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

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

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

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

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

2.2 Definizione. Sia $X = \{x_1, x_2, \ldots\}$ 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 $X = \{x_1, x_2, \ldots, x_n\}$, allora $C\langle X \rangle$ si indicherà col simbolo $C\langle x_1, x_2, \ldots, x_n \rangle$.
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 $X = \{x_1, x_2, \ldots\}$ 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:

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

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

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

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

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:

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

Siano $d \in \mathbb{N}$, $f = f(x_1, \ldots, x_d) \in C\langle X\rangle$ 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 $f(r_1, \ldots, r_d) := \psi(f)$.
Ovviamente $f(R) = \{f(r_1, \ldots, r_d) \,|\, \forall\, i \in \underline{d}\rfloor \quad r_i \in R\}$ essendo $C\langle X\rangle$ algebra libera su X. In particolare, se $R = C\langle X\rangle$, allora

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

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

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

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

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

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 $f(x_1, \ldots, x_m) \in C\langle X\rangle$. 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 $x_{i_1}, \ldots, x_{i_k}$ 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 $f = f(x_1, \ldots, x_m)$ e, per ogni $S \in \mathcal{P} := \mathcal{P}(\{x_1, \ldots, x_m\})$, 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 $T \subseteq S$ 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 $f(x_1, \ldots, x_t) \in C\langle X\rangle$. 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

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

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 $i, j \in \underline{n+1}\rfloor$ 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 $B := (\beta_{ij})_{i,j=1,\ldots,n+1}$ 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

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

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

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

□

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 $f = f(x_1, \ldots, x_m)$ e sia $n := deg^1(f)$. Per ogni $i \in \underline{n}\rfloor$, denotiamo con f_i la somma dei monomi di f di grado i in x_1. Allora

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

Poiché f è un'identità polinomiale,

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

e quindi

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

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

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

Iterando il procedimento per ogni $j \in \underline{m}\rfloor - \{1\}$ 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'identità 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'identità 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 $f(x_1, \ldots, x_m) \in F\langle X\rangle$ (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:

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

e quindi

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

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

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

e quindi

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

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 $i \in \underline{m}\rfloor - \{1\}$ 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 $m \in \mathbb{N}$, $f(x_1, \ldots, x_m) \in C\langle X\rangle$, $i \in \underline{m}\rfloor$ 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:

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

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 $M_t(C)$.

□