 i_2}, e_{j_2 i_3}, \ldots, e_{j_{m-1} i_m}, e_{j_m i}) =$

$$= \left(\sum_{\pi \in \mathcal{S}_m} (-1)^\pi a^{\pi(1)}_{i_1 j_1} a^{\pi(2)}_{i_2 j_2} \ldots a^{\pi(m)}_{i_m j_m} \right) e_{ii}.$$

Sia $b = (b_{hk}) \in M_m(F)$ tale che

$$\forall\, h, k \in \underline{m}\rfloor \qquad b_{hk} := a^h_{i_k j_k}.$$

Allora:

$$C_m(a_1, \ldots, a_m, e_{ii_1}, e_{j_1 i_2}, e_{j_2 i_3}, \ldots, e_{j_{m-1} i_m}, e_{j_m i}) = det(b) e_{ii}.$$

In particolare, se $m := n^2$, per ogni $h \in \underline{m}\rfloor$ basta porre $a_h := e_{i_h j_h}$ e si ottiene $det(b) = 1$. Pertanto

$$C_{n^2}(a_1, \ldots, a_m, e_{ii_1}, e_{j_1 i_2}, e_{j_2 i_3}, \ldots, e_{j_{m-1} i_m}, e_{j_m i}) = e_{ii} \neq 0$$

e quindi C_{n^2} non è un'identità polinomiale per $M_n(F)$.

□

Vediamo, ora, come si costruisce un polinomio centrale usando il metodo di Razmyslov.
Consideriamo lo spazio $sl_n(F)$ delle matrici di ordine n a traccia nulla. Si ha che $dim_F sl_n(F) = n^2 - 1$ e una base canonica di $sl_n(F)$ su F è la seguente:

$$B = \{e_{ij} \mid i, j \in \underline{n}\rfloor, i \neq j\} \cup \{e_{11} - e_{ii} \mid i \in \underline{n}\rfloor - \{1\}\},$$

dove, per ogni $i, j \in \underline{n}\rfloor$, e_{ij} è una matrice elementare.
Pertanto $C_{n^2}(x_1, \ldots, x_{n^2}, y_1, \ldots, y_{n^2+1})$ si annulla per ogni valutazione delle lettere $x_1, \ldots, x_{n^2}$ con matrici a traccia nulla e quindi è identità polinomiale debole per $M_n(F)$ in $x_1, \ldots, x_{n^2}$. Allora, considerate altre lettere $z_1, \ldots, z_{2(n^2-1)}$ e posto

$$f := C_{n^2}(x_1, [z_1, z_2], \ldots, [z_{2(n^2-1)-1}, z_{2(n^2-1)}], y_1, \ldots, y_{n^2+1}),$$

si ha che f è multilineare ed è un'identità polinomiale debole in x_1.
Facciamo vedere che f non è un'identità polinomiale per $M_n(F)$.
Osserviamo che

$$\forall\, i, j \in \underline{n}\rfloor, i \neq j \qquad e_{ij} = [e_{ii}, e_{ij}]$$

$$\forall\, i \in \underline{n}\rfloor - \{1\} \qquad e_{11} - e_{ii} = [e_{1i}, e_{i1}].$$

Allora, se $\overline{y}_1, \ldots, \overline{y}_{n^2+1} \in M_n(F)$ e $a_1, \ldots, a_{n^2-1}$ sono gli elementi di B, poniamo

$$\overline{f} := C_{n^2}(e_{11}, a_1, \ldots, a_{n^2-1}, \overline{y}_1, \ldots, \overline{y}_{n^2+1}).$$

Siano $j \in \underline{n^2-1}\rfloor$ e $i \in \underline{n}\rfloor - \{1\}$ tali che $a_j := e_{11} - e_{ii}$. Poiché il polinomio di Capelli è alternante rispetto alle prime n^2 lettere, si ha:

$$\begin{aligned}\overline{f} &= C_{n^2}(e_{11}, a_1, \ldots, a_{j-1}, e_{11} - e_{ii}, a_{j+1}, \ldots, a_{n^2-1}, \overline{y}_1, \ldots, \overline{y}_{n^2+1}) = \\ &= -C_{n^2}(e_{11}, a_1, \ldots, a_{j-1}, e_{ii}, a_{j+1}, \ldots, a_{n^2-1}, \overline{y}_1, \ldots, \overline{y}_{n^2+1}).\end{aligned}$$

Segue che esistono $(i_1, j_1), \ldots, (i_{n^2-1}, j_{n^2-1}) \in (\underline{n}\rfloor)^2 - (1,1)$ tali che

$$\overline{f} = (-1)^{n-1} C_{n^2}(e_{11}, e_{i_1 j_1}, e_{i_2 j_2}, \ldots, e_{j_{n^2-1} i_{n^2-1}}, \overline{y}_1, \ldots, \overline{y}_{n^2+1}).$$

Come nella dimostrazione di (**5.12**), è possibile scegliere $\overline{y}_1, \ldots, \overline{y}_{n^2+1}$ tra le matrici elementari in modo tale che quest'ultima valutazione sia non nulla. Pertanto f è un'identità polinomiale debole in senso stretto per $M_n(F)$ in x_1 e così, per (**5.9**), f^* è un polinomio centrale per $M_n(F)$.
Si noti che il polinomio ottenuto risulta centrale in $M_n(F)$ qualunque sia il campo F.

CAPITOLO 6

IL TEOREMA DI POSNER

Il Teorema di Posner può essere riguardato come una generalizzazione del teorema sugli anelli commutativi affermante che per ogni dominio d'integrità esiste, a meno di isomorfismi, un unico campo dei quozienti.
La dimostrazione originale del Teorema di Posner usa il Teorema di Goldie e la localizzazione non commutativa attraverso la condizione di Ore. Noi, invece, vedremo la dimostrazione data da L. H. Rowen che si basa su un suo teorema riguardante gli ideali di PI-algebre prime, su un teorema di Levitzki sugli ideali nil di PI-algebre prime e su un teorema di Amitsur sul radicale di Jacobson di anelli polinomiali.
Infine vedremo alcune applicazioni del Teorema di Posner alle PI-algebre e ai T-ideali dell'algebra libera.

6.1 Definizione. Un anello R è *primo* se e solo se, per ogni I, J ideali non nulli di R, si ha $IJ \neq 0$.
Analogamente una C-algebra R si dice *prima* se e solo se, per ogni I, J ideali non nulli di R, vale $IJ \neq 0$.
Un ideale I di R è un *ideale primo* se la struttura quoziente (anello o algebra) è prima.

