

POLINOMI IN UN'INDETERMINATA A COEFF. REALI

(20)

... Che c'entra?

Immagini tutto come sono fatti?

$$a(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 + \dots + a_n x^n = \sum_{i=0}^n a_i x^i \quad a_i \in \mathbb{R} \quad n \in \mathbb{N}$$

Formalmente: stringhe di lunghezza variabile:

$$(a_0, a_1, a_2, \dots, a_n) \quad a_i \in \mathbb{R}, n \in \mathbb{N}$$

o successioni "definitivamente nulle". *gli x^i sono segnaposto*

Scrittura ordinaria: $a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$.

Per le cose che vado a dire potrei anche prendere coefficienti in \mathbb{Q} o in \mathbb{C} o in un qualunque campo (vedi fine corso), ma non in \mathbb{Z} .

Indico l'insieme dei polinomi a coefficienti in \mathbb{R} in 1 indeterminate x con la scrittura $\mathbb{R}[x]$.

Grado del polinomio $a(x) = \max_{i \geq 0} \text{grado } a_i$

$$\text{grado } (2x+1) = 1$$

$$\text{grado } (\sqrt{2}x^2) = 2$$

$$\text{grado } (-5) = 0 \rightarrow 0 \in \mathbb{R}[x] ? \downarrow \text{Sì}$$

$$\text{grado } (0) = ?? \text{ per convenzione: } -\infty$$

Infatti non possiamo dire che è 0 ($a_0 = 0!$)

e ci piace poter dire che $\forall a(x), b(x) \in \mathbb{R}[x]$

si ha

$$\text{grado } (a(x) \cdot b(x)) = \text{grado } a(x) + \text{grado } b(x)$$

con $b(x) = 0$, $a(x) \cdot b(x) = 0$:

$$-\infty = \text{grado } (a(x) \cdot b(x)) = \text{grado } a(x) + (-\infty)$$

*a_i coefficienti
x indeterminata
... variabile?*

ATTENZIONE:

(21)

Non sono polinomi: $\frac{1}{x+1}$, x^{-1} , $\sqrt{x}-1$, $x^{3/2}+2\dots$

Sono polinomi a coeff. in \mathbb{R} : $\frac{1}{2}$, $\frac{\sqrt{3}+x}{2}$, $\frac{1-3x^2}{5}, \dots$

Domanda: quali dei precedenti polinomi appartengono anche a $\mathbb{Q}[x]$?

In $\mathbb{R}[x]$ sono definiti somma e prodotto e valgono proprietà del tutto analoghe a quelle viste in \mathbb{Z} .

In particolare ci sono due polinomi neutri rispetto alle 2 operazioni:

$0 = 0x^0$ polinomio nullo (o zero)

$1 = 1x^0$ polinomio unità

Per ogni polinomio $a_0 + a_1x + a_2x^2 + \dots + a_nx^n = a(x)$ c'è un polinomio "opposto": $-a_0 - a_1x - a_2x^2 - \dots - a_nx^n$ che sommato ad $a(x)$ dà il polinomio 0
... ma solo alcuni polinomi sono dotati di "reciproco".

Infatti se $b(x) = b_0 + b_1x + \dots + b_mx^m \in \mathbb{R}[x]$ ha grado m

$a(x) \cdot b(x)$ ha grado $n+m$

$\Rightarrow a(x) \cdot b(x)$ può essere 1 solo se $n+m=0$
cioè solo se $n=m=0$.

Dunque hanno "reciproco" solo i polinomi "costanti": $a(x) = a_0$ con $a_0 \neq 0$.

Questi polinomi giocano in $\mathbb{R}[x]$ lo stesso ruolo che ± 1 giocano in \mathbb{Z} .

DEF. Siano $a(x), b(x) \in \mathbb{R}[x] \setminus \{0\}$. Se $\exists q(x) \in \mathbb{R}[x]$
t.c.

$$a(x) = b(x) \cdot q(x)$$

dico che $b(x)$ divide $a(x)$ e scrivo $b(x) | a(x)$.

