0.1 Anelli di polinomi in n variabili

Vogliamo ora estendere il concetto di anello di polinomi ad un numero finito di variabili.

Definizione

Sia n un intero positivo. Denotiamo con $M = \text{mon}\{x_1, \dots, x_n\}$ l'insieme dei monomi nelle variabili $x_1, \dots, x_n$, cioè $M = \{x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n} : \alpha_i \in \mathbb{N}_0\}$.

Presi due elementi $u = x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n}$ e $v = x_1^{\beta_1} \cdot \dots \cdot x_n^{\beta_n}$ di M, è possibile definire su M un'operazione binaria corrispondente al prodotto di monomi:

$$u \cdot v = x_1^{\alpha_1+\beta_1} \cdot \dots \cdot x_n^{\alpha_n+\beta_n}.$$

Osserviamo che M dotato di tale operazione è un monoide commutativo. Infatti,

- $u \cdot v = x_1^{\alpha_1+\beta_1} \cdot \dots \cdot x_n^{\alpha_n+\beta_n} \in M$ perché $\alpha_i + \beta_i \in \mathbb{N}_0$, cioè M è chiuso rispetto a $\cdot$
- tale operazione agisce sugli esponenti delle variabili $x_1, \dots, x_n$ mediante la somma, ed essendo tali esponenti in $\mathbb{N}_0$ e la somma associativa su $\mathbb{N}_0$, anche $\cdot$ è associativo
- esiste un elemento neutro $1_M = x_1^0 \cdot \dots \cdot x_n^0 \in M$
- $u \cdot v = x_1^{\alpha_1+\beta_1} \cdot \dots \cdot x_n^{\alpha_n+\beta_n} = x_1^{\beta_1+\alpha_1} \cdot \dots \cdot x_n^{\beta_n+\alpha_n} = v \cdot u$, cioè M è commutativo.

Per semplicità di notazione, sia $I_n = \{1, \dots, n\}$ e sia $\underline{\alpha} \colon I_n \to \mathbb{N}_0$ la funzione che associa alla i-esima variabile x_i l'esponente $\underline{\alpha}(i) = \alpha_i$. Denotiamo con $x^{\underline{\alpha}} = x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n} \in M$.

Esempio. Se $M = \text{mon}\{x_1, x_2, x_3, x_4\}$ e $\underline{\alpha} \colon \{1, 2, 3, 4\} \to \mathbb{N}_0$ è la funzione definita come $\underline{\alpha}(1) = 2$, $\underline{\alpha}(2) = \underline{\alpha}(3) = 1$ e $\underline{\alpha}(4) = 0$, abbiamo che $x^{\underline{\alpha}} = x_1^2 x_2^1 x_3^1 x_4^0 = x_1^2 x_2 x_3 \in M$. □

Detto $\mathcal{F} = \mathcal{F}(I_n, \mathbb{N}_0)$ l'insieme delle funzioni $\underline{\alpha} \colon I_n \to \mathbb{N}_0$,[1] vi è una corrispondenza biunivoca tra $\mathcal{F}$ e l'insieme dei monomi M. Infatti, ogni monomio $x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n}$ corrisponde in modo naturale all'unica funzione $\underline{\alpha} \in \mathcal{F}$ tale che $\underline{\alpha}(i) = \alpha_i$ per ogni $i \in I_n$, e ogni funzione $\underline{\beta} \in \mathcal{F}$ rappresenta univocamente il monomio $x_1^{\beta(1)} \cdot \dots \cdot x_n^{\beta(n)} \in M$.

Prima di procedere nella costruzione dei polinomi nelle variabili $x_1, \dots, x_n$, richiamiamo un importante concetto derivante dalla topologia e alcune sue proprietà.

Definizione

Siano X e Y insiemi non vuoti e sia $f \colon X \to Y$ una funzione. Si definisce supporto di f l'insieme $\text{supp}(f) = \{x \in X : f(x) \neq 0_Y\}$.

Esempio. Sia $f \colon \mathbb{Z} \to \mathbb{R}$ la funzione $f(x) = x^2 - 1$. Allora, $\text{supp}(f) = \mathbb{Z} \setminus \{\pm 1\}$. □

Se $|\text{supp}(f)| < \infty$, diciamo che f ha supporto finito. Si osservi che tale definizione ha senso solo se l'insieme Y contiene un elemento neutro 0_Y: nel nostro caso, avendo a che fare con anelli, è naturale identificare tale elemento con l'elemento neutro dell'addizione.