Vediamo una caratterizzazione delle algebre prime:

6.2 Proposizione. *Sia R una C-algebra. R è un'algebra prima se e solo se*

$$\forall\, a, b \in R \qquad aRb = 0 \Rightarrow a = 0 \text{ o } b = 0.$$

Dimostrazione. "$\Rightarrow$" Supponiamo che R sia algebra prima e siano $a, b \in R$ tali che $aRb = 0$. Allora $(RaR)(RbR) = 0$ e, poiché RaR e RbR sono ideali di R, dall'ipotesi segue che $RaR = 0$ oppure $RbR = 0$. Nel primo caso aR risulta un ideale bilatero di R e quindi $aR = 0$. Analogamente si ha $Ra = 0$

e quindi $\mathbb{Z}a$ è bilatero in R. Essendo $\mathbb{Z}aR = 0$ segue $a = 0$.
"$\Leftarrow$" Supponiamo che

$$\forall\, a, b \in R \qquad aRb = 0 \Rightarrow a = 0 \text{ o } b = 0.$$

Siano I, J ideali non nulli di R e siano $a \in I - \{0\}$, $b \in J - \{0\}$. Allora dall'ipotesi segue che $aRb \neq 0$ e quindi, essendo $aRb \subseteq IJ$, si ha $IJ \neq 0$. Pertanto R è un'algebra prima.

□

La caratterizzazione precedente mostra che una C-algebra R è prima se e solo se lo è come anello.

6.3 Proposizione. *Sia R un anello primo che non sia dominio d'integrità. Allora esiste $s \in R$ tale che $s \neq 0$ e $s^2 = 0$.*

Dimostrazione. Siano $a, b \in R - \{0\}$ tali che $ab = 0$. Allora, per **(6.2)**, $bRa \neq 0$ e quindi esiste $r \in R$ tale che $bra \neq 0$. Posto $s := bra$ si ha che $s \in R$, $s \neq 0$ e

$$s^2 = (bra)^2 = (bra)(bra) = br(ab)ra = 0.$$

□

Nel caso commutativo la definizione di anello primo equivale alla definizione di dominio d'integrità in quanto vale la seguente proposizione:

6.4 Proposizione. *Sia R un anello primo. Allora ogni elemento del suo centro è regolare in R.*

Dimostrazione. Siano R un anello, $Z(R)$ il suo centro, $z \in Z(R)$ e $a \in R$ tali che $z \neq 0$ e $za = 0$. Allora $Rza = 0$ e quindi, essendo $z \in Z(R)$, $zRa = 0$. Poiché R è primo, da **(6.2)** segue che $a = 0$.

□

6.5 Osservazione. Ogni anello primitivo è primo. Infatti siano R un anello primitivo, M un R-modulo fedele irriducibile e I, J ideali non nulli di R. Allora JM è un sottomodulo di M ed è non nullo perché M è fedele. Dall'irriducibilità di M segue che $JM = M$ e quindi $IJM = IM$. Ma anche $IM \neq 0$ e così $IJM \neq 0$, cioè $IJ \neq 0$.

Si dimostra che ogni dominio d'integrità può essere riguardato come il centro di un anello primitivo.

6.6 Definizione. Sia R un anello primo tale che $Z(R) \neq 0$. Posto

$$S := \{(r, z) \mid r \in R, z \in Z(R) - \{0\}\},$$

definiamo su S la seguente relazione d'equivalenza:

$$\forall\, (r, z), (s, t) \in S \qquad (r, z) \sim (s, t) \Leftrightarrow tr = zs.$$

Sia $Q(R) := S / \sim$ e, per ogni $(s,t) \in S$, indichiamo con $t^{-1}s$ la classe di equivalenza di (s,t). Per ogni $z_1^{-1}a_1, z_2^{-1}a_2 \in Q(R)$, definiamo le operazioni di addizione e moltiplicazione in $Q(R)$ nel seguente modo:

$$z_1^{-1}a_1 + z_2^{-1}a_2 := (z_1z_2)^{-1}(z_2a_1 + z_1a_2)$$

$$(z_1^{-1}a_1)(z_2^{-1}a_2) := (z_1z_2)^{-1}a_1a_2.$$

Con tali operazioni $Q(R)$ risulta essere un anello detto *anello dei quozienti centrali di R.*
Naturalmente , se R è una C-algebra, anche $Q(R)$ è un'algebra su C con moltiplicazione definita nel seguente modo:

$$\forall\, \alpha \in C, z^{-1}r \in Q(R) \qquad \alpha(z^{-1}r) := z^{-1}(\alpha r).$$

6.7 Proposizione. *Sia R un anello primo con centro non nullo. Allora R e $Q(R)$ soddisfano le stesse identità polinomiali a coefficienti in $Z(R)$.*

Dimostrazione. Ovviamente R soddisfa tutte le identità polinomiali di $Q(R)$ perché R può essere riguardato come un sottoanello di $Q(R)$. Dimostriamo che vale il viceversa.
Se $Z(R)$ è finito allora è un campo in quanto, per **(6.4)**, $Z(R)$ è un dominio d'integrità finito. Allora $Q(R) \cong R$ e la tesi è banalmente vera.
Supponiamo, ora, che $Z(R)$ sia infinito. Allora, essendo privo di divisori dello zero in R, $Z(R)$ soddisfa la condizione di regolarità. Analogamente a quanto fatto per **(2.18)**, usando l'argomento di Vandermonde si prova che ogni identità polinomiale per R è multiomogenea.
Dimostriamo, ora, che ogni identità polinomiale per R multiomogenea è un'identità polinomiale anche per $Q(R)$. Proviamo ciò per induzione sullo ordine lessicografico del multigrado dell'identità multiomogenea considerata.
Osserviamo innanzitutto che

$$Q(R) \cong R \bigotimes_{Z(R)} Q(Z(R)) \qquad (\star)$$

e quindi, se f è un'identità polinomiale multilineare per R, da **(3.2)** segue che f è un'identità polinomiale anche per $Q(R)$.
Sia $n \in \mathbb{N}$ e sia $f(x_1, \ldots, x_n) \in (Z(R))\langle X\rangle$ un'identità polinomiale multiomogenea per R.
Supponiamo vera la tesi per ogni identità polinomiale multiomogenea avente multigrado minore di quello di f nell'ordine lessicografico.
Per ogni $i \in \underline{n}\rfloor$ tale che $deg^i(f) > 1$, sia $k_i \in \mathbb{N}$ e poniamo $g_i := \Delta_{i,k_i}(f)$. Allora g_i è multiomogeneo ed ha multigrado minore rispetto a f. Inoltre, per **(2.25(1))**, g_i è un'identità polinomiale per R e quindi, per l'ipotesi induttiva, g_i è un'identità polinomiale per $Q(R)$.