ESEMPI .

- 1) $2x+1$ divide $4x+2$ $4x+2 = 2 \cdot (2x+1)$: SI
- 2) $4x+2$ divide $2x+1$ $2x+1 = \frac{1}{2} \cdot (4x+2)$: SF
- 3) in generale: se $b(x)$ divide $a(x)$, $\forall k \in \mathbb{R} \setminus \{0\}$:
 - $k b(x)$ divide $a(x)$
 - $b(x)$ divide $k a(x)$
- 4) $x-1$ divide $x^2 - 2x + 1 = (x-1)(x-1)$ SI
- 5) $x+1$ " $x^3 + 1$ ma non $x^2 + 1$
 $x^3 + 1 = (x+1)(x^2 - x + 1)$ vedi PAG 22 bis

Si porta avanti come in \mathbb{Z} la teoria della
divisibilità

TEOR. del quoziente e del resto (algoritmo della divisione)

Siano $a(x), b(x) \in \mathbb{R}[x]$ e $b(x) \neq 0$. Esistono
e sono unici i polinomi $q(x)$ e $r(x)$ tali che

1. $a(x) = b(x) \cdot q(x) + r(x)$
2. $r(x) = 0$ oppure grado $r(x) <$ grado $b(x)$.

L'algoritmo che andiamo a illustrare ha
termine poiché il grado è un numero intero
non negativo e quindi in un numero di
passaggi pari al più a (grado $b(x)$) si arriva
in fondo.

$q(x)$ = quoziente , $r(x)$ = resto nelle divisione
di $a(x)$ per $b(x)$

Se $x+1$ dividesse x^2+1 dovei avere

$$x^2+1 = (x+1)(ax+b)$$

(il grado del
quoziente deve essere
= al grado del
dividendo - il
grado del divisore)

Cioè

$$x^2+1 = ax^2 + (a+b)x + b$$

Cioè (2 polinomi sono uguali se
hanno i coefficienti ordinatamente
uguali)

$$\begin{cases} a=1 \\ a+b=0 \\ b=1 \end{cases}$$

IMPOSSIBILE poiché $1+1 \neq 0$

ESEMPI

- 1) $a(x)=0 \quad b(x) \neq 0 \Rightarrow a(x)=b(x) \cdot 0 + 0$
quoziente e resto sono nulli
- 2) grado $a(x) < \text{grado } b(x) \Rightarrow a(x)=b(x) \cdot 0 + a(x)$
quoziente nullo, resto $a(x)$
- 3) $b(x)=b_0 \neq 0 \Rightarrow$ il resto, se fosse $\neq 0$ dovrebbe
avere grado < 0 ???

in realtà $b_0 \neq 0 \Rightarrow \exists \frac{1}{b_0} \Rightarrow$

$$a(x) = b(x) \left(\frac{1}{b_0} a(x) \right) + 0$$

$$\text{ad es. se } a(x) = 3x^2 + 1 \text{ e } b(x) = -2$$

$$q(x) = -\frac{1}{2}(3x^2 + 1) = -\frac{3}{2}x^2 - \frac{1}{2} \text{ e } r(x) = 0,$$

$$4) \quad a(x) = 4x^4 + 3x^2 + x - 1 \quad b(x) = x^2 + 1$$

<p>dividendo iniziale $\rightarrow 4x^4 + 3x^2 + x - 1$</p> $\begin{array}{r} -4x^4 - 4x^2 \\ \hline -x^2 + x - 1 \end{array}$ <p>dividendo corrente \rightarrow</p> $\begin{array}{r} x^2 + 1 \\ \hline x \end{array}$ <p>dividendo corrente \rightarrow</p> <p>resto: grado < 2</p>	<p><u>Divisione tra termine diretto del dividendo e del divisore</u></p> <p>$\frac{4x^4}{x^2} = 4x^2$</p> <p>$\frac{-x^2}{x^2} = -1$</p> <p>$a(x) = b(x) \cdot (4x^2 - 1) + x$</p>
---	---

