0.1 Anelli di polinomi in più variabili

Vogliamo ora generalizzare il concetto di anello di polinomi ad un numero qualsiasi di variabili, anche infinito. Sia X un insieme non vuoto e sia $\mathcal{F}^\times = \mathcal{F}^\times(X, \mathbb{N})$ l'insieme delle funzioni $\underline{\alpha}\colon X \to \mathbb{N}$ che hanno supporto finito.[1]

Definizione

Sia X un insieme. Denotiamo con $M = \mathrm{mon}\{X\}$ l'insieme dei monomi di X, cioè $M = \{X^{\underline{\alpha}} : \underline{\alpha} \in \mathcal{F}^\times\}$ dove $X^{\underline{\alpha}} = \prod_{x \in X} x^{\underline{\alpha}(x)}$.

Poiché abbiamo scelto $\underline{\alpha}$ con supporto finito, osserviamo che ogni monomio di X è il prodotto di un numero finito di elementi di X, anche nel caso in cui X sia un insieme infinito. Inoltre, analogamente al caso dei polinomi in n variabili, M è un monoide commutativo ed esiste una corrispondenza biunivoca tra i monomi di M e le funzioni di $\mathcal{F}^\times$.

Sia R un anello commutativo e sia $\mathcal{F}^\times(\mathcal{F}^\times, R) = \{f\colon \mathcal{F}^\times \to R : |\mathrm{supp}(f)| < \infty\}$, cioè l'insieme delle funzioni che associano ad ogni funzione di $\mathcal{F}^\times$ un elemento dell'anello R, e che sono diverse da 0_R solo per un numero finito elementi di $\mathcal{F}^\times$. Al variare di $\underline{\alpha} \in \mathcal{F}^\times$, sia $r_\_ \in \mathcal{F}^\times(\mathcal{F}^\times, R)$ la funzione che associa ad ogni $\underline{\alpha} \in \mathcal{F}^\times$ l'elemento $r_{\underline{\alpha}} \in R$. Osserviamo che possiamo definire un polinomio a variabili in X ponendo

$$f(X) = \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} X^{\underline{\alpha}}.$$

Infatti, $f(X)$ è la somma di un numero finito di monomi non nulli, ognuno con un numero finito di variabili e preceduto dal relativo coefficiente $r_{\underline{\alpha}}$.

Sia $R[X] = \left\{ \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} X^{\underline{\alpha}} : r_\_ \in \mathcal{F}^\times(\mathcal{F}^\times, R) \right\}$. Presi due elementi $f(X) = \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} X^{\underline{\alpha}}$ e $g(X) = \sum_{\underline{\beta} \in \mathcal{F}^\times} s_{\underline{\beta}} X^{\underline{\beta}}$ di $R[X]$, definiamo su $R[X]$ le operazioni binarie di somma e prodotto

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

$$f(X) \cdot g(X) = \sum_{\underline{\gamma} \in \mathcal{F}^\times} t_{\underline{\gamma}} X^{\underline{\gamma}}$$

dove abbiamo posto $\underline{\gamma} = \underline{\alpha} + \underline{\beta}$ e $t_{\underline{\gamma}} = \sum_{\underline{\alpha}+\underline{\beta}=\underline{\gamma}} r_{\underline{\alpha}} s_{\underline{\beta}}$. In modo del tutto analogo a quanto visto nel caso di $R[x_1, \ldots, x_n]$, si dimostra che tali operazioni sono ben poste e che $R[X]$ dotato di tali operazioni di somma e prodotto è un anello commutativo con elemento neutro il polinomio nullo $\sum_{\underline{\alpha} \in \mathcal{F}^\times} 0_{\underline{\alpha}} X^{\underline{\alpha}} = 0_R$ e unità il monomio banale $X^{\underline{0}} = 1_R$.

Definizione

Sia R un anello commutativo e sia X un insieme non vuoto. Allora, l'insieme $R[X]$ è detto anello dei polinomi a coefficienti in R e a variabili in X.