Allora, per ogni $a_1, \ldots, a_n, a_{n+1} \in Q(R)$, $g_i(a_1, \ldots, a_n, a_{n+1}) = 0$ e quindi $f(a_1, \ldots, a_{i-1}, a_i + a_{n+1}, a_{i+1}, \ldots, a_n) =$

$$= f(a_1, \ldots, a_n) + f(a_1, \ldots, a_{i-1}, a_{n+1}, a_{i+1}, \ldots, a_n) \qquad (\star\star)$$

Siano $c_1, \ldots, c_n \in Q(R)$. Allora, per $(\star)$, per ogni $j \in \underline{n}\rfloor$, esistono $r_j \in \mathbb{N}$, $i_j \in \underline{r_j}\rfloor$, $a_{i_j}^{(j)} \in R$ e $b_{i_j}^{(j)} \in Q(Z(R))$ tali che

$$c_j = \sum_{i_j=1}^{r_j} a_{i_j}^{(j)} \otimes b_{i_j}^{(j)}.$$

Pertanto da $(\star\star)$ segue

$$f(c_1, \ldots, c_n) = \sum_{i_1, \ldots, i_n = 1}^{r_1, \ldots, r_n} f\left(a_{i_1}^{(1)} \otimes b_{i_1}^{(1)}, \ldots, a_{i_n}^{(n)} \otimes b_{i_n}^{(n)}\right).$$

Poiché f è multiomogeneo e i $b_{i_j}^{(j)}$ commutano, esistono $m_1, \ldots, m_n \in \mathbb{N}$ tali che

$$f(c_1, \ldots, c_n) = \sum_{i_1, \ldots, i_n = 1}^{r_1, \ldots, r_n} \left(f\left(a_{i_1}^{(1)}, \ldots, a_{i_n}^{(n)}\right) \otimes \left(b_{i_1}^{(1)}\right)^{m_1} \cdots \left(b_{i_n}^{(n)}\right)^{m_n}\right).$$

Ma f è un'identità polinomiale per R e quindi $f\left(a_{i_1}^{(1)}, \ldots, a_{i_n}^{(n)}\right) = 0$. Pertanto $f(c_1, \ldots, c_n) = 0$ e, per l'arbitrarietà di $c_1, \ldots, c_n$ in $Q(R)$, f è un'identità polinomiale per $Q(R)$.

□

La procedura seguita nella dimostrazione precedente prova che:

6.8 Proposizione. *Siano F un campo infinito e R una F-algebra. Se K è un'estensione di F allora R e $R \bigotimes_F K$ soddisfano le stesse identità polinomiali.*

Dimostrazione. Sia $f \in F\langle X \rangle$ un'identità polinomiale per R. Da **(2.30(1))** segue che f è equivalente alle sue componenti multiomogenee e quindi, senza perdere di generalità, possiamo supporre che f sia multiomogeneo.
Procedendo in modo analogo a quanto fatto per **(6.7)**, si dimostra che f è un'identità polinomiale per $R \bigotimes_F K$.
Infine, essendo K-algebra unitaria, R può essere riguardata come sottoalgebra di $R \bigotimes_F K$ e quindi R soddisfa tutte le identità polinomiali di $R \bigotimes_F K$.

□

6.9 Corollario. *Siano $n \in \mathbb{N}$ e A un'algebra semplice di dimensione n^2 sul suo centro F. Allora A e $M_n(F)$ soddisfano le stesse identità polinomiali.*

Dimostrazione. Osserviamo innanzitutto che per **(4.7)** $dim_F A$ è un quadrato.
Per il Teorema di Wedderburn-Artin, esistono $r \in \mathbb{N}$ e un corpo D tali che $A \cong M_r(D)$. Inoltre, per **(4.7)**, esiste $t \in \mathbb{N}$ tale che $t^2 = dim_F D$ e $n = rt$.
Se F è un campo finito, allora D è un corpo finito perché spazio vettoriale di dimensione finita su F. Allora D è commutativo e quindi $D = F$. Segue che $t = 1$ e così $n = r$. Pertanto $A \cong M_r(D) = M_n(F)$ e quindi A e $M_n(F)$ soddisfano le stesse identità polinomiali.
Supponiamo, ora, che F sia infinito e sia K un sottocampo massimale di D. Allora, essendo K commutativo e F infinito, per **(6.8)**, $A \otimes_F K$ soddisfa le stesse identità polinomiali di A. Inoltre

$$\begin{aligned} A \bigotimes_F K &\cong M_r(D) \bigotimes_F K \cong M_r(F) \bigotimes_F \left(D \bigotimes_F K \right) \cong \\ &\cong M_r(F) \bigotimes_F M_t(K) \cong M_{rt}(K) \cong M_{rt}(F) \bigotimes_F K. \end{aligned}$$

Per **(6.8)**, $M_{rt}(F) \otimes_F K$ soddisfa le stesse identità polinomiali di $M_{rt}(F)$ e quindi $A \otimes_F K$ soddisfa le stesse identità polinomiali di $M_{rt}(F) = M_n(F)$. □

6.10 Corollario. *Siano $n \in \mathbb{N}$ e A un'algebra semplice di dimensione n^2 sul suo centro F. Allora ogni polinomio centrale per $M_n(F)$ è centrale anche per A.*

Enunciamo, ora, il Teorema di Posner:

6.11 Teorema. ***(Teorema di Posner [15])***
Sia R una C-algebra prima soddisfacente un'identità polinomiale propria in $C\langle X\rangle$. Allora

(1) $Z(R) \neq 0$;

(2) L'anello dei quozienti centrali $Q(R)$ è un'algebra semplice di dimensione finita sul suo centro e il centro è il campo dei quozienti $Q(Z(R))$ del centro di R;

(3) R e $Q(R)$ soddisfano le stesse identità polinomiali in $C\langle X\rangle$.

Come già accennato all'inizio del capitolo, per la dimostrazione di tale teorema sfrutteremo tre risultati dovuti ad Amitsur, Levitzki e Rowen.
Prima di enunciare il teorema di Amitsur è necessario introdurre i concetti di radicale primo, di radicale di Jacobson e di elemento quasi regolare:

6.12 Definizione. Sia R un anello. Si dice *radicale primo di R* il seguente ideale:

$$P(R) := \bigcap_{\substack{P \text{ ideale} \\ \text{primo di } R}} P.$$

Se non esistono ideali primi in R allora $P(R) := R$.

6.13 Proposizione. *Il radicale primo di un anello R è un ideale nil.*

Dimostrazione. Se R è un anello nil la conclusione è ovvia. Pertanto, sia $a \in R$ un elemento non nilpotente e poniamo

$$S := \{a^n \mid n \in \mathbb{N}\}$$

$$T := \{J \mid J \text{ ideale di } R, J \cap S = \emptyset\}.$$

Sicuramente $T \neq \emptyset$ perché l'ideale nullo appartiene a T. Inoltre T è ordinato per inclusione e quindi, per il Lemma di Zorn, esiste $I \in T$ elemento massimale in T. Dimostriamo che I è un ideale primo di R.
Siano $\overline{I}_1, \overline{I}_2$ ideali di R/I tali che $\overline{I}_1\overline{I}_2 = 0$. Per il Teorema di corrispondenza per gli anelli, esistono I_1 e I_2 ideali di R contenenti I e tali che $I_1 I_2 \subseteq I$. Allora, poiché I è massimale in T, si ha che $I_1 = I$ oppure $I_1 \cap S = \emptyset$ e $I_2 = I$ oppure $I_2 \cap S = \emptyset$. Supponiamo che $I \subsetneqq I_1$ e $I \subsetneqq I_2$ e siano $n_1, n_2 \in \mathbb{N}$ tali che $a^{n_1} \in I_1$ e $a^{n_2} \in I_2$. Allora

$$a^{n_1+n_2} \in I_1 I_2 \subseteq I$$

e ciò è impossibile perché $I \in T$. Pertanto $I_1 = I$ oppure $I_2 = I$e quindi R/I è un anello primo. Segue che I è un ideale primo e, in particolare, che $P(R) \subseteq I$.
Poiché $I \cap S = \emptyset$, si ha che $a \notin I$ e $a \notin P(R)$. Quindi, per l'arbitrarietà di a come elemento non nilpotente di R, $P(R)$ può contenere solo elementi nilpotenti, cioè $P(R)$ è un ideale nil. □

6.14 Definizione. Sia R un anello. Si dice *radicale di Jacobson di R* il seguente ideale:

$$J(R) := \bigcap_{\substack{M \ R-\text{modulo} \\ \text{irriducibile}}} Ann_R(M).$$

Se non esistono R-moduli irriducibili allora $J(R) := R$.