Esempio. Se $f \colon \text{Mat}_{2\times 2}(\mathbb{F}_2) \to \mathbb{F}_2$ è il determinante, allora f ha supporto finito perché $\text{supp}(f) = \text{GL}(2, \mathbb{F}_2) = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$.[2] □

[1] In generale, dati due insiemi X e Y, si denota con $\mathcal{F}(X, Y)$ l'insieme di tutte le funzioni $f \colon X \to Y$.
[2] Ricordiamo che $\text{GL}(n, \mathbb{K})$ è il gruppo delle matrici $n \times n$ invertibili con entrate nel campo $\mathbb{K}$.

Proposizione 1.2.1

Siano $f, g\colon X \to Y$ funzioni e siano $(f+g)(x) = f(x)+g(x)$ e $(f\cdot g)(x) = f(x)\cdot g(x)$. Allora, $\operatorname{supp}(f+g) \subseteq [\operatorname{supp}(f) \cup \operatorname{supp}(g)]$ e $\operatorname{supp}(f\cdot g) \subseteq [\operatorname{supp}(f) \cap \operatorname{supp}(g)]$.

Dimostrazione. Osserviamo che se $x \in \operatorname{supp}(f+g)$, allora per definizione $f(x)+g(x) \neq 0_Y$, cioè almeno uno tra $f(x)$ e $g(x)$ è non nullo e quindi $x \in [\operatorname{supp}(f) \cup \operatorname{supp}(g)]$.
Analogamente, se $x \in \operatorname{supp}(f\cdot g)$, per definizione abbiamo che $f(x)\cdot g(x) \neq 0_Y$, dunque $f(x) \neq 0_Y$ e $g(x) \neq 0_Y$, ossia $x \in [\operatorname{supp}(f) \cap \operatorname{supp}(g)]$. ■

Esempio. Siano $f, g\colon \mathbb{Z} \to \mathbb{R}$ le funzioni $f(x) = x^2 - 3x + 2$ e $g(x) = x^2 + x - 2$. Allora, è evidente che $\operatorname{supp}(f) = \mathbb{Z} \setminus \{1, 2\}$ e $\operatorname{supp}(g) = \mathbb{Z} \setminus \{1, -2\}$, ed essendo $(f+g)(x) = 2x^2 - 2x$ e $(f\cdot g)(x) = (x-1)^2(x-2)(x+2)$, abbiamo che

$$\operatorname{supp}(f+g) = \mathbb{Z} \setminus \{0, 1\} \subseteq \mathbb{Z} \setminus \{1\} = \operatorname{supp}(f) \cup \operatorname{supp}(g)$$

$$\operatorname{supp}(f\cdot g) = \mathbb{Z} \setminus \{1, \pm 2\} = \operatorname{supp}(f) \cap \operatorname{supp}(g)$$

in accordo con la *Proposizione 1.2.1.* □

Sia R un anello e sia $\mathcal{F}^\times(\mathcal{F}, R) = \{r\_ : \mathcal{F} \to R : |\operatorname{supp}(r\_)| < \infty\}$, cioè l'insieme di tutte le funzioni $r\_$ che associano ad ogni funzione $\underline{\alpha} \in \mathcal{F}$ un elemento $r_{\underline{\alpha}} \in R$ e che sono diverse dall'elemento neutro 0_R solo per un numero finito di elementi di $\mathcal{F}$. Possiamo quindi definire un polinomio nelle variabili $x_1, \dots, x_n$ ponendo

$$f(x_1, \dots, x_n) = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}}.$$

Infatti, $f(x_1, \dots, x_n)$ risulta essere la somma di un numero finito di monomi non nulli, ognuno con il relativo coefficiente $r_{\underline{\alpha}}$. Questo punto è fondamentale: abbiamo scelto $r\_ \in \mathcal{F}^\times(\mathcal{F}, R)$ con supporto finito così che soltanto un numero finito degli infiniti monomi di M abbia un coefficiente $r_{\underline{\alpha}} \neq 0_R$. Così facendo, nella sommatoria vi è solo un numero finito di elementi perché tutti gli infiniti altri sono nulli, dunque f è effettivamente un polinomio.

