Lezione 10

Prerequisiti: Lezione 5

Anelli di polinomi

Sia *A* un anello commutativo unitario.

Consideriamo l'insieme

$$P = \left\{(a_0, a_1, a_2, ..., a_n, ...) \middle| a_n \in A \text{ per ogni } n \in \mathbb{N}, \text{ed esiste } n_0 \in \mathbb{N} \text{ tale che } a_n = 0 \text{ per ogni } n > n_0\right\}.$$

Scriveremo, per brevità, $(a_n)_{n\in\mathbb{N}}$ al posto di $(a_0, a_1, a_2, ..., a_n, ...)$: tale simbolo indica la successione a valori in *A* il cui *n*-esimo *termine* è a_n, ossia l'applicazione $f : \mathbb{N} \to A$ tale che, per ogni $n \in \mathbb{N}$, si abbia $f(n) = a_n$.
Dunque *P* è l'insieme delle successioni a valori in *A* che sono *definitivamente nulle*. Secondo una formulazione equivalente, considerato il *supporto* della successione $(a_n)_{n\in\mathbb{N}}$, che, per definizione, è

$$\text{Supp}(a_n)_{n\in\mathbb{N}} = \left\{n \in \mathbb{N} \middle| a_n \neq 0\right\},$$

P è l'insieme delle successioni a valori in *A* aventi supporto finito. La successione nulla (i cui termini sono tutti uguali all'elemento zero di *A*) è l'unica avente supporto vuoto.

Gli elementi di questo insieme sono detti *polinomi a coefficienti in A*. La successione nulla sarà detta *polinomio nullo*.

Definizione 10.1 Per ogni polinomio *f* non nullo a coefficienti in *A*, si definisce *grado* di *f* il numero

$$\deg(f) = \max \text{Supp}(f).$$

Nota Alcuni autori estendono la definizione di grado anche al polinomio nullo, assegnandogli grado pari a –1 oppure $-\infty$.
Un polinomio di grado zero si dice *costante*, un polinomio di grado uno si dice *lineare*, un polinomio di grado due si dice *quadratico*, un polinomio di grado tre si dice *cubico*.
Anche il polinomio nullo si dice costante. In generale, i polinomi costanti sono quindi tutti e soli quelli della forma $(a, 0, 0, 0, ...)$, con $a \in A$.

Sull'insieme dei polinomi a coefficienti in *A* definiamo le seguenti operazioni:

- una somma, ponendo, per ogni $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in P$, $(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}}$;
- un prodotto, ponendo, per ogni $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in P$, $(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (\sum_{i+j=n} a_i b_j)_{n\in\mathbb{N}}$.

Proviamo che queste operazioni sono ben definite.

Siano $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in P$. Esistono allora $n_0, m_0 \in \mathbb{N}$ tali che, per ogni $n > n_0$, $a_n = 0$ e, per ogni $n > m_0$, $b_n = 0$. Quindi, posto $N = \max(n_0, m_0)$, per ogni $n > N$ si ha $a_n = b_n = 0$, e pertanto $a_n + b_n = 0$. Dunque $(a_n + b_n)_{n\in\mathbb{N}} \in P$. Ciò prova che la somma è ben definita.
Sia ora $M = n_0 + m_0$. Per ogni $n \in \mathbb{N}$ sia $c_n = \sum_{i+j=n} a_i b_j$. Sia $n > M$. Allora, se i e j sono numeri naturali tali che $n = i + j$, non possono valere contemporaneamente le disuguaglianze $i \le n_0$ e $j \le m_0$ (altrimenti sarebbe $i + j \le M$). Quindi $i > n_0$ oppure $j > m_0$. Nel primo caso $a_i = 0$, nel secondo caso $b_j = 0$. Dunque, in ogni caso, $a_i b_j = 0$. Pertanto, per ogni $n > M$, $c_n = 0$. Quindi $(\sum_{i+j=n} a_i b_j)_{n\in\mathbb{N}} \in P$. Ciò prova che il prodotto è ben definito.

Dalle considerazioni appena effettuate si può determinare il comportamento del grado dei polinomi rispetto alla somma ed al prodotto.

Proposizione 10.2 *(Formule del grado)*. Siano f, g polinomi non nulli a coefficienti in *A*.

(a) Se $f + g$ è non nullo, $\deg(f + g) \le \max(\deg(f), \deg(g))$.