[1] Notare come a differenza dei polinomi in n variabili, ora richiediamo esplicitamente che tali funzioni $\underline{\alpha}$ abbiano supporto finito. Infatti, nel caso dei polinomi in n variabili, X è un insieme finito con n elementi, quindi ogni funzione $\underline{\alpha}\colon X \to \mathbb{N}$ ha in realtà supporto finito perché $\mathrm{supp}(\underline{\alpha}) \subseteq X$, che è finito. Dunque, se $|X| < \infty$, non vi è differenza tra $\mathcal{F}^\times(X, \mathbb{N}) = \mathcal{F}(X, \mathbb{N})$.

Anche per gli anelli di polinomi in più variabili vale la *Proprietà universale*.

Teorema 1.3.1: Proprietà universale

Sia X un insieme e sia R un anello commutativo. Allora, per ogni anello commutativo $S \supseteq R$ e per ogni mappa $\varphi\colon X \to S$ esiste un unico omomorfismo di anelli $\phi\colon R[X] \to S$ tale che $\phi(X^{\underline{\delta}_x}) = \varphi(x)\ \forall x \in X$ e $\phi_{|R} = \mathrm{id}_R$, dove $\underline{\delta}_x\colon X \to \mathbb{N}$, $\underline{\delta}_x(y) = \begin{cases} 1 & \text{se } y = x \\ 0 & \text{se } y \neq x \end{cases}$

Dimostrazione. Siano $f = \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} X^{\underline{\alpha}}$ e $g = \sum_{\underline{\beta} \in \mathcal{F}^\times} s_{\underline{\beta}} X^{\underline{\beta}}$ due elementi di $R[X]$. Per ogni monomio $X^{\underline{\alpha}} \in M$, sia $\phi(X^{\underline{\alpha}}) = \prod_{x \in X} \varphi(x)^{\underline{\alpha}(x)}$, e sia quindi $\phi(f) = \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} \phi(X^{\underline{\alpha}})$. Poiché $r_{\underline{\alpha}} \in R \subseteq S$ per ipotesi e $\phi(f) \in S$ perché somma di prodotti di elementi di S, che in quanto anello è chiuso rispetto a somma e prodotto, ϕ è ben definita. Inoltre, $\phi(X^{\underline{\delta}_x}) = \varphi(x)$ e $\phi(\rho) = \rho$ per ogni $\rho \in R$, quindi ϕ soddisfa le condizioni richieste.[2] Mostriamo ora che è un omomorfismo di anelli. Infatti,

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

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

$$\phi(f \cdot g) = \sum_{\underline{\gamma} \in \mathcal{F}^\times} \sum_{\underline{\alpha} + \underline{\beta} = \underline{\gamma}} r_{\underline{\alpha}} s_{\underline{\beta}}\ \phi(X^{\underline{\gamma}}) = \left(\sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} \phi(X^{\underline{\alpha}}) \right) \cdot \left(\sum_{\underline{\beta} \in \mathcal{F}^\times} s_{\underline{\beta}} \phi(X^{\underline{\beta}}) \right) = \phi(f) \cdot \phi(g)$$

perché $\phi(X^{\underline{\gamma}}) = \prod_{x \in X} \varphi(x)^{\underline{\gamma}(x)} = \prod_{x \in X} \varphi(x)^{\underline{\alpha}(x)} \cdot \prod_{x \in X} \varphi(x)^{\underline{\beta}(x)} = \phi(X^{\underline{\alpha}}) \cdot \phi(X^{\underline{\beta}})$. Poiché $\phi(0_R) = 0_S$ e $\phi(1_R) = 1_S$, concludiamo che ϕ è un omomorfismo di anelli.