Esempio. Siano $M = \operatorname{mon}\{x, y\}$ e $R = \mathbb{Z}$. Detta $r\_ : \mathcal{F} \to \mathbb{Z}$ la funzione

$$r_{\underline{\alpha}} = \begin{cases} 2\underline{\alpha}(1) - \underline{\alpha}(2) & \text{se } \underline{\alpha}(1) + \underline{\alpha}(2) = 3 \\ 0 & \text{altrimenti} \end{cases}$$

al variare di $\underline{\alpha} \in \mathcal{F} = \mathcal{F}(I_2, \mathbb{N}_0)$, essendo $\underline{\alpha}(1) \geq 0$ e $\underline{\alpha}(2) \geq 0$, è evidente che esista solo un numero finito di funzioni $\underline{\alpha} \in \mathcal{F}$ per cui $\underline{\alpha}(1) + \underline{\alpha}(2) = 3$. In tutti gli altri casi abbiamo che $r_{\underline{\alpha}} = 0$, quindi $r\_$ ha supporto finito, cioè $r\_ \in \mathcal{F}^\times(\mathcal{F}, R)$. Se identifichiamo $\underline{\alpha}$ con la coppia $(\alpha_1, \alpha_2) = (\underline{\alpha}(1), \underline{\alpha}(2))$,[3] possiamo quindi definire il polinomio

$$\begin{aligned} f(x, y) &= \sum_{\underline{\alpha} \in \mathcal{F}} r_{(\alpha_1, \alpha_2)} x^{\alpha_1} y^{\alpha_2} \\ &= r_{(3,0)} x^3 y^0 + r_{(2,1)} x^2 y^1 + r_{(1,2)} x^1 y^2 + r_{(3,0)} x^3 y^0 + \dots \text{[4]} \\ &= (2\cdot 3 - 0) x^3 + (2\cdot 2 - 1) x^2 y + (2\cdot 1 - 2) x y^2 + (2\cdot 0 - 3) y^3 \\ &= 6x^3 + 3x^2 y - 3y^3. \ \square \end{aligned}$$

[3] Infatti $\mathcal{F}(I_n, \mathbb{N}_0) \cong \mathbb{N}_0^n$ mediante l'isomorfismo $\varphi\colon \mathcal{F}(I_n, \mathbb{N}_0) \to \mathbb{N}_0^n$, $\underline{\alpha} \mapsto (\underline{\alpha}(1), \dots, \underline{\alpha}(n))$.

[4] Tutti gli altri termini della sommatoria sono nulli perché $\underline{\alpha}(1) + \underline{\alpha}(2) \neq 3$ e quindi, per come abbiamo definito $r\_$, il coefficiente del monomio $x^{\alpha_1} y^{\alpha_2}$ è $r_{\underline{\alpha}} = 0$.

Possiamo procedere nella costruzione dell'anello dei polinomi nelle variabili $x_1, \dots, x_n$. Detto

$$R[x_1, \dots, x_n] = \left\{ \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}} : r_\_ \in \mathcal{F}^\times(\mathcal{F}, R) \right\}$$

vogliamo quindi introdurre su tale insieme delle operazioni binarie di somma e prodotto così che esso sia effettivamente un anello. Presi due elementi

$$f(x_1, \dots, x_n) = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}} \quad \text{e} \quad g(x_1, \dots, x_n) = \sum_{\underline{\beta} \in \mathcal{F}} s_{\underline{\beta}} x^{\underline{\beta}}$$

di $R[x_1, \dots, x_n]$, definiamo le operazioni di somma e prodotto

$$f(x_1, \dots, x_n) + g(x_1, \dots, x_n) = \sum_{\underline{\alpha} \in \mathcal{F}} (r_{\underline{\alpha}} + s_{\underline{\alpha}}) x^{\underline{\alpha}}$$

$$f(x_1, \dots, x_n) \cdot g(x_1, \dots, x_n) = \sum_{\underline{\gamma} \in \mathcal{F}} t_{\underline{\gamma}} x^{\underline{\gamma}}$$

dove abbiamo posto $t_{\underline{\gamma}} = \sum_{\underline{\alpha} + \underline{\beta} = \underline{\gamma}} r_{\underline{\alpha}} s_{\underline{\beta}}$. Anche in questo caso, tali operazioni non sono altro che la formalizzazione delle usuali operazioni di somma e prodotto tra polinomi.