6.15 Osservazione. Se R è un anello commutativo unitario allora

$$J(R) = \bigcap_{\substack{I \text{ ideale} \\ \text{massimale} \\ \text{di } R}} I.$$

6.16 Definizione. Un anello R si dice *semisemplice* (o *semiprimitivo*) se e solo se $J(R) = 0$.

6.17 Definizione. Siano R un anello e $a \in R$. a si dice *quasi regolare a sinistra* se e solo se esiste $b \in R$ tale che $a + b + ba = 0$. b è il *quasi inverso sinistro* di a.
Analogamente, si dice che a è *quasi regolare a destra* se e solo se esiste $c \in R$ tale che $a + c + ac = 0$ e c si dice *quasi inverso destro* di a.
Infine, a è *quasi regolare* se è quasi regolare a sinistra e a destra.

Se L è un ideale (destro, sinistro o bilatero) di R, L è un *ideale quasi regolare a sinistra* se ogni suo elemento è quasi regolare a sinistra. Analogamente si definiscono gli ideali quasi regolari a destra e quelli quasi regolari.

6.18 Osservazione. Siano R un anello e L un ideale sinistro di R quasi regolare a sinistra. Allora $L \subseteq J(R)$.
Infatti sia M un R-modulo irriducibile e dimostriamo che $LM = 0$. Supponiamo che $LM \neq 0$. Allora esiste $v \in M$ tale che $Lv \neq 0$, cioè Lv è un sottomodulo non nullo di M. Dall'irriducibilità di M segue che $Lv = M$ e quindi esiste $a \in L$ tale che $av = -v$. Per l'ipotesi su L, a è quasi regolare a sinistra e sia $b \in R$ il quasi inverso sinistro di a. Allora $0 = (a + b + ba)v = -v$ che è impossibile perché altrimenti $Lv = 0$. Pertanto $LM = 0$ e quindi $L \subseteq J(R)$.

6.19 Proposizione. *Sia R un anello. Allora*

(1) *$J(R)$ è un ideale quasi regolare di R;*

(2) *$J(R)$ è l'intersezione di tutti gli ideali sinistri (o destri) di R quasi regolari a sinistra (a destra).*

Segue che $J(R)$ è il più grande ideale quasi regolare a sinistra (e a destra).

6.20 Osservazione. Siano R un anello unitario e $a \in R$. a è quasi regolare se e solo se $1 + a$ è invertibile in R. In particolare se b è il quasi inverso di a allora l'inverso di $1 + a$ è $1 + b$.

6.21 Proposizione. *Siano R un anello commutativo, $f \in R[x]$ e $a_0, \ldots, a_n \in R$ tali che $f = a_0 + a_1x + \ldots + a_nx^n$. Se f è quasi regolare in $R[x]$ allora a_0 è quasi regolare in R e $a_1, \ldots, a_n$ sono nilpotenti.*

Dimostrazione. Sia $g := b_0 + b_1x + \ldots + b_nx^n \in R[x]$ il quasi inverso di f. Allora $f + g + gf = 0$ e $f + g + fg = 0$ e quindi $a_0 + b_0 + b_0a_0 = 0$ e $a_0 + b_0 + a_0b_0 = 0$, cioè a_0 è quasi regolare in R.
Se $P(R) = R$ allora, per **(6.13)**, ogni elemento di R è nilpotente. Pertanto, sia $P \neq R$ un ideale primo di R e poniamo

$$\forall i \in \underline{n}\rfloor \cup \{0\} \qquad \overline{a}_i := a_i + P$$

e

$$\overline{f} := \overline{a}_0 + \overline{a}_1x + \ldots + \overline{a}_nx^n \in (R/P)[x].$$

Se F è il campo dei quozienti di R/P, poiché f è quasi regolare in $R[x]$, $\overline{f}$ è quasi regolare in $(R/P)[x] \subseteq F[x]$. Allora da **(6.20)** segue che $1 + \overline{f}$ è invertibile in $F[x]$. Ma un polinomio a coefficienti in un campo è invertibile se e solo se è un elemento non nullo del campo e quindi $1 + \overline{f} = 1 + \overline{a}_0$, $1 + \overline{a}_0$ è invertibile in F e, per ogni $i \in \underline{n}\rfloor$, $\overline{a}_i = 0$. Allora, per ogni $i \in \underline{n}\rfloor$, $a_i \in P$ e così

$$\forall i \in \underline{n}\rfloor \qquad a_i \in \bigcap_{\substack{J \text{ ideale} \\ \text{primo di } R}} J = P(R)$$

Ma $P(R)$ è un ideale nil di R e quindi $a_1, \ldots, a_n$ sono nilpotenti.

□

6.22 Proposizione. *Siano R un anello, $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$ quasi regolare in $R[x]$ e $g = b_0+b_1x+\ldots+b_nx^n \in R[x]$ il quasi inverso di f in $R[x]$. Allora $b_1, \ldots, b_n$ appartengono al sottoanello generato da $a_0, a_1, \ldots, a_n$ e da b_0.*

Dimostrazione. Per ipotesi $f+g+gf = 0$ e $f+g+fg = 0$. Per ogni $k \in \underline{n}\rfloor$, il coefficiente di x^k in $f+g+gf$ è $a_k + b_k + \sum_{i=1}^{k} a_ib_{k-i} + a_0b_k$ e quindi

$$b_k + a_0b_k = -a_k - \sum_{i=1}^{k} a_ib_{k-i}.$$

Dalla quasi regolarità di a_0 segue:

$$b_k = -a_k - \sum_{i=1}^{k} a_ib_{k-i} + b_0\left(- a_k - \sum_{i=1}^{k} a_ib_{k-i}\right).$$

Procedendo per induzione su k si ottiene la tesi.

□

6.23 Teorema. ***(Amitsur [1])***
Sia R un anello privo di nil ideali non nulli e sia $J(R[t])$ il radicale di Jacobson dell'anello dei polinomi $R[t]$. Allora $J(R[t]) = 0$, cioè $R[t]$ è semisemplice.

