Facoltà di Ingegneria

Precorso di Matematica

Parte III : Algebra Polinomiale

1. Richiami sulle potenze

Ricordiamo brevemente la nozione di *potenza di un numero reale* e le relative proprietà fondamentali:

1.1. Definizione. Siano $a \in \mathbb{R}$ e $n \in \mathbb{N}^*$. Si dice *n-esima potenza di a* il numero reale:

$$a^n := a \cdot a \cdot \cdots \cdot a \quad (n \text{ volte}).$$

Il numero a si dice *base* della potenza e il numero n si dice *esponente*.

E' immediato dimostrare le seguenti proprietà:

1.2. Proposizione. *Siano $a \in \mathbb{R}$ e $n \in \mathbb{N}^*$. Allora valgono:*

i) il prodotto di due potenze di ugual base è uguale ad una potenza che ha per base la stessa base e per esponente la somma degli esponenti, cioè

$$a^n \cdot a^m = a^{n+m} \ ;$$

ii) il quoziente di due potenze di ugual base è uguale ad una potenza che ha per base la stessa base e per esponente la differenza degli esponenti, cioè

$$\frac{a^n}{a^m} = a^{n-m} \ , \quad \text{ove } a \neq 0 \text{ e } n > m;$$

iii) la potenza di una potenza è uguale ad una potenza di ugual base elevata ad un esponente uguale al prodotto degli esponenti, cioè

$$(a^n)^m = a^{nm} \ .$$

E' immediato estendere la nozione di potenza agli esponenti interi negativi o nulli. Infatti, ammettendo anche il caso $n \leq m$ nella proprietà *ii*), e tenendo conto che la base, in questo caso, deve essere non nulla, si pone in modo naturale la seguente:

1.3. Definizione. Siano $a \in \mathbb{R}^*$ e $n \in \mathbb{Z}$. Allora

$$a^n := \begin{cases} a \cdot a \cdot \cdots \cdot a, & \text{se } n > 0 \\ 1, & \text{se } n = 0 \\ 1/a^{-n}, & \text{se } n < 0. \end{cases}$$

1.3.1. Esempio. Dalla definizione: $2^3 = 2 \cdot 2 \cdot 2 = 8$; $2^0 = 1$; $2^{-3} = 1/2^3 = 1/8$.
Inoltre: $10.000 = 10^4$ e $0,00000001 = 1/10.000.000 = 10^{-7}$.

Richiamiamo la ben nota

1.4. Definizione. Siano $a \in \mathbb{R}$, $a > 0$ e $n \in \mathbb{N}^*$. Si dice *radice n-esima* di a l'unico numero reale positivo b tale che $b^n = a$ e si denota: $b = \sqrt[n]{a}$.

L'esistenza e l'unicità di tale numero si prova utilizzando i numeri complessi.
Analogamente a quanto visto prima per le potenze a esponente intero negativo, si può definire una potenza a esponente razionale "estendendo " la proprietà *iii*) di 1.2. Infatti osservando che $\sqrt[n]{a^n} = 1$, è naturale dare la seguente

1.5. Definizione. Siano $a \in \mathbb{R}$, $a > 0$ e $n, m \in \mathbb{N}$, con $m \neq 0$. Allora:

$$a^{\frac{n}{m}} = \sqrt[m]{a^n} \quad \text{in particolare} \quad a^{\frac{1}{m}} = \sqrt[m]{a}.$$

1.5.1. Esempio. Dalla definizione: $7^{\frac{2}{3}} = \sqrt[3]{7^2}$ e $7^{\frac{3}{2}} = \sqrt[2]{7^3} = 7 \cdot \sqrt[2]{7}$.

2. Polinomi

2.1. Definizione. Sia K un campo. Si dice *polinomio* nella variabile X *a coefficienti in* K un'espressione del tipo

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 = \sum_{i=0}^{n} a_i X^i$$

ove $a_i \in K$, $n \in \mathbb{N}$.
L'insieme dei polinomi a coefficienti in K si denota con $K[X]$.

2.2. Osservazione. Con le operazioni analoghe a quelle definite in $\mathbb{Z}[X]$ (vedi 2.1.2), si verifica che $K[X]$ è un anello, detto *anello dei polinomi a coefficienti in* K.

2.2.1. Esempio. Gli insiemi $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ sono anelli.
Notiamo che, poiché $\mathbb{Z} \subset \mathbb{Q}$, anche $\mathbb{Z}[X] \subset \mathbb{Q}[X]$, cioè ogni polinomio a coefficienti interi si può pensare con coefficienti razionali.

Al lettore sarà familiare la terminologia relativa ai polinomi, che, per comodità riassumiamo brevemente:

2.3. Definizione. Un polinomio del tipo $aX^p \in K[X]$, con $a \in K^*$, si dice *monomio* e p è detto *grado* del monomio. Scriveremo $p = deg(aX^p)$.
Se $p(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in K[X]$ è un polinomio a coefficienti in K, allora $a_i X^i$, con $a_i \neq 0$, si dice *monomio di grado i* di $p(X)$. Si definisce *grado* di $p(X)$ il massimo dei gradi dei suoi monomi non nulli; cioè, se $a_n \neq 0$, allora $deg(p(X)) = n$.