(b) Se $f \cdot g$ è non nullo, $\deg(f \cdot g) \le \deg(f) + \deg(g)$.
Inoltre, se *A* è integro, $f \cdot g$ è non nullo e $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Dimostrazione: Siano $f = (a_n)_{n\in\mathbb{N}}, g = (b_n)_{n\in\mathbb{N}}$. Allora, se $a_n = b_n = 0$, si ha che $a_n + b_n = 0$. Ciò prova che se $n \notin \mathrm{Supp}(f) \cup \mathrm{Supp}(g)$, allora $n \notin \mathrm{Supp}(f + g)$, ossia, equivalentemente, $\mathrm{Supp}(f + g) \subset \mathrm{Supp}(f) \cup \mathrm{Supp}(g)$. Quindi, se $f + g$ è non nullo,

$$\deg(f + g) = \max \mathrm{Supp}(f + g) \le \max(\mathrm{Supp}(f) \cup \mathrm{Supp}(g)) = \max(\max \mathrm{Supp}(f), \max \mathrm{Supp}(g))$$
$$= \max(\deg(f), \deg(g)).$$

Ciò prova (a).

Siano ora $n_0 = \deg(f)$, $m_0 = \deg(g)$, e sia $f \cdot g = (c_n)_{n\in\mathbb{N}}$. Come abbiamo visto sopra, per ogni $n > n_0 + m_0$, $c_n = 0$. Quindi si ha che $\mathrm{Supp}(c_n) \subset \{n \in \mathbb{N} \mid n \le n_0 + m_0\}$, e, conseguentemente, se $f \cdot g$ è non nullo, $\deg(f \cdot g) = \max \mathrm{Supp}(f \cdot g) \le n_0 + m_0 = \deg(f) + \deg(g)$. Supponiamo ora che *A* sia integro. Allora

$$c_{n_0+m_0} = \sum_{i+j=n_0+m_0} a_i b_j = a_{n_0} b_{m_0}. \qquad (1)$$

Infatti, se $i + j = n_0 + m_0$, e $(i, j) \ne (n_0, m_0)$, allora $i < n_0$ e $j > m_0$, oppure $i > n_0$ e $j < m_0$: nel primo caso $b_j = 0$, nel secondo caso $a_i = 0$, e in entrambi casi $a_i b_j = 0$. Essendo $a_{n_0} \ne 0, b_{m_0} \ne 0$, e valendo in *A* la legge di annullamento del prodotto, dalla (1) segue che $c_{n_0+m_0} \ne 0$. Quindi $f \cdot g$ è non nullo, e $n_0 + m_0 \in Supp(f \cdot g)$, e, conseguentemente, si ha che $\max \mathrm{Supp}(f \cdot g) \ge n_0 + m_0$, ovverosia $\deg(f \cdot g) \ge \deg(f) + \deg(g)$. Poiché l'altra disuguaglianza vale sempre, abbiamo così dimostrato l'uguaglianza voluta. Ciò prova (b). □

Nota Per i polinomi, usualmente, si utilizza una scrittura basata sull'introduzione di un simbolo formale, detto *indeterminata.* Se X è un'indeterminata, e $f=(a_n)_{n\in\mathbb{N}}$ è un polinomio nullo o di grado minore o uguale a n_0, si scrive

$$f=\sum_{i=0}^{n_0} a_i X^i.$$

(Gli a_i con indice $i>n_0$ non compaiono, e sono nulli). Per ogni indice *i*, a_i si dice il *termine di grado i* di *f*. Il termine di grado 0 si dice *termine noto*. Il termine di grado $\deg(f)$ si dice *coefficiente direttore* di *f*.
Solitamente, al posto dell'addendo a_0X^0 si scrive semplicemente a_0. Inoltre, se $a_i=0$, l'addendo a_iX^i si può omettere. Di conseguenza, se *f* non è il polinomio nullo, quasi sempre n_0 sarà il suo grado e a_{n_0} sarà il suo coefficiente direttore.
Nelle scritture di *f* che non fanno uso del simbolo di sommatoria, l'ordine in cui compaiono gli addendi è del tutto irrilevante. Normalmente, però, questi si dispongono secondo l'ordine crescente (o decrescente) dei gradi.
Il polinomio *f*, indicato anche con $f(X)$, viene detto polinomio nell'indeterminata *X*, a coefficienti in *A*. L'insieme di tutti i polinomi siffatti – che all'inizio avevamo provvisoriamente chiamato *P* - viene indicato con $A[X]$.

Esempio 10.3 In $\mathbb{Z}[X]$ possiamo considerare il polinomio $f=(0,1,-2,0,6,0,0,0,,...)$, che si scrive nella forma

$$f(X)=X-2X^2+6X^4.$$

Il suo termine noto è 0, il suo grado è 4, ed il coefficiente direttore è 6.
In $\mathbb{Z}[X]$ consideriamo anche

$$g(X)=1-X^2+X^3,$$

di termine noto 1, grado 3, e coefficiente direttore 1. Calcolare la somma ed il prodotto di questi due polinomi secondo la definizione data sopra significa calcolare la loro somma ed il loro prodotto secondo le consuete regole del calcolo letterale. Si ottiene:

$$f(X)+g(X)=1+X-3X^2+X^3+6X^4,$$
$$f(X)\cdot g(X)=X-2X^2-X^3+9X^4-2X^5-6X^6+6X^7.$$

Inoltre si ha la seguente proposizione, di cui, per brevità, omettiamo la dimostrazione.