Dimostrazione. Sia $f \in J(R[t]) - \{0\}$ con supporto di ordine minimo in $J(R[t])$, cioè f ha il minor numero di coefficienti non nulli tra i polinomi di $J(R[t])$. Siano $n \in \mathbb{N}, a_0, a_1, \ldots, a_n \in R$ tali che $a_n \neq 0$ e

$$f = a_0 + a_1t + \ldots + a_nt^n.$$

Siano $i, j \in \underline{n}\rfloor$ tali che $a_i \neq 0$ e $a_j \neq 0$. Allora

$$C_R(a_i) = C_R(a_j), \tag{$\star\star\star$}$$

cioè i centralizzanti in R di a_i e di a_j coincidono. Infatti, se $b \in C_R(a_i)$, $bf - fb \in J(R[t])$ e, per la minimalità del supporto di f in $J(R[t]) - \{0\}$, si ha $bf - fb = 0$, cioè $bf = fb$. Pertanto $ba_j = a_jb$ e così $b \in C_R(a_j)$. Analogamente si dimostra che $C_R(a_j) \subseteq C_R(a_i)$ e quindi $C_R(a_i) = C_R(a_j)$. Per **(6.19(1))**, $J(R[t])$ è quasi regolare e quindi f è quasi regolare. Sia $g \in R[t]$ il quasi inverso di f. Se R_0 è il sottoanello generato dai coefficienti di f e dal termine noto di g, allora, per **(6.22)**, esistono $b_0, b_1, \ldots, b_n \in R_0$ tali che $g = b_0 + b_1t + \ldots + b_nt^n$.
Da $(\star\star\star)$ segue che R_0 è commutativo e quindi, poichè $f \in R_0[t]$, da **(6.21)** segue che a_0 è quasi regolare in R_0 mentre $a_1, \ldots, a_n$ sono nilpotenti.

Supponiamo $n > 0$ e sia I l'ideale generato da a_n in R. Se $v \in I$, esistono $m \in \mathbb{N}$, $r, s, r_1, s_1, \ldots, r_m, s_m \in R, u \in \mathbb{Z}$ tali che

$$v = ra_n + a_n s + \sum_{i=1}^{m} r_i a_n s_i + u a_n.$$

Posto

$$h := rf + fs + \sum_{i=1}^{m} r_i f s_i + uf \in J(R[t]),$$

si ha che il numero dei coefficienti non nulli di h è non superiore al numero dei coefficienti non nulli di f. Inoltre v è il coefficiente di t^n in h e quindi, se $v \neq 0$, v è nilpotente perché h risulta avere supporto di ordine minimo. Pertanto I è nil e quindi dalle ipotesi segue $n = 0$.
Allora ogni polinomio di $J(R[t])$ con supporto di ordine minimo è costante e quindi $f = a_0$. Segue che, per ogni $b \in R$, $fbt = a_0 bt \in J(R[t])$ e, poiché deve essere un polinomio costante, $a_0 bt = 0$, cioè $a_0 b = 0$. Analogamente si dimostra che

$$\forall b \in R \qquad ba_0 = 0.$$

Segue che lo $\mathbb{Z}$-modulo $\mathbb{Z}a_0$ generato da a_0 è un ideale bilatero nil di R e quindi è nullo per l'ipotesi su R. Ma ciò è impossibile perché $0 \neq a_0 \in \mathbb{Z}a_0$ e pertanto $J(R[t]) = 0$.

□

6.24 Teorema. *(Levitzki [14])*
Se R è una C-algebra prima soddisfacente un'identità polinomiale propria, allora R è privo di nil ideali non nulli.

Dimostrazione. Sia $\overline{f} \in C\langle X \rangle$ un'identità polinomiale propria per R. Applicando il metodo di multilinearizzazione si ottiene una nuova identità polinomiale multilineare f di R e, per **(2.24(2))**, f è propria. Allora sia $c \in C$ un coefficiente di f tale che $cR \neq 0$ e sia $n \in \mathbb{N}$ tale che $deg(f) = n$. Per ogni $\pi \in \overline{S}_n := S_n - \{id_{\underline{n}|}\}$, sia $\alpha_\pi \in C$ tale che

$$f(x_1, \ldots, x_n) = cx_1 \ldots x_n + \sum_{\pi \in \overline{S}_n} \alpha_\pi x_{\pi(1)} \ldots x_{\pi(n)}.$$

Dimostriamo il teorema per induzione sul grado n di f.
Se $n = 1$ allora $f = cx_1$. Ma f è un'identità polinomiale per R e quindi $cR = 0$ che è una contraddizione.
Supponiamo, ora, vera la tesi per ogni anello primo soddisfacente un'identità polinomiale di grado $n - 1$ e proviamola per n. Sia I un nil ideale di R non nullo e sia $a \in I - \{0\}$ tale che $a^2 = 0$.
Posto $L := Ra$ e $R_1 := L/(L \cap Ann_d(L))$, si ha che R_1 è un anello primo.
Inoltre $cR_1 \neq 0$ perché altrimenti $cRa \subseteq Ann_d(L)$ e perciò $RacRa = 0$. Ma $c \in C$ e quindi $cRaRa = 0$. Poiché R è primo e $a \neq 0$, si ha $cRa = 0$ e

così $cRRa = 0$. Sempre perché R è primo e $a \neq 0$, segue $cR = 0$ che è impossibile in quanto contraddice l'ipotesi su c. Pertanto $cR_1 \neq 0$.
Siano $g \in C\langle X\rangle$ tale che $deg^1(g) = 0$ e

$$h := \sum_{\substack{\pi\in\overline{S}_n\\ \pi(1)\neq 1}} \alpha_\pi x_{\pi(1)}\dots x_{\pi(n)}$$

tali che $f = x_1 g(x_2,\dots,x_n) + h(x_1,x_2,\dots,x_n)$.
Per ogni $r_1,r_2,\dots,r_n \in R$ si ha:

$$\begin{aligned} 0 &= f(ar_1, r_2a, r_3a,\dots,r_na) = \\ &= ar_1g(r_2a,\dots,r_na) + h(ar_1,r_2a,r_3a,\dots,r_na). \end{aligned}$$

Per ogni $\pi \in \overline{S}_n$ tale che $\pi(1) \neq 1$, sia $j_\pi \in \underline{n}] - \{1\}$ tale che $\pi(j_\pi) = 1$. Allora

$$h(x_1,x_2,\dots,x_n) = \sum_{\substack{\pi\in\overline{S}_n\\ \pi(1)\neq 1}} \alpha_\pi x_{\pi(1)}\dots x_{\pi(j_\pi-1)}x_1x_{\pi(j_\pi+1)}\dots x_{\pi(n)}$$

e quindi, essendo $a^2 = 0$,
$h(ar_1,r_2a,r_3a,\dots,r_na) =$

$$= \sum_{\substack{\pi\in\overline{S}_n\\ \pi(1)\neq 1}} \alpha_\pi(r_{\pi(1)}a)\dots(r_{\pi(j_\pi-1)}a)(ar_1)(r_{\pi(j_\pi+1)}a)\dots(r_{\pi(n)}a) = 0.$$

