Giorno 31: l'anello dei polinomi

Consideriamo il campo $\mathbb{R}$ (oppure qualunque anello R).

Una funzione $f : \mathbb{R} \to \mathbb{R}$ si dice *polinomiale* se si può scrivere nella forma

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k \tag{1}$$

L'intero k (finito) si chiama il grado del polinomio. L'insieme di tutte le funzioni polinomiali di grado al più k si denota con $\mathbb{P}_k[x]$. Denotiamo invece con $\mathbb{P}[x]$ l'insieme di tutte le funzioni polinomiali di grado qualunque (ma finito).

Possiamo sommare 2 polinomi (sommando i termini simili, cioè le potenze con lo stesso esponente) e otteniamo un polinomio.

Nota: Ad esempio:

$$(3x^2 - 2x) + (x^3 + 2x + 7) = x^3 + 3x^2 + (-2 + 2)x + 7 = x^3 + 3x^2 + 7 \tag{2}$$

Possiamo moltiplicare un polinomio per un numero e abbiamo un altro polinomio.

Nota: Ad esempio:

$$5(3x^2 - 2x) = 15x^2 - 10x \tag{3}$$

Siccome sappiamo le proprietà delle potenze (tra cui $x^n x^m = x^{n+m}$) e sappiamo che vale la proprietà distributiva, possiamo moltiplicare 2 polinomi e otteniamo un polinomio.

Nota: Ad esempio:

$$\begin{aligned}(3x^2 - 2x)(x^3 + 2x + 7) &= 3x^5 - 2x^4 + 6x^3 - 4x^2 + 21x^2 - 14x = \\ &= 3x^5 - 2x^4 + 6x^3 + (-4 + 21)x^2 - 14x = \\ &= 3x^5 - 2x^4 + 6x^3 + 17x^2 - 14x\end{aligned} \tag{4}$$

In altre parole $\mathbb{P}[x]$ è pure un anello con in più l'operazione di moltiplicare gli elementi per un numero, che si definisce *un'algebra*. Abbiamo quindi l'algebra dei polinomi $\mathbb{P}[x]$.

Nota: Notate che i polinomi, essendo elementi di un anello, potete ora pensarli come numeri e manipolarli come tale. L'equazione $2X = Q + 4X$ con $X, Q \in \mathbb{P}[x]$ può essere risolta come $X = -\frac{1}{2}Q$ senza neanche specificare quale polinomio sia Q che entra nell'equazione come un parametro.

Siccome però $\mathbb{P}[x]$ è un anello e non un campo, possiamo avere difficoltà a risolvere equazioni tipo $PX = Q$ perché in genere P non ammette un inversa, nel senso che $1/P$ non è un polinomio (e oltretutto, se P ha zeri, $1/P$ non è neanche una funzione : $\mathbb{R} \to \mathbb{R}$ visto che non è definita sugli zeri).

Ovviamente però la situazione è simile a quella che abbiamo in $\mathbb{Z}$ (che pure è un anello) se consideriamo l'equazione $3x = 6$. Non esiste l'inverso di 3 in $\mathbb{Z}$ ma in questo caso specifico $3|6$, cioè possiamo scrivere $6 = 3 \cdot 2$. Ora l'equazione $3(x - 2) = 0$ è soddisfatta se $3 = 0$ oppure $x - 2 = 0$. Siccome $3 \neq 0$, l'unica soluzione è $x = 2$.

In altre parole, possiamo definire una divisione con resto in $\mathbb{P}[x]$ come abbiamo fatto in $\mathbb{N}$, solo che usiamo il grado del polinomio per approssimare la soluzione.

Ad esempio consideriamo $p(x) = 5x^4 - 3x^2 + 5x - 2$ e $d(x) = 1 - x^2$ e proviamo a calcolare il quoziente d tale che $p = qd + r$ con il grado di r minore del grado di d.

Come prima approssimazione prendiamo un monomio di grado 2, cioè $q_1 = ax^2$ e scegliamo a in modo che il resto $r_1 = p - dq_1$ abbia grado 3, cioè scegliamo $q_1 = -5x^2$ e abbiamo resto $r_1 = 5x^4 - 3x^2 + 5 - 2 + 5x^2(1 - x^2) = 2x^2 + 5x - 2$.

Quindi abbiamo come prima approssimazione

$$5x^4 - 3x^2 + 5x - 2 = (1 - x^2)(-5x^2) + 2x^2 + 5x - 2 \tag{5}$$

e possiamo cercare una seconda approssimazione $q_2 = -5x^2 + bx$ per ridurre il grado del resto r_1

$$2x^2 + 5x - 2 = (1 - x^2)(-2) + 5x \tag{6}$$

Quindi abbiamo

$$5x^4 - 3x^2 + 5x - 2 = (1 - x^2)(-5x^2 - 2) + 5x \tag{7}$$

e *vedrete che questa è la soluzione cercata*.

Nota:

$$\begin{aligned}(1 - x^2)(-5x^2 - 2) + 5x =& -5x^2 - 2 + 5x^4 + 2x^2 + 5x = \\ =& 5x^4 - 5x^2 + 2x^2 + 5x - 2 = p\end{aligned} \tag{8}$$

Ora sappiamo fare le divisioni tra polinomi, possiamo scrivere che $q|p$ quando q divide p con resto nullo. Possiamo definire un *polinomio primo* come un polinomio p (non unità, cioè di grado maggiore di 0) tale che se $p|ab$ allora $p|a$ o $p|b$.

I polinomi di primo grado $\alpha x + \beta$ (con $\alpha \neq 0$) sono primi

Nota: infatti se abbiamo $(\alpha x + \beta)|ab$ significa che $ab = (\alpha x + \beta)q$ e possiamo sempre scrivere $a = q_1(\alpha x + \beta) + r_1$ e $b = q_2(\alpha x + \beta) + r_2$ con $r_1, r_2 \in \mathbb{R}$.

Ma allora

$$\begin{aligned}ab =& (q_1(\alpha x + \beta) + r_1)(q_2(\alpha x + \beta) + r_2) = \\ =& (q_1 q_2(\alpha x + \beta) + r_1 q_2 + r_2 q_1)(\alpha x + \beta) + r_1 r_2\end{aligned} \tag{9}$$

e confrontando con $ab = (\alpha x + \beta)q$ dobbiamo avere $r_1 r_2 = 0$, che è vero se e solo se $r_1 = 0$ o $r_2 = 0$ che corrispondono a dire che $(\alpha x + \beta)|a$ o $(\alpha x + \beta)|b$.

Se consideriamo i polinomi su $\mathbb{R}$, ci sono polinomi di secondo grado che non sono prodotto di polinomi di primo grado (e.g. $x^2 + 1$).

Nota: Il polinomio $x^2 + 1$ è primo (a meno che non lo si consideri come un polinomio complesso).

Al contrario, quando definiremo i numeri complessi, i polinomi complessi sono primi se e solo se sono di primo grado che sostanzialmente si chiama *teorema fondamentale dell'algebra*.