Mostriamo ora che ϕ è unico. Sia $\psi\colon R[X] \to S$ un omomorfismo di anelli tale che $\psi(X^{\underline{\delta}_x}) = \varphi(x)$ e $\psi_{|R} = \mathrm{id}_R$. Allora, per ogni monomio $X^{\underline{\alpha}} \in M$ vale

$$\psi(X^{\underline{\alpha}}) = \psi\left(\prod_{x \in X} x^{\underline{\alpha}(x)} \right) = \prod_{x \in X} \psi\left(x^{\underline{\alpha}(x)} \right) = \prod_{x \in X} \psi(X^{\underline{\delta}_x})^{\underline{\alpha}(x)} = \prod_{x \in X} \varphi(x)^{\underline{\alpha}(x)} = \phi(X^{\underline{\alpha}}).$$

Poiché ψ è un omomorfismo, per ogni $f = \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} X^{\underline{\alpha}} \in R[X]$ si ha che

$$\psi(f) = \psi\left(\sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} X^{\underline{\alpha}} \right) = \sum_{\underline{\alpha} \in \mathcal{F}^\times} \psi(r_{\underline{\alpha}} X^{\underline{\alpha}}) = \sum_{\underline{\alpha} \in \mathcal{F}^\times} \psi(r_{\underline{\alpha}}) \psi(X^{\underline{\alpha}}) = \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} \phi(X^{\underline{\alpha}}) = \phi(f)$$

essendo $\psi(r_{\underline{\alpha}}) = r_{\underline{\alpha}}$ perché $r_{\underline{\alpha}} \in R$ e $\psi(X^{\underline{\alpha}}) = \phi(X^{\underline{\alpha}})$ per quanto appena mostrato. Dunque, ψ coincide con ϕ, che risulta quindi essere unico. ■

In modo del tutto analogo al *Teorema 1.1.4* è possibile mostrare che, a meno di isomorfismi, $R[X]$ è l'unico anello contenente R avente questa proprietà.

[2] $\underline{\delta}_x$ è la funzione tale che per ogni $x \in X$ si abbia $X^{\underline{\delta}_x} = x$. Infatti, $X^{\underline{\delta}_x} = \prod_{y \in X} y^{\underline{\delta}_x(y)} = x^{\underline{\delta}_x(x)} = x^1 = x$ perché tutti gli altri termini del prodotto hanno esponente 0, essendo per definizione $\underline{\delta}_x(y) = 0$ se $y \neq x$.

Sia $R[x]$ l'anello dei polinomi a coefficienti in R nella variabile x. Possiamo considerare $R[x]$ stesso come anello dei coefficienti per l'anello dei polinomi nella variabile y, cioè

$$(R[x])[y] = \left\{ \sum_{i=0}^{n} f_i\, y^i : f_i \in R[x],\, n \in \mathbb{N} \right\}.$$

Poiché ogni polinomio di $(R[x])[y]$ può essere visto come un polinomio in due variabili di $R[x,y]$ e ogni polinomio di $R[x,y]$ può essere pensato come un polinomio di $(R[x])[y]$ raccogliendo i termini dello stesso grado in y, questo suggerisce che $(R[x])[y] \simeq R[x,y]$.

Esempio. Sia $f(y) = (x^2+1)y^2 + (2x)y + 3 \in (\mathbb{Z}[x])[y]$. Allora, possiamo vedere $f(y)$ come un polinomio in due variabili $g(x,y) = x^2y^2 + y^2 + 2xy + 3 \in \mathbb{Z}[x,y]$. Viceversa, preso $p(x,y) = xy^2 + 2xy + 3y + 4 \in \mathbb{Z}[x,y]$, raccogliendo i termini dello stesso grado in y possiamo pensare $p(x,y)$ come un polinomio $q(y) = (x)y^2 + (2x+3)y + 4 \in (\mathbb{Z}[x])[y]$. □

In generale, se X e Y sono insiemi non vuoti e $(R[X])[Y]$ è l'anello dei polinomi a coefficienti in $R[X]$ e a variabili in Y, detta $X \sqcup Y$ l'unione disgiunta,[3] vale il teorema seguente.