$$5) \quad a(x) = 4x^4 + 3x^2 + x - 1 \quad b(x) = x - 1$$

$$\begin{array}{r}
 4x^4 + 3x^2 + x - 1 \\
 - 4x^4 + 4x^3 \\
 \hline
 4x^3 + 3x^2 + x - 1 \\
 - 4x^3 + 4x^2 \\
 \hline
 7x^2 + x - 1 \\
 - 7x^2 + 7x \\
 \hline
 8x - 1 \\
 - 8x + 8 \\
 \hline
 7
 \end{array}$$

$$\begin{array}{r} x - 1 \\ \hline 4x^3 + 4x^2 + 7x + 8 \end{array}$$

$$a(x) = b(x) \cdot (4x^3 + 4x^2 + 7x + 8) + 7$$

Dal teor. del quoz. e del resto segue che se il divisore ha grado 1, il resto o è zero o ha grado zero



Teor di Ruffini. Siano $a(x) \in \mathbb{R}[x]$ e $b(x) = x + b_0$. Il resto nella divisione di $a(x)$ per $b(x)$ è il valore $a(-b_0)$

che la funzione polinomiale $a(x)$ assume in $(-b_0)$. In particolare

$$a(x) \text{ è divisibile per } b(x) \Leftrightarrow a(-b_0) = 0.$$

$$\text{Dim. } a(x) = (x + b_0)q(x) + r \text{ ove } r \in \mathbb{R}$$

$$\Rightarrow a(-b_0) = (-b_0 + b_0)q(-b_0) + r = 0 + r = r \quad \blacksquare$$

ESEMPI

1) Nel precedente esempio 5, $b_0 = -1$, $a(1) = 4 + 3 + 1 - 1 = 7$. E infatti il resto era 7.

2) $a(x) = x^3 - 3x + 3$ è divisibile per $b(x) = x + 1$?

$$a(-1) = -1 + 3 + 3 = 5 = \text{resto} \neq 0 : \text{NON È DIVISIBILE}$$

Come ricavare i coefficienti del quoziente senza scrivere per esteso l'algoritmo?

-1	1	0	-3	3
		-1	1	2
	1	-1	-2	5

$$a(x) = b(x)(x^2 - x - 2) + 5$$

3) $a(x) = x^4 - 3x^2 + 2$ è divisibile per $b(x) = x - \sqrt{2}$?

$$a(\sqrt{2}) = (\sqrt{2})^4 - 3(\sqrt{2})^2 + 2 = 4 - 3 \cdot 2 + 2 = 0 : \text{SI È DIVISIBILE}$$

4) $a(x) = 2x^3 - 3x^2 + 3x - 1$ è divisibile per $b(x) = 2x - 1$?

$$b(x) \text{ non è della forma } x + b_0 \text{ ma } b(x) = 2(x - \frac{1}{2}) \dots$$

$$a(x) = 2x^3 - 3x^2 + 3x - 1$$

$$b(x) = \textcircled{2}x - 1$$

Non posso applicare Ruffini ma posso applicarlo

$$\alpha \quad \frac{1}{2} b(x) = x - \frac{1}{2}$$

$$\begin{array}{c|ccc|c} & 2 & -3 & 3 & -1 \\ \frac{1}{2} & & 1 & -1 & 1 \\ \hline & 2 & -2 & 2 & 0 \end{array}$$

Quindi $\frac{1}{2} b(x)$ divide $a(x)$

$\Rightarrow b(x)$ divide $a(x)$

$$\begin{aligned} Q(x) &= \left(x - \frac{1}{2}\right)(2x^2 - 2x + 2) + 0 = \\ &= (2x - 1)(x^2 - x + 1) \end{aligned}$$

Terminologia

Sia $a(x) \in \mathbb{R}[x]$ e $k \in \mathbb{R}$. Se $a(k) = 0$ si vuol dire che

- k è una radice del polinomio $a(x)$ oppure che

- k è una soluzione dell'equazione $a(x) = 0$

Il teor. di Ruffini afferma che le radici di un polinomio $a(x)$ sono tutti e soli i $k \in \mathbb{R}$ tali che $a(x)$ è divisibile per $(x-k)$.