Pertanto $aRg(r_2a,\dots,r_na) = 0$ e così $g(r_2a,\dots,r_na) = 0$ in quanto R è primo e $a \neq 0$. Inoltre c è un coefficiente di g e quindi g è un'identità polinomiale multilineare propria per R_1 tale che $deg(g) = n-1$. Dall'ipotesi induttiva segue che R_1 è privo di nil ideali non nulli. Ma Ra è un nil ideale di R perché $Ra \subseteq I$. Allora R_1 è nil e quindi $R_1 = 0$.
Pertanto $Ra \subseteq Ann_d(Ra)$ e così $RaRa = 0$. Poiché R è primo $Ra = 0$, cioè $a = 0$ che è assurdo.
Segue che l'unico nil ideale di R è 0. □

6.25 Teorema. ***(Teorema di Rowen [20])***
Sia R una C-algebra prima soddisfacente un'identità polinomiale propria. Allora $I \cap Z(R) \neq 0$ per ogni I ideale bilatero non nullo di R.

Dimostrazione. Sia I un ideale bilatero non nullo di R e supponiamo dapprima che R sia primo e semisemplice. Allora $J(R) = 0$ e, se $\{P_\gamma\}_{\gamma\in\Gamma}$ è l'insieme di tutti gli ideali primitivi di R, da **(6.19(2))** segue che

$$\bigcap_{\gamma\in\Gamma} P_\gamma = 0.$$

Sia $f \in C\langle X\rangle$ un'identità polinomiale propria per R e sia $c \in C$ un coefficiente di f tale che $cR \neq 0$. Poniamo:

$$\Gamma_1 := \{\gamma \in \Gamma \mid cR \subseteq P_\gamma\}$$

$$\Gamma_2 := \Gamma - \Gamma_1 = \{\gamma \in \Gamma \,|\, cR \not\subseteq P_\gamma\}$$

$$I_1 := \bigcap_{\gamma \in \Gamma_1} P_\gamma$$

$$I_2 := \bigcap_{\gamma \in \Gamma_2} P_\gamma.$$

Ovviamente $I_1 \cap I_2 = J(R)$ e quindi $I_1 \cap I_2 = 0$. Poiché $I_1 I_2 \subseteq I_1 \cap I_2 = 0$ e R è primo, $I_1 = 0$ oppure $I_2 = 0$. Se fosse $I_1 = 0$ allora $cR \subseteq I_1 = 0$ e ciò è impossibile perché per ipotesi $cR \neq 0$. Pertanto $I_2 = 0$ e così, posto

$$\forall \gamma \in \Gamma_2 \qquad R_\gamma := R/P_\gamma,$$

si ha che R è prodotto sottodiretto degli R_γ. Allora, per ogni $\gamma \in \Gamma_2$, f è un'identità polinomiale propria per R_γ e R_γ è un anello primitivo perché P_γ è un ideale primitivo. Pertanto sono verificate tutte le ipotesi del teorema di Kaplansky e così esiste $n_\gamma \in \mathbb{N}$ tale che R_γ è un'algebra semplice di dimensione n_γ^2 sul suo centro (che è un campo). Il teorema di Kaplansky fornisce anche un limite per tale dimensione in quanto abbiamo provato che $2n_\gamma \leq deg(f)$. Sia π_γ la γ-esima proiezione canonica e, posto

$$\overline{n} := max\{n_\gamma \,|\, \pi_\gamma(I) \neq 0\},$$

sia g il polinomio centrale di Razmyslov per $M_{\overline{n}}(\mathbb{Q})$. Allora, per ogni $\gamma \in \Gamma_2$ tale che $n_\gamma = \overline{n}$, g è centrale per R_γ mentre, per ogni $\gamma \in \Gamma_2$ tale che $n_\gamma < \overline{n}$, dal Teorema di Kaplansky e da **(5.4)** segue che g è un'identità polinomiale per R_γ .

Per ogni $\gamma \in \Gamma_2$, $\pi_\gamma(I)$ è un ideale bilatero di R_γ che è un anello semplice. Allora $\pi_\gamma(I) = 0$ oppure $\pi_\gamma(I) = R_\gamma$ e sicuramente esiste $\overline{\gamma} \in \Gamma_2$ tale che $\pi_{\overline{\gamma}}(I) \neq 0$ perché altrimenti si avrebbe $I = 0$. Segue:

$$\pi_\gamma(g(I)) = g(\pi_\gamma(I)) = \begin{cases} g(0) & \text{se } \pi_\gamma(I) = 0 \\ g(R_\gamma) & \text{se } \pi_\gamma(I) = R_\gamma \end{cases}$$

e $g(R_\gamma) = 0$ se $n_\gamma < \overline{n}$ e $0 \neq g(R_\gamma) \subseteq Z(R_\gamma)$ se $n_\gamma = \overline{n}$.

Segue che

$$\forall \gamma \in \Gamma_2 \qquad \pi_\gamma(g(I)) \subseteq Z(R_\gamma)$$

e quindi $g(I) \subseteq Z(R)$. Inoltre $g(I) \neq 0$. Infatti sia $\overline{\gamma} \in \Gamma_2$ tale che $n_{\overline{\gamma}} = \overline{n}$. Allora $\pi_{\overline{\gamma}}(I) = R_{\overline{\gamma}}$ e quindi

$$\pi_{\overline{\gamma}}(g(I)) = g(\pi_{\overline{\gamma}}(I)) = g(R_{\overline{\gamma}}) \neq 0,$$

cioè $g(I) \neq 0$.

Infine $g(I) \subseteq I$ perché I è bilatero e g è privo di termine noto. Pertanto

$$0 \neq g(I) \subseteq I \cap Z(R).$$

Abbiamo così dimostrato il teorema nel caso in cui R sia primo e semisemplice. Supponiamo, ora, che R sia solo primo e sia $f \in C\langle X\rangle$ un'identità polinomiale propria per R. Possiamo assumere che f sia multilineare, così, per **(3.2)**, f è un'identità polinomiale propria anche per $R[t]$ che risulta essere un anello primo. Da **(6.23)** e **(6.24)** segue che $J(R[t]) = 0$, cioè $R[t]$ è semisemplice. Pertanto, essendo $I[t]$ un ideale bilatero di $R[t]$, dalla prima parte della dimostrazione segue che

$$0 \neq I[t] \cap Z(R[t]) = I[t] \cap (Z(R))[t] = (I \cap Z(R))[t]$$

e quindi $I \cap Z(R) \neq 0$.