Teorema 1.3.2

Sia R un anello commutativo e siano X e Y non vuoti. Allora, $R[X \sqcup Y] \simeq (R[X])[Y]$.

Dimostrazione. Sia S un anello commutativo tale che $R \subseteq R[X] \subseteq S$ e sia $\varphi_X \colon X \to S$ definita come $\varphi_X(x) = X^{\underline{\delta}_x}$. Presa una qualunque funzione $\varphi_Y \colon Y \to S$, sia $\widetilde{\varphi} \colon X \sqcup Y \to S$ l'unica mappa tale che $\widetilde{\varphi}_{|_X} = \varphi_X$ e $\widetilde{\varphi}_{|_Y} = \varphi_Y$. Allora, per il *Teorema 1.3.1* esiste un unico omomorfismo $\widetilde{\phi} \colon R[X \sqcup Y] \to S$ tale che $\widetilde{\phi}(Z^{\underline{\delta}_z}) = \widetilde{\varphi}(z)$ per ogni $z \in X \sqcup Y$ e $\widetilde{\phi}_{|_R} = \mathrm{id}_R$. Per ogni $\underline{\alpha} \in \mathcal{F}^{\times}(X, \mathbb{N})$, sia $\widetilde{\underline{\alpha}} \in \mathcal{F}^{\times}(X \sqcup Y, \mathbb{N})$ l'unica funzione tale che $\widetilde{\underline{\alpha}}_{|_X} = \underline{\alpha}$ e $\widetilde{\underline{\alpha}}_{|_Y} = \underline{0}$. Allora, possiamo pensare ogni monomio $X^{\underline{\alpha}}$ di $R[X]$ come monomio $Z^{\widetilde{\underline{\alpha}}}$ di $R[X \sqcup Y]$, da cui

$$\begin{aligned}\widetilde{\phi}(Z^{\widetilde{\underline{\alpha}}}) &= \widetilde{\phi}\left(\prod_{z \in X \sqcup Y} z^{\widetilde{\underline{\alpha}}(z)} \right) = \prod_{z \in X \sqcup Y} \widetilde{\phi}\left(z^{\widetilde{\underline{\alpha}}(z)} \right) = \prod_{z \in X \sqcup Y} \widetilde{\phi}\left(Z^{\underline{\delta}_z} \right)^{\widetilde{\underline{\alpha}}(z)} = \prod_{z \in X \sqcup Y} \widetilde{\varphi}(z)^{\widetilde{\underline{\alpha}}(z)} \\ &= \prod_{x \in X} \varphi_X(x)^{\underline{\alpha}(x)} \cdot \prod_{y \in Y} \varphi_Y(y)^{\underline{0}} = \prod_{x \in X} (X^{\underline{\delta}_x})^{\underline{\alpha}(x)} \cdot 1_R = X^{\underline{\alpha}}\end{aligned}$$

per come abbiamo definito $\widetilde{\varphi}$ e $\widetilde{\underline{\alpha}}$ ed usando il fatto che $\widetilde{\phi}$ è un omomorfismo. Quindi, preso $f = \sum_{\underline{\alpha} \in \mathcal{F}^{\times}} r_{\underline{\alpha}} X^{\underline{\alpha}} \in R[X]$, pensando f come elemento $\widetilde{f} = \sum_{\widetilde{\underline{\alpha}} \in \mathcal{F}^{\times}} r_{\widetilde{\underline{\alpha}}} Z^{\widetilde{\underline{\alpha}}} \in R[X \sqcup Y]$ si ha che