2.4. Osservazione. Si verificano facilmente le seguenti proprietà: sia K un campo e siano $f(X), g(X) \in K[X]$; allora:
i) $deg(f(X) + g(X)) \leq \max\{deg(f(X)), deg(g(X))\}$;
ii) $deg(f(X) \cdot g(X)) = deg(f(X)) + deg(g(X))$.
Notiamo che in *i*) vale "$\leq$"; ad esempio se $f(X) = X^3 + X^2 - 1$ e $g(X) = -X^3 + 3X^2 + X$, allora $f(X) + g(X) = 4X^2 + X - 1$.

Quindi $deg(f(X)+g(X))=2$, mentre $deg(f(X))=deg(g(X))=3$.
La *ii*) discende direttamente dalla definizione di prodotto.

E' noto l'algoritmo di divisione fra polinomi a coefficienti razionali. La procedura è analoga per polinomi a coefficienti in un campo qualunque. Si ha dunque:

2.5. Teorema. *Sia K un campo e $f(X), g(X) \in K[X]$ tali che $g(X)$ non è il polinomio nullo e $deg(g(X)) \leq deg(f(X))$. Allora esistono e sono unici due polinomi $q(X), r(X) \in K[X]$ tali che:*

$$f(X) = g(X) \cdot q(X) + r(X)$$

ove $deg(r(X)) < deg(g(X))$. Il polinomio $q(X)$ si dice quoziente e il polinomio $r(X)$ si dice resto della divisione di f per g. •

2.6. Definizione. Se $f(X), g_1(X), g_2(X) \in K[X]$ e vale

$$f(X) = g_1(X) \cdot g_2(X)$$

si dice che $f(X)$ si *fattorizza* in $K[X]$, che $g_1(X)$ e $g_2(X)$ sono *divisori* di $f(X)$ e che $f(X)$ è un *multiplo* sia di $g_1(X)$ che di $g_2(X)$.

2.7. Definizione. Se un polinomio $f(X) \in K[X]$ non si fattorizza in polinomi di $K[X]$ tutti di grado strettamente minore diremo che $f(X)$ è *irriducibile* in K. Diremo che è *riducibile* altrimenti.

2.7.1. Esempio. Il polinomio $f(X) = 2X^2 - 4 \in \mathbb{Q}[X]$ si fattorizza in

$$2X^2 - 4 = 2(X^2 - 2)$$

ma non possiamo dedurre che è riducibile in $\mathbb{Q}$ perché tale fattorizzazione è banale: non tutti i divisori hanno grado strettamente minore di 2! In effetti è irriducibile in $\mathbb{Q}$, in quanto se fosse

$$2X^2 - 4 = 2(X^2 - 2) = 2(X - \alpha)(X - \beta)$$

dovrebbe essere $\beta = -\alpha$ e $\alpha^2 = 2$, con $\alpha \in \mathbb{Q}$. Ma ciò è impossibile.
Tuttavia lo stesso polinomio pensato a coefficienti reali è riducibile! Infatti $f(X) = 2X^2 - 4 \in \mathbb{R}[X]$ si fattorizza in

$$2X^2 - 4 = 2(X^2 - 2) = 2(X - \sqrt{2})(X + \sqrt{2}).$$

Un buon criterio per la divisibilità per un polinomio di primo grado (cioè un binomio) è il seguente risultato, di cui omettiamo la dimostrazione, ottenibile come facile applicazione di 2.5:

2.8. Teorema. *Sia $f(X) \in K[X]$ e $\alpha \in K$. Allora:*

$$f(X) \text{ è divisibile per } X - \alpha \iff f(\alpha) = 0.$$

2.8.1. Esempio. Sia $f(X) = 2X^3 - X^2 + 3X - 4$. Si vede immediatamente che $f(1) = 0$, dunque $f(X)$ è divisibile per $X - 1$. Infatti, operando la divisione, si ottiene:

$$2X^3 - X^2 + 3X - 4 = (X - 1) \cdot (2X^2 + X + 4).$$

E' chiaro, dal teorema precedente, che il problema della riducibilità di un polinomio $f(X)$ è legato alla determinazione di quei numeri α per cui $f(\alpha) = 0$. Tali numeri si dicono *radici* o *zeri* del polinomio f.

2.9. Osservazione. Dal teorema 2.8 segue che, se $\alpha_1, \ldots, \alpha_n$ sono radici di un polinomio $f(X)$, allora f è divisibile per $X - \alpha_1, \ldots, X - \alpha_n$, cioè:

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n) \cdot g(X)$$

dove $g(X)$ è un opportuno polinomio. Da ciò e da 2.4 *ii)* si ha che: $deg(f) = n + deg(g)$; in particolare $n \leq deg(f)$. Dunque il numero di radici di un polinomio è minore o uguale al suo grado. Vediamo alcuni esempi:

2.9.1. Esempio. Il polinomio $f(X) = X^2 - 3 \in \mathbb{R}[X]$ ha grado 2 e anche 2 radici in $\mathbb{R}$: $\sqrt{3}$ e $-\sqrt{3}$. Infatti $X^2 - 3 = (X - \sqrt{3})(X + \sqrt{3})$.
Lo stesso polinomio, pensato in $\mathbb{Q}[X]$, è invece irriducibile, infatti non ha radici in $\mathbb{Q}$.

