Appunti di Algebra II

Dipartimento di Matematica e Applicazioni, Univerisita' degli studi di Milano-Bicocca. A.A 2020/2021

> Lorenzo Feroleto September 2020

Indice

1	Con	nplementi di teoria degli anelli	1
	1.1	Anelli di polinomi in una variabile	1

1 Complementi di teoria degli anelli

1.1 Anelli di polinomi in una variabile

Andiamo a definire l'anello dei polinomi senza il concetto di successione normalmente utilizzato in approcci piu' rigorosi.

Definizione 1.1: Anello di polinomi a coefficienti in R nella variabile x

Sia R un anello commutativo e definiamo l'anello di polinomi in una variabile come la seguente struttura algebrica

$$R[x] = \{ f := \sum_{i=0}^{n} a_i x^i \mid a_i \in R, n \in \mathbb{N} \}$$
 (1)

Sia f un polinomio come quello sopracitato; allora il coefficiente a_n viene chiamato coefficiente direttivo di f. Se $a_n = 1$, allora il polinomio viene detto monico.

Notiamo come x^i in questo contesto non e' nient'altro che una indeterminata che obbedisce alle proprieta' degli esponenti di una potenza.

Procediamo ora a definire le operazioni di somma e prodotto di polinomi in una variabile.

Definizione 1.2: Operazioni tra polinomi in una variabile

Siano
$$f = \sum_{i=0}^n r_i \cdot x^i, \ g = \sum_{i=0}^n s_i \cdot x^i \in R[x]$$
. Definiamo la somma

$$+: R[x] \times R[x] \to R[x], \ f + g = \sum_{i=0}^{\max\{n,m\}} (r_i + s_i) \cdot x^i$$
 (2)

ponendo $r_{n+1} = \cdots = r_m = 0$ se m > n e $s_{m+1} = \cdots = s_n = 0$ se n > m. Definiamo il prodotto

$$: R[x] \times R[x] \to R[x], \ f \cdot g = \sum_{k=0}^{n+m} (\sum_{i=0}^{k} r_i \cdot s_{k-i}) \cdot x^i$$
 (3)

Tale scrittura e' la normale moltiplicazione tra i polinomi ma scritta formalmente.

Vediamo alcuni semplici esempi:

Esempio 1.3

Aggiungere esempio

Come visto nel corso di Algebra I, si verifica facilmente che R[x] dotato di tali operazioni di somma e prodotto e' un anello commutativo con elemento neutro il polinomio identicamente nullo $0_{R[x]} = 0_R$ e unita' il polinomio costante $1_{R[x]} = 1_R$.

Definiamo ora un imporante funzione che descrive un polinomio.

Definizione 1.4: Funzione grado; grado di un polinomio

Sia R un anello commutativo e sia $f(x) = f \in R[x]$ definita come in precedenza. Allora definiamo la funzione grado:

$$deg^*(f) := \left\{ \begin{array}{ll} \max\{k \in \mathbb{N} : a_k \neq 0_R\}, & \text{se } f(x) \not\equiv 0_R \\ -\infty, & \text{se } f(x) \equiv 0_R \end{array} \right\}$$
 (4)

e il risultato di $deg^*(f)$ come il grado del polinomio f. Se $deg^*(f)=0$ si dice che f e' un polinomio costante.

Tale definizionne coincide con quella classica di grado di un polinomio tranne nel caso in cui f(x) sia identicamente nullo.

Esempio 1.5: Grado di un polinomio

Se consideriamo i polinomi $f(x) = x^2 + 1, g(x) = 1$ e $h(x) = 0, f, g, h \in \mathbb{Z}[x]$, si ha che

$$deg * (f) = 2, \ deg * (g) = 0, \ deg * (h) = -\infty.$$

Per calcolare il grado di un prodotto di un polinomio e' necessario aritmetizzare alcuni simboli.

Definizione 1.6: \mathbb{N}_k , somma in $\mathbb{N}_k \cup \{-\infty\}$

Poniamo $\mathbb{N}_k := \{z \in \mathbb{Z} \mid z \geq k \in \mathbb{Z}\}; \text{ ad esempio, } \mathbb{N}_0 = \{0, 1, 2, \dots\}.$ Definiamo la somma in $\mathbb{N}_k \cup \{-\infty\}$

$$+: \mathbb{N}_k \cup \{-\infty\} \times \mathbb{N}_k \cup \{-\infty\} \to \mathbb{N}_k \cup \{-\infty\},$$

dove per $n, m \in N_k$, n + m coincide con la somma definita su \mathbb{Z} , e

$$n + (-\infty) = -\infty + n := -\infty \tag{5}$$

per ogni $n \in N_k$

Riportiamo ora una definizione precedente discussa nel corso di Algebra I

Definizione 1.7: Dominio d'integrita'

Un dominio d'integrita' e' un anello commutativo R che soddisfa:

- 1. $1_R \neq 0_R$,
- 2. $\forall a, b \ (a, b \in R \land a \cdot b = 0 \Rightarrow (a = 0 \lor b = 0)).$

La seconda condizione e' equivalente ad affermare che R e' privo di divisori dello zero.

Riportiamo alcuni fatti che mettono in relazioni i domini di integrita con i polinomi.

Proposizione 1.8

Sia R un dominio di integrita'. Allora per ogni $f,g\in R[x]$ vale

$$deg^*(f \cdot g) = deg^*(f) + deg^*(g). \tag{6}$$

Dimostrazione. Se f oppure g e' il poliniomio nullo, allora l'uguaglianza e' verificata in seguito a (5). Supponendo che

$$f = \sum_{i=0}^{n} r_i x^i, \ g = \sum_{i=0}^{m} s_i x^i \neq 0_{R[x]}$$

dove $r_n, s_m \neq 0_R$, e poiche' R e' un dominio di integrita', allora $r_n s_m \cdot x^{n+m}$ e' il monomio di grado massimo presente nel prodotto $f \cdot g$, quindi

$$deg^*(f \cdot g) = n + m = deg^*(f) + deg^*(g)$$

Proposizione 1.9

Se R un dominio di integrita', allora lo e' anche R[x].

Dimostrazione. Devono essere soddisfatti i due assiomi di dominio di integrita'. Il primo deriva da $1_{R[x]} \equiv 1_R \neq 0_R \equiv 0_{R[x]}$. Per il secondo assioma siano $f, g \in R[x]$ tali che $f \cdot g = 0$. Allora

$$deg^*(f\cdot g) = -\infty \Longrightarrow (deg^*(f) = -\infty \land f = 0_{R[x]}) \lor (deg^*(g) = -\infty \land g = 0_{R[x]})$$

Grazie alle precedenti proposizioni, denotiamo il gruppo dei polinomi invertibili

Definizione 1.10: Gruppo dei polinomi invertibili

Sia R un dominio di integrita'. Allora possiamo definire

$$R[x]^{\times} = \{ f \in R[x] \mid \exists g \ (g \in R[x] \land f \cdot g = 1_{R[x]}) \},$$

ovvero il gruppo degli elementi invertibili in R[x].

Proposizione 1.11

Sia R un dominio di integrita'. Allora $R[x]^{\times} = R^{\times}$

Dimostrazione. Siano $f \in R[x]^{\times}$, $g \in R[x]$ tali che $f \cdot g = 1_{R[x]}$. Allora dalla proposizione 1.8 segue che

$$deg^*(f) + deg^*(g) = 0 \land deg^*(g) = 0 \Longrightarrow deg^*(f) = 0 \Longrightarrow f \in R[x]$$

3