□

Possediamo, ora, tutti gli elementi utili per dimostrare il Teorema di Posner:

Dimostrazione del Teorema di Posner.
Da **(6.25)** segue subito che $Z(R) \neq 0$.
Consideriamo l'anello dei quozienti centrali di R:

$$Q(R) = \{z^{-1}r \mid r \in R, z \in Z(R) - \{0\}\}.$$

Si vede subito che $Q(R)$ è un'algebra prima e che il suo centro $Z(Q(R))$ è il campo dei quozienti di $Z(R)$.
Sia $f \in C\langle X\rangle$ un'identità polinomiale propria per R e sia $z \in Z(R)$ tale che $z \neq 0$. Allora $zf \in (Z(R))\langle X\rangle$ e quindi zf è un'identità polinomiale per R a coefficienti in $Z(R)$. Per **(6.7)**, zf è un'identità polinomiale anche per $Q(R)$ ed è propria perché $zR \neq 0$ in quanto $Z(R)$ è privo di divisori dello zero in R.
Pertanto $Q(R)$ verifica tutte le ipotesi di **(6.25)** e quindi, se I è un ideale bilatero non nullo di $Q(R)$, si ha $I \cap Z(Q(R)) \neq 0$.
Sia $a \in I \cap Z(Q(R))$ tale che $a \neq 0$. Essendo $Z(Q(R))$ un campo e I un ideale, $1 = a^{-1}a \in I$ e quindi $I = Q(R)$. Pertanto $Q(R)$ è un'algebra semplice sul suo centro $Z(Q(R)) = Q(Z(R))$. Il fatto che la dimensione di $Q(R)$ sul centro sia finita segue dal Teorema di Kaplansky.
Infine, poiché il centro di un anello primo è privo di divisori dello zero nell'anello, da **(6.7)** segue che, per un fissato polinomio $f \in C\langle X\rangle$ e per $0 \neq z \in Z(R) \subseteq Z(Q(R))$, vale:

$$f \in T(R) \Leftrightarrow zf \in T(R) \Leftrightarrow zf \in T(Q(R)) \Leftrightarrow f \in T(Q(R))$$

□

Utilizzando il Teorema di Posner, possiamo dare, ora, una dimostrazione del seguente importante risultato dovuto ad Amitsur.

6.26 Teorema. ***(Amitsur [2])***
Sia R una PI-algebra su C. Allora esistono $m, d \in \mathbb{N}$ tali che R soddisfa $S_d(x_1, \ldots, x_d)^m$.

Prima di dimostrare il teorema facciamo alcune osservazioni. Innanzitutto ricordiamo la definizione di algebra con identità polinomiale data in (2.6):

Definizione. Sia A una C-algebra. A è un'algebra con identità polinomiale se e solo se esiste $f \in C\langle X\rangle$ tale che f sia identità polinomiale per A e uno dei monomi di f di grado più alto abbia 1 come coefficiente.
Un'algebra con identità polinomiale si dice PI-algebra.

6.27 Osservazione. L'importanza della definizione precedente risiede soprattutto nel fatto che se A è una PI-algebra e f è un'identità polinomiale per A tale che uno dei monomi di f di grado più alto ha 1 come coefficiente, allora f continua ad essere una identità polinomiale propria anche per ogni quoziente di A mentre in generale ciò non è vero.

6.28 Osservazione. Siano F un campo, A una F-algebra e $f \in F\langle X\rangle$ tale che $f \neq 0$. Se f è un'identità polinomiale per A allora A è una PI-algebra. Infatti se $c \in F$ è un coefficiente di un monomio di f di grado più alto, allora $c^{-1}f$ è un'identità polinomiale per A e quindi A è una PI-algebra.

6.29 Osservazione. Se A è una C-algebra prima e $f \in C\langle X\rangle$ è un'identità polinomiale propria per A allora A è una PI-algebra. Infatti, per il Teorema di Posner, $Q(A)$ è un'algebra semplice di dimensione finita sul centro F. Pertanto per **(6.9)** esiste $n \in \mathbb{N}$ tale che $Q(A)$ e $M_n(F)$ soddisfano le stesse identità. Allora, per il Teorema di Amitsur-Levitzki, il polinomio standard $S_{2n}(x_1, \dots, x_{2n})$ è un'identità polinomiale per $Q(A)$ ed ha come coefficienti 1 e -1. Per **(6.11(3))**, A soddisfa $S_{2n}(x_1, \dots, x_{2n})$ e quindi A è una PI-algebra.

Dimostrazione di (6.26).
Sia $T(R)$ il T-ideale delle identità polinomiali di R in $C\langle X\rangle$ e poniamo $\overline{R} := C\langle X\rangle / T(R)$.
Come mostrato nella proposizione **(2.16)**, si ha $T(R) = T(\overline{R})$, cioè R e $\overline{R}$ sono PI-equivalenti.
In particolare $\overline{R}$ è una PI-algebra perché lo è R e quindi soddisfa un'identità polinomiale f avente 1 come coefficiente di uno dei suoi monomi di grado massimo.
Supponiamo ora $P(\overline{R}) \neq \overline{R}$, e sia P un ideale primo di $\overline{R}$. Allora $\overline{R}/P$ è un'algebra prima e, per **(6.27)**, soddisfa f. Per il Teorema di Posner, $Q(\overline{R}/P)$ soddisfa f ed è un'algebra centrale e semplice di dimensione finita sul suo centro F. Siano $n, d \in \mathbb{N}$ tali che $dim_F Q(\overline{R}/P) = n^2$ e $deg(f) = d$. Allora, per il corollario **(6.9)** e per il Teorema di Amitsur-Levitzki, $Q(\overline{R}/P)$ soddisfa $S_{2n}(x_1, \dots, x_{2n})$ e inoltre $2n \leq d$. Pertanto $Q(\overline{R}/P)$ soddisfa anche $S_d(x_1, \dots, x_d)$ e in particolare,

$$\forall r_1, \dots, r_d \in \overline{R} \qquad S_d(r_1, \dots, r_d) \in P.$$

Per l'arbitrarietà di P si ha

$$\forall r_1,\dots,r_d \in \overline{R} \qquad S_d(r_1,\dots,r_d) \in \bigcap_{\substack{P \text{ ideale} \\ \text{primo di } \overline{R}}} P = P(\overline{R}) \qquad (\Diamond)$$

Ma $P(\overline{R})$ è un ideale nil di $\overline{R}$. Poiché

$$S_d(x_1,\dots,x_d) + T(R) = S_d(x_1 + T(R),\dots,x_d + T(R)),$$

da $(\Diamond)$ segue che $S_d(x_1,\dots,x_d) + T(R)$ è nilpotente in $\overline{R}$. Pertanto esiste $m \in \mathbb{N}$ tale che $S_d(x_1,\dots,x_d)^m \in T(R)$, cioè R soddisfa una potenza del polinomio standard.

□

Vediamo, ora, un'applicazione del Teorema di Posner ai T-ideali primi.