L'esempio precedente mostra che ci sono polinomi a coefficienti in $\mathbb{Q}$ che hanno un numero di radici strettamente minore del loro grado. Ciò può accadere anche se i coefficienti sono reali:

2.9.2. Esempio. Il polinomio $f(X) = X^2 + 1 \in \mathbb{R}[X]$ ha grado 2 ma nessuna radice in $\mathbb{R}$, dunque è irriducibile. E' naturale chiedersi se accade qualcosa di analogo a 2.9.1, cioè se esiste un campo, contenente $\mathbb{R}$, in cui tale polinomio abbia radici.

3. Numeri complessi

Intuitivamente "aggiungiamo" a $\mathbb{R}$ una radice del polinomio a coefficienti reali $X^2 + 1$; denotiamo tale numero con i. Se consideriamo il più piccolo campo che contenga $\mathbb{R}$ ed i, esso deve sicuramente contenere tutte le possibili somme e prodotti di tali elementi. Diamo dunque la seguente

3.1. Definizione. Un *numero complesso* è un'espressione formale del tipo

$$z = a + ib\ , \quad \text{dove} \quad a, b \in \mathbb{R}.$$

Il numero reale a si dice *parte reale* e il numero reale b si dice *parte immaginaria* di z; in simboli:

$$a = Re(z), \quad b = Im(z).$$

L'insieme di tutti i numeri complessi si denota con $\mathbb{C}$, cioè

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}.$$

Lasciamo al lettore la verifica del seguente risultato:

3.2. Proposizione. *Si definiscano in* $\mathbb{C}$ *le seguenti operazioni:*

$$(a+ib)+(c+id) := (a+b)+i(c+d)$$
$$(a+ib)\cdot(c+id) := (ac-bd)+i(bc+ad).$$

Si pongano inoltre $0_{\mathbb{C}} = 0_{\mathbb{R}} + i0_{\mathbb{R}}$ *e* $1_{\mathbb{C}} = 1_{\mathbb{R}} + i0_{\mathbb{R}}$. *Allora, rispetto a tali operazioni ed elementi speciali,* $\mathbb{C}$ *è un campo.* •

3.2.1. Esempio. Calcoliamo le seguenti operazioni in $\mathbb{C}$:

$$(2+3i)+(1-2i) = 3+i; \quad (2+3i)\cdot(1-2i) = 8-i.$$

Inoltre, poiché $\mathbb{C}$ è un campo, ogni elemento non nullo ammette inverso; ad esempio: $(2+3i)^{-1} = (2/13) - i(3/13)$ e, in generale:

$$(a+ib)^{-1} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2} = \frac{1}{a^2+b^2}(a-ib).$$

3.3. Osservazione. Si noti che nell'enunciato di 3.2 i segni "+" e "·" assumono significati differenti a seconda del contesto. Inoltre, utilizzando la definizione di prodotto, si verifica immediatamente che $i^2 = -1$ e ciò concorda con quanto illustrato all'inizio del paragrafo.

3.4. Osservazione. E' evidente che il polinomio $X^2+1 \in \mathbb{C}[X]$ è riducibile, in quanto i e $-i$ sono sue radici; dunque

$$X^2+1 = (X+i)(X-i).$$

Questo non sorprende, in quanto si è ampliato $\mathbb{R}$ ad un campo che contiene anche una radice di tale polinomio. Ma il fatto sorprendente è che questo nuovo campo dei numeri complessi contiene tutte le radici di *ogni* polinomio a coefficienti reali. Ricordiamo questo importante risultato:

3.5. Teorema fondamentale dell'algebra. *Sia* $f(X)$ *un polinomio a coefficienti reali. Allora* f *ammette almeno una radice complessa. Più precisamente, se* $n = deg(f)$, *allora esistono* n *radici di* f *in* $\mathbb{C}$; *equivalentemente, poste* $z_1, \ldots, z_n$ *tali radici, il polinomio* f *si fattorizza completamente in* $\mathbb{C}$:

$$f(X) = a(X-z_1)(X-z_2)\cdots(X-z_n).$$

•

Un risultato ancora più generale dice che:

3.6. Teorema. *Sia* $f(X) \in \mathbb{C}[X]$ *un polinomio a coefficienti complessi di grado* n. *Allora esistono* n *radici di* f *in* $\mathbb{C}$; *cioè il polinomio* f *si fattorizza completamente in* $\mathbb{C}$. •

La proprietà suddetta si riassume dicendo che $\mathbb{C}$ è un campo *algebricamente chiuso.*