Proposizione 1.2.2

Tali operazioni di somma e prodotto su $R[x_1, \dots, x_n]$ sono ben poste.

Dimostrazione. Nel caso della somma, è sufficiente mostrare che $(r_\_ + s_\_) \in \mathcal{F}^\times(\mathcal{F}, R)$, cioè che la somma di due funzioni in $\mathcal{F}^\times(\mathcal{F}, R)$ è ancora una funzione in $\mathcal{F}^\times(\mathcal{F}, R)$. Osserviamo che $(r_\_ + s_\_)(\underline{\alpha}) = r_{\underline{\alpha}} + s_{\underline{\alpha}} \in R$ per ogni $\underline{\alpha} \in \mathcal{F}$ essendo $r_{\underline{\alpha}}, s_{\underline{\alpha}} \in R$ e R chiuso rispetto alla somma in quanto anello, quindi $r_\_ + s_\_$ è effettivamente una funzione da $\mathcal{F}$ in R. Inoltre, per la *Proposizione 1.2.1* si ha che

$$\operatorname{supp}(r_\_ + s_\_) \subseteq [\operatorname{supp}(r_\_) \cup \operatorname{supp}(s_\_)]$$

e tale insieme è finito poiché unione di insiemi finiti. Dunque, $r_\_ + s_\_$ ha supporto finito, da cui concludiamo che $(r_\_ + s_\_) \in \mathcal{F}^\times(\mathcal{F}, R)$, cioè che $\mathcal{F}^\times(\mathcal{F}, R)$ è chiuso rispetto alla somma.

Nel caso del prodotto, dobbiamo mostrare che $t_\_ \in \mathcal{F}^\times(\mathcal{F}, R)$. Osserviamo innanzitutto che per ogni $\underline{\gamma} \in \mathcal{F}$ fissato, la somma

$$t_{\underline{\gamma}} = \sum_{\underline{\alpha} + \underline{\beta} = \underline{\gamma}} r_{\underline{\alpha}} s_{\underline{\beta}}$$

contiene un numero finito di addendi. Infatti, la condizione $\underline{\gamma} = \underline{\alpha} + \underline{\beta} \Rightarrow \underline{\gamma}(i) = \underline{\alpha}(i) + \underline{\beta}(i)$ per ogni $i \in I_n$ implica che $0 \leq \underline{\alpha}(i) \leq \underline{\gamma}(i)$, dunque abbiamo un numero finito di scelte per ogni $\underline{\alpha}(i)$ e quindi anche per $\underline{\alpha}$. Essendo $t_{\underline{\gamma}}$ la somma di un numero finito di prodotti $r_{\underline{\alpha}} s_{\underline{\beta}} \in R$, anche $t_{\underline{\gamma}} \in R$ per ogni $\underline{\gamma} \in \mathcal{F}$, cioè $t_\_$ è effettivamente una funzione da $\mathcal{F}$ in R. Infine, osserviamo che sempre per la *Proposizione 1.2.1* si ha che

$$\operatorname{supp}(r_\_ \cdot s_\_) \subseteq [\operatorname{supp}(r_\_) \cap \operatorname{supp}(s_\_)]$$

dove tale insieme è finito poiché intersezione di insiemi finiti, quindi $(r_\_ \cdot s_\_) \in \mathcal{F}^\times(\mathcal{F}, R)$. Dunque, $t_\_$ è la somma di un numero finito di funzioni in $\mathcal{F}^\times(\mathcal{F}, R)$, e avendo mostrato sopra che $\mathcal{F}^\times(\mathcal{F}, R)$ è chiuso rispetto alla somma, concludiamo che $t_\_ \in \mathcal{F}^\times(\mathcal{F}, R)$. ■

Per semplicità di notazione denoteremo di qui in seguito gli elementi di $R[x_1, \dots, x_n]$ come f, g, eccetera, dove si intende che $f = f(x_1, \dots, x_n)$, $g = g(x_1, \dots, x_n)$ e così via. Possiamo quindi finalmente dimostrare la proposizione seguente.