6.30 Proposizione. *Siano K un campo infinito e I un T-ideale primo di $K\langle X\rangle$. Allora esiste $n \in \mathbb{N}$ tale che $I = T(M_n(K))$.*

Dimostrazione. Posto $R := K\langle X\rangle / I$, si ha che R è una PI-algebra prima e $T(R) = I$.
Dal Teorema di Posner segue che $T(R) = T(Q(R))$ e che esiste $n \in \mathbb{N}$ tale che $Q(R)$ è un'algebra centrale semplice di dimensione n^2 sul proprio centro L.
Per **(6.9)**, $T(Q(R)) = T(M_n(L))$ in $L\langle X\rangle$ e, poiché $K \subseteq L$ e

$$M_n(L) \cong L \bigotimes_K M_n(K),$$

da **(3.2)** segue che $T(M_n(L))) = T(M_n(K))$ in $K\langle X\rangle$.
Pertanto $T(R) = T(M_n(K))$ in $K\langle X\rangle$ e quindi $I = T(M_n(K))$.

□

6.31 Osservazione. Se K è un campo infinito, allora i T-ideali primi di $K\langle X\rangle$ costituiscono una catena discendente di T-ideali. Infatti, per **(2.38)**, $T(M_n(K)) \supset T(M_{n+1}(K))$ e quindi

$$T(M_1(K)) \supset T(M_n(K)) \supset \dots \supset T(M_n(K)) \supset \dots$$

Osserviamo che le inclusioni sono tutte strette in quanto, per il Teorema di Amitsur-Levitzki,

$$\forall n \in \mathbb{N} \qquad S_{2n}(x_1,\dots,x_{2n}) \in T(M_n(K)) - T(M_{n+1}(K)).$$

Da **(6.30)** segue la tesi.

6.32 Definizione. Sia K un campo di caratteristica zero e sia I un T-ideale di una K-algebra A. I è un *T-ideale T-primo* (o *K-primo* o *verbalmente primo*) di A se, per ogni I_1, I_2 T-ideali di A tali che $I_1 I_2 \subseteq I$ si ha $I_1 \subseteq I$ oppure $I_2 \subseteq I$.

6.33 Teorema. *(Kemer [11])*
Sia K un campo tale che $char(K) = 0$, sia $E = E_0 \bigoplus E_1$ l'algebra esterna su K generata da X e sia I un T-ideale di $K\langle X\rangle$. I è un T-ideale T-primo non banale di $K\langle X\rangle$ se e solo se si verifica una delle seguenti condizioni:

(1) *Esiste $n \in \mathbb{N}$ tale che $I = T(M_n(K))$;*

(2) *Esiste $n \in \mathbb{N}$ tale che $I = T(M_n(E))$;*

(3) *Esistono $k \in \mathbb{N}$, $l \in \underline{k}\rfloor$ tali che $I = T(M_{k,l}(E))$.*

dove con $M_{k,l}(E)$ si intende la sottoalgebra di $M_{k+l}(E)$ costituita dalle matrici a blocchi del seguente tipo:

$$A = \begin{pmatrix} B & C \\ D & F \end{pmatrix}$$

con $B \in M_k(E_0)$, $C, D \in M_{k\times l}(E_1)$ e $F \in M_l(E_0)$.

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 $Y := \left\{u_{ij}^{(k)} \mid ij \in \underline{n}\rfloor, k \in \mathbb{N}\right\}$ 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

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

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 $f(x_1,\dots,x_t) \in T(M_n(K))$. 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

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

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

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

Siano $r_1,\dots,r_t \in M_n(K)$ e, per ogni $k \in \underline{t}|$, $i,j \in \underline{n}|$, 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

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

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

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

Allora

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

Dall'arbitrarietà di $r_1,\dots,r_t$ 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 $K[x_1, \dots, x_n]$, cioè $L := K(x_1, \dots, x_n)$.
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

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

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 $m \in \mathbb{N}_0$, $a_0, a_1, \dots, a_n \in L$ 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

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

In particolare, se $b = 1$, allora

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

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 $i \equiv 0 (\text{mod } n)$.
Siano $r \in \underline{m}\rfloor \cup \{0\}$ e $b_0, b_1, \dots, b_r \in L$ tali che

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

Segue che

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

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

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

e quindi

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

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 $k \in \underline{n^2}\rfloor$, denotiamo 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 $k \in \underline{n^2}]$ e $i,j \in \underline{n}]$, 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 $\{e_{ij} \mid i,j \in \underline{n}]\}$ 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

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

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

$$y_5 := tr(UV)$$

BIBLIOGRAFIA

[1] S. A. Amitsur, *Radicals of polynomial rings*, Canadian J. Math. **8** (1956), 355-361.

[2] S. A. Amitsur, *The identities of PI-rings*, Proc. Amer. Math. Sc. **3** (1952), 27-34.

[3] S. A. Amitsur, *The T-ideals of the free ring*, J. London Math Soc. **30** (1955), 470-475.

[4] S. A. Amitsur and J. Levitzki, *Minimal identities for algebras*, Proc. Amer. Math. Soc. **2** (1950), 449-463.

[5] S. Franciosi e F. de Giovanni, *Elementi di Algebra*, Aracne Editrice, Roma, 1992.

[6] V. Drensky, *Free algebras and PI-algebras. Graduate course in algebra*, Springer, Singapore, 1999.

[7] T. W. Hungerford, *Algebra*, Holt, Rinehart and Winston, New York, 1974.

[8] N. Jacobson, *Basic Algebra I and II*, Second Edition, W. H. Freeman and Co., 1989.

[9] N. Jacobson, *PI-Algebras: An Introduction*, Lecture Notes in Mathematics 441, Springer-Verlag, Berlin, 1975.

[10] I. Kaplansky, *Rings with a polynomial identity*, Bull. Amer. Math. Soc. **54** (1948), 575-580.

[11] A. Kemer, *Ideals of identities of associative algebras*, Translations Math. Monographs **87**, Amer. Math. Soc., 1991.

[12] B. Kostant, *A theorem of Frobenius, a theorem of Amitsur-Levitzki and cohomology theory*, J. Math. Mech. **7** (1958), 237-264.

[13] T. Y. Lam, *A First Course in Noncommutative Rings*, Springer-Verlag, New York, 1991.

[14] J. Levitzki, *A theorem on polynomial identities*, Proc. Amer. Math. Soc. **1** (1950), 334-341.

[15] E. C. Posner, *Prime rings satisfying a polynomial identity*, Pro. Amer. Math. Soc. **11** (1960), 180-184.

[16] C. Procesi, *Non-commutative affine rings*, Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **8** (1967), 239-255.

[17] C. Procesi, *Rings with Polinomial Identities*, Marcel Dekker, New York, 1973.

[18] Y. P. Razmyslov, *Trace identities of full matrix algebras over a field of characteristic zero*, Izv. Akad. Nauk SSSR **38** (1974), 723-756 (Russian). Translation: Math. USSR-Izv. **8** (1974), 727-760.

[19] S. Rosset, *A new proof of the Amitsur-Levitzki identity*, Israel J. Math. **23** (1976), 187-188.

[20] L. H. Rowen, *On rings with central polynomials*, J. Algebra **31** (1974), 393-426.

[21] L. H. Rowen, *Ring Theory I and II*, Academic Press, New York, 1988.

[22] L. H. Rowen, *Polinomial Identities in Ring Theory*, Academic Press, New York, 1980.