Quest'osservazione è importante quando si voglia scomporre il polinomio nel prodotto di pol. irriducibili.

DEF. Sia $a(x) \in \mathbb{R}[x]$ e sia grado $a(x) \geq 1$

Dico che $a(x)$ è riducibile se esistono due pol. $b(x), c(x) \in \mathbb{R}[x]$ entrambi di grado minore del grado di $a(x)$ tali che

$$a(x) = b(x)c(x).$$

garantisce
che non
esiste il
polinomio
reciproco.

In caso contrario dico che $a(x)$ è irriducibile

ESEMPI

1) $2x+4$ è irriducibile in $\mathbb{R}[x]$

2) $x^2 - 1$ è riducibile in $\mathbb{R}[x]$: $(x+1)(x-1)$

3) $x^2 - 2$ è riducibile in $\mathbb{R}[x]$: $(x+\sqrt{2})(x-\sqrt{2})$
ma non lo è in $\mathbb{Q}[x]$

4) $x^2 + 1$ è irriducibile in $\mathbb{R}[x]$
ma non lo è in $\mathbb{C}[x]$: $(x+i)(x-i)$

OSSERVAZIONI

- 1) un polinomio di grado 1 è sempre irriducibile
 2) per un polinomio di grado > 1 l'irriducibilità dipende dall'insieme in cui variano i coefficienti.

In particolare in $\mathbb{C}[x]$ vale il teorema fondamentale dell'algebra: ogni polinomio di grado n è prodotto di n polinomi di 1° grado a coefficienti in \mathbb{C} .

Quindi in $\mathbb{C}[x]$ gli unici polinomi irriducibili sono quelli di 1° grado.

↓ vedi pag 26 bis

in $\mathbb{R}[x]$ gli unici polinomi irriducibili sono quelli di 1° grado e quelli di 2° grado: $ax^2+bx+c=0$ con discriminante $\Delta = b^2 - 4ac$ negativo.

Ad es. x^4+1 in $\mathbb{C}[x]$ si rappresenta come

$$x^4+1 = \left(x - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right) \underbrace{\left(x - \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)}_{\text{in } \mathbb{R}[x] \text{ come}} \underbrace{\left(x + \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)}_{\text{in } \mathbb{R}[x] \text{ come}} \left(x + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)$$

$$x^4+1 = (x^2+1)^2 - 2x^2 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$$

IRRIDUC. IN $\mathbb{R}[x]$ poiché $\Delta = 2 - 4 < 0$

Come negli interi, si mostra che un polinomio $a(x) \in \mathbb{R}[x]$ è irriducibile se e solo se è primo cioè se

$$a(x) \mid b(x) \cdot c(x) \text{ e } a(x) \nmid b(x) \Rightarrow a(x) \mid c(x)$$

Poiché in $\mathbb{R}[x]$ gli unici polinomi irriducibili sono quelli di 1° grado e quelli di 2° grado con $\Delta < 0$?

Ragiono così : $a(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{R}[x]$ può essere visto come un polinomio di $\mathbb{C}[x]$ poiché $\mathbb{R} \subseteq \mathbb{C}$.

\Rightarrow (T.F.A.) in \mathbb{C} esistono z_1, z_2, \dots, z_n (eventualmente non tutti distinti) tali che

$$a(z_k) = 0 \quad \forall k = 1, 2, \dots, n$$

e quindi (Ruffini)

$$a(x) = a_n (x - z_1)(x - z_2) \cdots (x - z_n).$$

Considero il coniugato di $a(z_k)$:

$$\overline{a(z_k)} = \bar{a}_0 + \bar{a}_1 \bar{z}_k + \dots + \bar{a}_n \bar{z}_k^n = \bar{0} = 0$$

e, poiché $a_j = \bar{a}_j$ ^(*) $\forall j = 0, 1, \dots, n$, questo significa

$a(\bar{z}_k) = 0$: anche \bar{z}_k è radice di $a(x)$.