Proposizione 1.2.3

Sia R un anello commutativo. Allora, $R[x_1, \dots, x_n]$ dotato di tali operazioni di somma e prodotto è un anello commutativo.

Dimostrazione. Siano $f = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}}$, $g = \sum_{\underline{\beta} \in \mathcal{F}} s_{\underline{\beta}} x^{\underline{\beta}}$ e $h = \sum_{\underline{\gamma} \in \mathcal{F}} t_{\underline{\gamma}} x^{\underline{\gamma}}$ elementi di $R[x_1, \dots, x_n]$. Osserviamo innanzitutto che

$$\begin{aligned}(f+g)+h &= \sum_{\underline{\alpha} \in \mathcal{F}} (r_{\underline{\alpha}} + s_{\underline{\alpha}}) x^{\underline{\alpha}} + \sum_{\underline{\gamma} \in \mathcal{F}} t_{\underline{\gamma}} x^{\underline{\gamma}} = \sum_{\underline{\alpha} \in \mathcal{F}} (r_{\underline{\alpha}} + s_{\underline{\alpha}} + t_{\underline{\alpha}}) x^{\underline{\alpha}} \\ &= \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}} + \sum_{\underline{\beta} \in \mathcal{F}} (s_{\underline{\beta}} + t_{\underline{\beta}}) x^{\underline{\beta}} = f + (g+h)\end{aligned}$$

da cui la somma è associativa. Poiché $(R, +)$ è abeliano, $r_{\underline{\alpha}} + s_{\underline{\alpha}} = s_{\underline{\alpha}} + r_{\underline{\alpha}}$, quindi

$$f + g = \sum_{\underline{\alpha} \in \mathcal{F}} (r_{\underline{\alpha}} + s_{\underline{\alpha}}) x^{\underline{\alpha}} = \sum_{\underline{\alpha} \in \mathcal{F}} (s_{\underline{\alpha}} + r_{\underline{\alpha}}) x^{\underline{\alpha}} = g + f$$

da cui anche $(R[x_1, \dots, x_n], +)$ è un gruppo abeliano con elemento neutro $\sum_{\underline{\alpha} \in \mathcal{F}} 0_{\underline{\alpha}} x^{\underline{\alpha}} = 0_R$, dove $0_{\underline{\alpha}} = 0_R \ \forall \underline{\alpha} \in \mathcal{F}$ è la funzione nulla, e opposto $-f = \sum_{\underline{\alpha} \in \mathcal{F}} -r_{\underline{\alpha}} x^{\underline{\alpha}}$. Inoltre,

$$\begin{aligned}(f \cdot g) \cdot h &= \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\alpha}+\underline{\beta}=\underline{\delta}} r_{\underline{\alpha}} s_{\underline{\beta}} \, x^{\underline{\delta}} \cdot \sum_{\underline{\gamma} \in \mathcal{F}} t_{\underline{\gamma}} x^{\underline{\gamma}} = \sum_{\underline{\varepsilon} \in \mathcal{F}} \sum_{\underline{\delta}+\underline{\gamma}=\underline{\varepsilon}} \sum_{\underline{\alpha}+\underline{\beta}=\underline{\delta}} r_{\underline{\alpha}} s_{\underline{\beta}} t_{\underline{\gamma}} \, x^{\underline{\varepsilon}} \\ &= \sum_{\underline{\varepsilon} \in \mathcal{F}} \sum_{\underline{\alpha}+\underline{\beta}+\underline{\gamma}=\underline{\varepsilon}} r_{\underline{\alpha}} s_{\underline{\beta}} t_{\underline{\gamma}} \, x^{\underline{\varepsilon}} = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}} \cdot \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\beta}+\underline{\gamma}=\underline{\delta}} s_{\underline{\beta}} t_{\underline{\gamma}} \, x^{\underline{\delta}} = f \cdot (g \cdot h)\end{aligned}$$

da cui il prodotto è associativo. Essendo R commutativo, $r_{\underline{\alpha}} s_{\underline{\beta}} = s_{\underline{\beta}} r_{\underline{\alpha}}$ e quindi