Proposizione 10.4 $(A[X],+,\cdot)$ è un anello commutativo unitario.

Osserviamo soltanto che l'elemento zero di $A[X]$ è il polinomio nullo, e l'elemento uno è il polinomio costante di termine noto 1.

Possiamo però provare il seguente

Corollario 10.5 L'anello *A* è isomorfo al sottoanello di $A[X]$ formato dai polinomi costanti.

Dimostrazione: Per ogni $a \in A$ consideriamo il polinomio $\hat{a} = (a, 0, 0, 0, ...)$ (il polinomio costante di termine noto a) e definiamo l'applicazione $\varphi : A \to A[X]$ ponendo, per ogni $a \in A$, $\varphi(a) = \hat{a}$. Questa applicazione è evidentemente iniettiva. Inoltre, per ogni $a \in A, b \in A$ abbiamo:

- $\varphi(a+b) = \widehat{a+b} = (a+b, 0, 0, 0, ...) = (a, 0, 0, 0, ...) + (b, 0, 0, 0, ...) = \hat{a} + \hat{b} = \varphi(a) + \varphi(b)$;
- $\varphi(ab) = \widehat{ab} = (ab, 0, 0, 0, ...) = (a, 0, 0, 0, ...)(b, 0, 0, 0, ...) = \hat{a}\hat{b} = \varphi(a)\varphi(b)$.

Ciò prova che φ è un monomorfismo di anelli. Inoltre $B = \operatorname{Im}\varphi = \{\hat{a} \mid a \in A\}$ è l'insieme dei polinomi costanti di $A[X]$, ed è un sottoanello di $A[X]$ in virtù del Corollario 5.40. L'omomorfismo $\varphi_{\#} : A \to B$ indotto da φ per corestrizione è allora l'isomorfismo cercato. □

Nota L'isomorfismo del Corollario 10.5 ci consente di identificare ogni $a \in A$ col polinomio $\hat{a}$, ossia, viceversa, ogni polinomio costante col suo termine noto. D'altronde, nella scrittura con l'indeterminata, entrambi gli elementi si scrivono allo stesso modo: a.
D'ora in poi adotteremo questa identificazione, così che, per noi, A sarà il sottoanello dei polinomi costanti di $A[X]$.

Proviamo, infine, alcune proprietà che legano l'anello di polinomi $A[X]$ all'anello A.

Corollario 10.6 *(Anelli di polinomi integri*) L'anello $A[X]$ è integro se e solo se A è integro.

Dimostrazione: Supponiamo che $A[X]$ sia integro. Allora è integro anche il suo sottoanello A formato dai polinomi costanti. Viceversa, supponiamo che A sia integro. Allora, in base alla Proposizione 10.2 (b), in $A[X]$ vale la legge di annullamento del prodotto, e quindi $A[X]$ è integro. □

Corollario 10.7 *(Polinomi invertibili*) Sia A integro e non nullo. Un elemento di $A[X]$ è invertibile se e solo se è costante e invertibile in A.

Dimostrazione: Ogni elemento di A invertibile in A è invertibile anche in $A[X]$ ed ha ivi lo stesso inverso. Viceversa, sia $f \in A[X]$ invertibile. Allora esiste $g \in A[X]$ tale che $fg = 1$. Ma allora, in base alla Proposizione 10.2 (b), $0 = \deg(1) = \deg(f) + \deg(g)$. Segue che $\deg(f) = \deg(g) = 0$, ossia f e g sono entrambi costanti, e quindi appartenenti ad A, dove, pertanto, f è invertibile con inverso g. □

Osservazione 10.8 Il "se" del Corollario 10.7 è valido per ogni anello commutativo A. Il "solo se", invece, in generale non vale se A non è un anello integro. Lo mostra il seguente controesempio, in cui $A = \mathbb{Z}_4$. Il polinomio $f(X) = [2]_4 X + [1]_4$ non è costante, però è invertibile, ed ha come inverso se stesso:

$$f(X)^2 = \left([2]_4 X + [1]_4\right)^2 = [4]_4 X^2 + [4]_4 X + [1]_4 = [1]_4 .$$

Essendo $\deg(f^2) = 0 < 2\deg(f) = 2$, questo esempio mostra anche che, se A non è integro, l'uguaglianza della Proposizione 10.2 (b), in generale, non è verificata.

A proposito del significato dell'indeterminata, può essere utile il seguente

Esercizio 10.9 Nell'anello dei polinomi $A[X]$ sia dato il polinomio $f = \sum_{i=0}^{N} a_i X^i$. Si consideri, inoltre, il polinomio $u = (0,1,0,0,...)$. Si provi che $f = \sum_{i=0}^{N} a_i u^i$.