$$\widetilde{\phi}(\widetilde{f}\,) = \sum_{\widetilde{\underline{\alpha}} \in \mathcal{F}^{\times}} \widetilde{\phi}(r_{\widetilde{\underline{\alpha}}}) \widetilde{\phi}(Z^{\widetilde{\underline{\alpha}}}) = \sum_{\widetilde{\underline{\alpha}} \in \mathcal{F}^{\times}} r_{\widetilde{\underline{\alpha}}}\, \widetilde{\phi}(Z^{\widetilde{\underline{\alpha}}}) = \sum_{\underline{\alpha} \in \mathcal{F}^{\times}} r_{\underline{\alpha}} X^{\underline{\alpha}} = f$$

perché $\widetilde{\phi}(r_{\widetilde{\underline{\alpha}}}) = r_{\widetilde{\underline{\alpha}}}$ essendo $\widetilde{\phi}_{|_R} = \mathrm{id}_R$, da cui $\widetilde{\phi}_{|_{R[X]}} = \mathrm{id}_{R[X]}$. Inoltre, per ogni $y \in Y$ si ha che $\widetilde{\phi}(Z^{\underline{\delta}_y}) = \widetilde{\varphi}(y) = \varphi_Y(y)$. Poiché $R[X \sqcup Y]$ è un anello commutativo contenente $R[X]$ che soddisfa la proprietà universale di $(R[X])[Y]$,[4] per la generalizzazione del *Teorema 1.1.4* possiamo effettivamente concludere che $R[X \sqcup Y] \simeq (R[X])[Y]$. ■

[3] Ricordiamo che l'unione disgiunta di una famiglia di insiemi $\{A_i\}_{i \in I}$ è l'insieme $\bigsqcup_{i \in I} A_i = \bigcup_{i \in I} (A \times \{i\})$. Ad esempio, presi $A_0 = \{3,4,5\}$ e $A_1 = \{5,6\}$, si ha che $A_0 \sqcup A_1 = \{(3,0),(4,0),(5,0),(5,1),(6,1)\}$.

[4] Infatti, abbiamo appena mostrato che per ogni anello $S \supseteq R[X]$ e per ogni mappa $\varphi_Y \colon Y \to S$, esiste un unico omomorfismo $\widetilde{\phi} \colon R[X \sqcup Y] \to S$ tale che $\widetilde{\phi}(Z^{\underline{\delta}_y}) = \varphi_Y(y)$ per ogni $y \in Y$ e $\widetilde{\phi}_{|_{R[X]}} = \mathrm{id}_{R[X]}$.

Nel caso in cui l'insieme delle variabili sia finito, vale il corollario seguente.

Corollario 1.3.3

Sia n un intero positivo. Allora, $R[x_1, \dots, x_n] \simeq (\cdots((R[x_1])[x_2])\cdots)[x_n]$.

Dimostrazione. Procediamo per induzione sul numero n di variabili. Chiaramente, se $n = 1$ allora $R[x_1] \simeq R[x_1]$. Supponiamo quindi che la tesi sia vera per un certo intero $n \geq 1$. Detti $X = \{x_1, \dots, x_n\}$ e $Y = \{x_{n+1}\}$, per il *Teorema 1.3.2* si ha che $R[X \sqcup Y] \simeq (R[X])[Y]$ da cui $R[x_1, \dots, x_{n+1}] \simeq (R[x_1, \dots, x_n])[x_{n+1}] \simeq ((\cdots((R[x_1])[x_2])\cdots)[x_n])[x_{n+1}]$. ■

Possiamo quindi estendere agli anelli di polinomi in più variabili anche la *Proposizione 1.1.1*. Per fare ciò, osserviamo innanzitutto che ogni polinomio di $R[X]$ è la somma di un numero finito di monomi non nulli, ognuno con un numero finito di variabili. Dunque, ogni polinomio di $R[X]$ può essere pensato come un polinomio in un numero finito di variabili, o meglio, per ogni $f \in R[X]$ esiste un sottoinsieme delle variabili $X_f \subseteq X$ finito tale che $f \in R[X_f]$.[5]

Proposizione 1.3.4

Sia X un insieme non vuoto e sia R un dominio di integrità. Allora, anche l'anello dei polinomi $R[X]$ è un dominio di integrità.