$$f \cdot g = \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\alpha}+\underline{\beta}=\underline{\delta}} r_{\underline{\alpha}} s_{\underline{\beta}} \, x^{\underline{\delta}} = \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\beta}+\underline{\alpha}=\underline{\delta}} s_{\underline{\beta}} r_{\underline{\alpha}} \, x^{\underline{\delta}} = g \cdot f$$

da cui anche $R[x_1, \dots, x_n]$ è commutativo con unità $\sum_{\underline{\alpha} \in \mathcal{F}} 1_{\underline{\alpha}} x^{\underline{\alpha}} = 1_R$ dove $1_{\underline{\alpha}}$ è la funzione che vale 1_R per $\underline{\alpha} = \underline{0}$ e 0_R per ogni altro $\underline{\alpha} \in \mathcal{F}$.[5] Infine,

$$\begin{aligned}(f+g) \cdot h &= \sum_{\underline{\alpha} \in \mathcal{F}} (r_{\underline{\alpha}} + s_{\underline{\alpha}}) x^{\underline{\alpha}} \cdot \sum_{\underline{\gamma} \in \mathcal{F}} t_{\underline{\gamma}} x^{\underline{\gamma}} = \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\alpha}+\underline{\gamma}=\underline{\delta}} (r_{\underline{\alpha}} + s_{\underline{\alpha}}) t_{\underline{\gamma}} \, x^{\underline{\delta}} \\ &= \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\alpha}+\underline{\gamma}=\underline{\delta}} r_{\underline{\alpha}} t_{\underline{\gamma}} \, x^{\underline{\delta}} + \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\alpha}+\underline{\gamma}=\underline{\delta}} s_{\underline{\alpha}} t_{\underline{\gamma}} \, x^{\underline{\delta}} = f \cdot h + g \cdot h\end{aligned}$$

dunque vale la proprietà distributiva e $(R[x_1, \dots, x_n], +, \cdot)$ è un anello commutativo. ∎

[5] Chiaramente si intende che $x^{\underline{0}} = x_1^0 \cdot \ldots \cdot x_n^0 = 1_R \cdot \ldots \cdot 1_R = 1_R$.

Definizione

Sia R un anello commutativo e sia n un intero positivo. Allora, l'insieme $R[x_1, \dots, x_n]$ è detto anello dei polinomi a coefficienti in R nelle variabili $x_1, \dots, x_n$.

Anche per gli anelli di polinomi in n variabili vale il corrispondente della *Proprietà universale*, che per semplicità ci limiteremo a dimostrare nel caso in cui $R \subseteq S$.

Teorema 1.2.4: Proprietà universale

Sia R un anello commutativo. Allora, per ogni anello commutativo $S \supseteq R$ e per ogni $\underline{s} = (s_1, \dots, s_n) \in S^n$ esiste un unico omomorfismo di anelli $\phi_{\underline{s}} \colon R[x_1, \dots, x_n] \to S$ tale che $\phi_{\underline{s}}(x_i) = s_i$ per ogni $i = 1, \dots, n$ e $\phi_{\underline{s}}|_R = \mathrm{id}_R$.

Dimostrazione. Siano $f = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}}$ e $g = \sum_{\underline{\beta} \in \mathcal{F}} t_{\underline{\beta}} x^{\underline{\beta}}$ due elementi di $R[x_1, \dots, x_n]$. Per ogni monomio $x^{\underline{\alpha}} \in M$ definiamo $\phi_{\underline{s}}(x^{\underline{\alpha}}) = \prod_{i=1}^{n} s_i^{\alpha_i}$, e sia quindi $\phi_{\underline{s}}(f) = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} \phi_{\underline{s}}(x^{\underline{\alpha}})$. Osserviamo innanzitutto che $\phi_{\underline{s}}(f)$ è ben definita. Infatti, $r_{\underline{\alpha}} \in R \subseteq S$ e $\phi_{\underline{s}}(f) \in S$ perché somma di prodotti di elementi dell'anello S, che è chiuso rispetto a somma e prodotto. Inoltre, $\phi_{\underline{s}}(x_i) = s_i$ e $\phi_{\underline{s}}(\rho) = \rho$ per ogni $\rho \in R$, quindi $\phi_{\underline{s}}$ soddisfa le condizioni richieste. Mostriamo ora che $\phi_{\underline{s}}$ preserva le operazioni. Infatti,

