3 Numeri interi e Polinomi

Terminato l'esempio che spero non sia stato troppo traumatico, introduco i due principali protagonisti - dramatis personae - del corso. A livello poco formale dovreste averli incontrati già ripetute volte. Si tratta degli interi $\mathbb{Z}$ e dell'insieme dei polinomi a coefficienti .... reali? complessi? razionali? Vedremo che si possono definire polinomi a coefficienti su un qualsiasi insieme dotato della struttura di anello commutativo. Noi ci limiteremo al caso in cui questo anello è un campo. Se denoto con K il misterioso campo (K è l'iniziale di Körper, ossia campo in tedesco), indicherò con $K[x]$ l'insieme dei polinomi a coefficienti in K nella variabile x.

Spesso indicherò con A, $\mathbb{Z}$ oppure $K[x]$, A perché loro stessi sono degli anelli, perfino commutativi. Come vedremo si possono analizzare le due strutture in parallelo. Molti testi preferiscono parlare prima e più a lungo degli interi e, successivamente, quando tipicamente ci siamo dimenticati quasi tutto si trattano i polinomi. Spero che questa mia scelta risulti vincente.

Si potrebbero definire i polinomi in modo più formale rendendo solido il concetto di variabile o indeterminata (sarà un caso se viene chiamata così?).

Osservazione 3.1 *Si osservi che sulla base della definizione data si ha che due polinomi sono uguali sse coincidono in quanto successioni a valori in $A = K[x]$. Si deve prestare attenzione alla differenza che intercorre tra il concetto di* ***funzione polinomiale*** *(comunemente usata in contesti analitici) e il concetto di polinomio. Ad ogni polinomio è associata una funzione polinomiale $F : A \to A$ definita attraverso la notazione simbolica:*

$$b \longmapsto a_n b^n + \cdots + a_1 b + a_0 \in A$$

solitamente detta ***valutazione*** *del polinomio $a_0 + \ldots a_n x^n$ in b. Nel caso dei polinomi definiti su un campo infinito vi è una corrispondenza biunivoca tra funzioni polinomiali e polinomi ma in generale questo non è vero. Si consideri a titolo di esempio l'anello B_0 incontrato nel precedente capitolo e il polinomio $a(x) := x^2 - x$. Allora si vede subito che $a(x)$ ha come funzione polinomiale associata la funzione nulla ma non è il polinomio nullo.*

Definizione 3.2 *Si definisce* ***grado*** *di un polinomio non nullo $a(x) = \sum_i a_i x^i$ il massimo intero n tale $a_n \neq 0$. Il coefficiente a_n viene detto* ***coefficiente direttivo*** *di $a(x)$. Scriveremo $\deg(a(x)) =$. I polinomi di grado 0 incluso il polinomio nullo si dicono costanti.*

Osservazione 3.3 *Se $a(x)$ e $b(x)$ sono due polinomi allora il grado della somma $a(x) + b(x)$ non può ovviamente superare il massimo tra i gradi di $a(x)$ e $b(x)$. Potrebbe però essere minore, ad esempio siano $a(x) = 5x + 1$ e $b(x) = -5x + 2$ in $\mathbb{R}[x]$, allora $a(x) + b(x) = 3$ ha grado 0.*

Per quanto riguarda il prodotto $a(x)b(x)$ di due generici polinomi si ha (pensando alla scrittura simbolica usuale) che il grado è al più pari alla somma dei gradi dei due polinomi.

Lemma 3.4 *Siano $a(x), b(x) \in K[x]$ l'anello di polinomi su un campo K, allora*

(i) $\deg(a(x)+b(x)) \leq \max(\deg(a(x)), \deg(b(x)))$.

(ii) $\deg(a(x)b(x)) = \deg(a(x)) + \deg(b(x))$.

Rimane da considerare se sia sensato attribuire un grado anche al polinomio nullo. Nel caso in cui K è un dominio sarebbe interessante preservare la proprietà $\deg(a(x)b(x)) = \deg(a(x)) + \deg(b(x))$ (Principio di Hankel-Peacock). Questo obbliga a definire

$$\deg(0) = -\infty,$$

dove il segno meno sottintende che tale valore vada considerato come inferiore a qualsiasi altro grado.

Una conseguenza del lemma 3.4 è che $ab = 0$ sse uno dei due fattori è 0. Quindi sia $\mathbb{Z}$ che $K[x]$ sono dei **domini** ossia degli anelli commutativi in cui vale la **la legge di annullamento** del prodotto.

3.1 Algoritmo di divisione sugli Interi

Riprendiamo ed estendiamo a $\mathbb{Z}$ il classico algoritmo di divisione.

Proposizione 3.5 (Algoritmo di divisione) *Siano $a, b \in \mathbb{Z}$, $b \neq 0$. Allora esistono e sono unici $q, r \in \mathbb{Z}$ tali che:*

1. $a = bq + r$.
2. $0 \leq r < |b|$.

Dim. Sostituendo b con $-b$ e q con $-q$, possiamo supporre che $b \in \mathbb{N}$. Iniziamo ad analizzare il caso $a \in \mathbb{N}$.

Sia $R = \{a - bq : q \in \mathbb{Z}\} \cap \mathbb{N}$. Siccome $a \in R$, $R \neq \emptyset$. Pertanto, per il principio di induzione, esiste $r = \min(R)$. Il principio di induzione equivale al principio di buon ordinamento in $\mathbb{N}$, ossia ogni sottoinsieme non vuoto di $\mathbb{N}$ ammette minimo (si veda [Chi09, Chapter 2, Theorem 8]).

Se fosse $r = a - bq \geq b$, potrei scrivere $0 \leq r - b = a - (q+1)b < r$, contro la minimalità di r. Quindi $0 \leq r < b$.

Sia $a < 0$, allora, per il caso precedente, esistono $q', r' \in \mathbb{Z}$ tali che $-a = bq' + r'$, $0 \leq r' < b$. Se $r' = 0$, allora $a = bq$ con $q = -q'$. Altrimenti $r' > 0$ e $a = -b(q'+1) + (b - r')$ e l'asserto è verificato con $q = -(q'+1)$ e $r = b - r'$.

Sia ora $a = bq + r = bq' + r'$ con $r \geq r'$. Allora $b|(r - r')$. Ma $r - r' < b$, quindi $r = r'$ e, di conseguenza $q' = q$. □

Questa dimostrazione si potrebbe tradurre in un algoritmo - non molto efficiente. Si parte da a e si sottrae ($q > 0$) o aggiunge ($q < 0$) b fino ad ottenere un valore in $[0, |b|)$. Il costo computazionale di questo approccio è $|q|$. L'usuale algoritmo che credo insegnino ancora in corsi pre-universitari (Scuola Primaria, Secondaria, ecc...) richiede invece $\log_{10}|q|$ passi. Puntualizzo solo il fatto che questo algoritmo lavora per approssimazioni successive individuando per eccesso