Dimostrazione. Siano $f, g \in R[X]$ e siano $X_f, X_g \subseteq X$ finiti tali che $f \in R[X_f]$ e $g \in R[X_g]$. Osserviamo innanzitutto che $X_f \cup X_g$ è un sottoinsieme finito di X e $f \cdot g \in R[X_f \cup X_g]$. Dunque, detto $X_f \cup X_g = \{x_1, \dots, x_n\}$, per dimostrare che $R[X]$ è un dominio di integrità è sufficiente provare che $R[x_1, \dots, x_n]$ è un dominio di integrità.[6] Per fare ciò, procediamo per induzione sul numero di variabili. Se $n = 1$, per la *Proposizione 1.1.1* sappiamo che $R[y_1]$ è un dominio di integrità. Supponiamo quindi che la tesi valga per un certo intero $n \geq 1$. Allora, per il *Corollario 1.3.3* si ha che $R[y_1, \dots, y_{n+1}] \simeq (R[y_1, \dots, y_n])[y_{n+1}]$, ed essendo $R[y_1, \dots, y_n]$ un dominio di integrità per ipotesi induttiva, per la *Proposizione 1.1.1* anche $(R[y_1, \dots, y_n])[y_{n+1}]$ è un dominio di integrità, da cui lo è pure $R[y_1, \dots, y_{n+1}]$. Dunque, $R[Y]$ è un dominio di integrità per ogni insieme finito Y, ed in particolare lo è per $Y = X_f \cup X_g$. Per l'arbitrarietà di $f, g \in R[X]$, possiamo concludere che $R[X]$ è un dominio di integrità. ■

Concludiamo con un'osservazione che acquisirà importanza quando passeremo allo studio dell'estensione di campi. Preso un anello commutativo R e un qualunque oggetto $x \notin R$, l'anello dei polinomi $R[x]$ è il più piccolo anello contenente R e x. Infatti, se S è un anello contenente R e x, per la chiusura di S rispetto a somma e prodotto esso conterrà tutte le potenze non negative $\{x^0, x^1, x^2, \dots\}$ di x e tutte le combinazioni lineari tra potenze di x ed elementi di R, cioè tutti gli elementi della forma $a_n x^n + \dots + a_1 x + a_0$ con $a_0, \dots, a_n \in R$. In generale, se X è un insieme non vuoto, possiamo quindi vedere $R[X]$ come la più piccola "estensione" di R contenente X, cioè come il più piccolo anello contenente sia R che X.

[5] Più formalmente, preso $f = \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} X^{\underline{\alpha}} \in R[X]$ sappiamo che $\Omega_f = \mathrm{supp}(r\_) \subseteq \mathcal{F}^\times$ è finito, quindi esiste solo un numero finito di funzioni $\underline{\alpha} \in \mathcal{F}^\times$ per cui il monomio $X^{\underline{\alpha}}$ ha un coefficiente $r_{\underline{\alpha}}$ non nullo. Poiché ogni $\underline{\alpha} \in \mathcal{F}^\times$ ha supporto finito, $X_f = \bigcup_{\underline{\alpha} \in \Omega_f} \mathrm{supp}(\underline{\alpha})$ è finito in quanto unione finita di insiemi finiti.

[6] Se il polinomio $f \cdot g$ si annulla in $R[X]$, allora si annulla anche pensato come polinomio di $R[X_f \cup X_g]$. Dunque, se $R[X_f \cup X_g]$ è un dominio di integrità per ogni $f, g \in R[X]$, allora anche $R[X]$ deve essere un dominio di integrità. Infatti, se esistessero $f, g \in R[X]$ divisori dello zero, per quanto appena detto essi sarebbero divisori dello zero anche in $R[X_f \cup X_g]$, il che contraddice la definizione di dominio di integrità.