$$\phi_{\underline{s}}(f+g) = \sum_{\underline{\alpha} \in \mathcal{F}} (r_{\underline{\alpha}} + t_{\underline{\alpha}}) \phi_{\underline{s}}(x^{\underline{\alpha}}) = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} \phi_{\underline{s}}(x^{\underline{\alpha}}) + \sum_{\underline{\alpha} \in \mathcal{F}} t_{\underline{\alpha}} \phi_{\underline{s}}(x^{\underline{\alpha}}) = \phi_{\underline{s}}(f) + \phi_{\underline{s}}(g)$$

per la proprietà distributiva del prodotto rispetto alla somma, essendo S un anello, e

$$\phi_{\underline{s}}(f \cdot g) = \sum_{\underline{\gamma} \in \mathcal{F}} \sum_{\underline{\alpha} + \underline{\beta} = \underline{\gamma}} r_{\underline{\alpha}} t_{\underline{\beta}} \ \phi_{\underline{s}}(x^{\underline{\gamma}}) = \left(\sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} \phi_{\underline{s}}(x^{\underline{\alpha}}) \right) \cdot \left(\sum_{\underline{\beta} \in \mathcal{F}} t_{\underline{\beta}} \phi_{\underline{s}}(x^{\underline{\beta}}) \right) = \phi_{\underline{s}}(f) \cdot \phi_{\underline{s}}(g)$$

perché $\phi_{\underline{s}}(x^{\underline{\gamma}}) = \prod_{i=1}^{n} s_i^{\gamma_i} = \prod_{i=1}^{n} s_i^{\alpha_i + \beta_i} = \prod_{i=1}^{n} s_i^{\alpha_i} \cdot \prod_{i=1}^{n} s_i^{\beta_i} = \phi_{\underline{s}}(x^{\underline{\alpha}}) \cdot \phi_{\underline{s}}(x^{\underline{\beta}})$. Poiché $\phi_{\underline{s}}(0_R) = 0_S$ e $\phi_{\underline{s}}(1_R) = 1_S$, concludiamo che tale mappa $\phi_{\underline{s}}$ è effettivamente un omomorfismo di anelli.

Mostriamo ora che $\phi_{\underline{s}}$ è unico. Sia $\psi \colon R[x_1, \dots, x_n] \to S$ un altro omomorfismo di anelli tale che $\psi(x_i) = s_i$ per ogni $i = 1, \dots, n$ e $\psi|_R = \mathrm{id}_R$. Allora, per ogni monomio $x^{\underline{\alpha}} \in M$ vale

$$\psi(x^{\underline{\alpha}}) = \psi\left(\prod_{i=1}^{n} x_i^{\alpha_i} \right) = \prod_{i=1}^{n} \psi\left(x_i^{\alpha_i}\right) = \prod_{i=1}^{n} \psi(x_i)^{\alpha_i} = \prod_{i=1}^{n} s_i^{\alpha_i} = \phi_{\underline{s}}(x^{\underline{\alpha}}).$$

Poiché ψ preserva le operazioni, per ogni $f = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}} \in R[x_1, \dots, x_n]$ si ha quindi che

$$\psi(f) = \psi\left(\sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}} \right) = \sum_{\underline{\alpha} \in \mathcal{F}} \psi(r_{\underline{\alpha}} x^{\underline{\alpha}}) = \sum_{\underline{\alpha} \in \mathcal{F}} \psi(r_{\underline{\alpha}}) \psi(x^{\underline{\alpha}}) = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} \phi_{\underline{s}}(x^{\underline{\alpha}}) = \phi_{\underline{s}}(f)$$

essendo $\psi(r_{\underline{\alpha}}) = r_{\underline{\alpha}}$ perché $r_{\underline{\alpha}} \in R$ e $\psi(x^{\underline{\alpha}}) = \phi_{\underline{s}}(x^{\underline{\alpha}})$ per quanto provato sopra. Dunque, ψ coincide con $\phi_{\underline{s}}$ per ogni polinomio $f \in R[x_1, \dots, x_n]$, da cui $\phi_{\underline{s}}$ è unico. ■