Quindi le radici di $a(x)$ in \mathbb{C} o sono reali o sono a due a due coniugate.

Se $z_k = \alpha + \beta i$ e $z_h = \bar{z}_k = \alpha - \beta i$ si ha :

$$(x - z_k)(x - z_h) = x^2 - (\alpha + \beta i + \alpha - \beta i)x + (\alpha + \beta i)(\alpha - \beta i) = \\ = x^2 - 2\alpha x + \alpha^2 + \beta^2.$$

Questo è un polinomio di 2° grado a coefficienti reali con

$$\frac{\Delta}{4} = \alpha^2 - (\alpha^2 + \beta^2) = -\beta^2 < 0, \text{ poiché } \beta \neq 0.$$

(*) $a_j \in \mathbb{R} \Leftrightarrow \operatorname{Im}(a_j) = 0 \Leftrightarrow a_j = \bar{a}_j$

(27)

Si fatti anche in $\mathbb{R}[x]$ vale l'algoritmo euclideo delle divisioni successive che permette di dimostrare l'esistenza (e di calcolare) un H.C.D. tra due polinomi non nulli.

NOTA : in $\mathbb{R}[x]$ i H.C.D. ($a(x), b(x)$) sono infiniti, poiché se $d(x)$ è uno di essi e $k \in \mathbb{R} \setminus \{0\}$ anche $k \cdot d(x)$ è un H.C.D. ($a(x), b(x)$).

ESEMPIO . Trovare M.C.D. ($a(x), b(x)$) ove

$$a(x) = 4x^4 - 3x^3 + 4x^2 + 1 \quad b(x) = x^3 + 1$$

$$\begin{array}{r}
 \begin{array}{c}
 4x^4 - 3x^3 + 4x^2 + 1 \\
 -4x^4 - 4x \\
 \hline
 -3x^3 + 4x^2 - 4x + 1 \\
 3x^3 + 3 \\
 \hline
 4x^2 - 4x + 4
 \end{array}
 & \left| \begin{array}{c} x^3 + 1 \\ \hline 4x - 3 \end{array} \right. & \begin{array}{l}
 a(x) = b(x)(4x - 3) + \\
 + 4x^2 - 4x + 4
 \end{array} \\
 & & \begin{array}{l}
 b(x) = (4x^2 - 4x + 4) \cdot \frac{x+1}{4} + 0
 \end{array}
 \end{array}$$

\Downarrow

$$\Rightarrow \text{M.C.D. } (a(x), b(x)) = 4x^2 - 4x + 4 \quad \text{ma anche} \\
 = x^2 - x + 1 \quad \text{ecc.}$$

Anche in $\mathbb{R}[x]$ vale :

TEOR. DI FATTORIZZAZIONE UNICA . Ogni polinomio di grado ≥ 1 di $\mathbb{R}[x]$ si può scomporre in modo "essenzialmente" unico come prodotto di polinomi irriducibili in $\mathbb{R}[x]$.

- ▷ può cambiare l'ordine dei fattori
- qualche fattore può cambiare per un coefficiente multiplo $\neq 0$

Ad es. $3x^2 - 3 = (3x - 3)(x + 1) = (x + 1)(3x - 3) =$
 $= (x - 1)(3x + 3) = (3x + 3)(x - 1) =$
 $= (\frac{1}{2} - \frac{1}{2}x)(-6x - 6) = (-6x - 6)(\frac{1}{2} - \frac{1}{2}x) = \dots$

Sono considerate come una sola fattorizzazione.

In particolare il teor. di fattorizzazione unica per i polinomi di $\mathbb{R}[x]$ dice che ogni $a(x) \in \mathbb{R}[x]$ si può scomporre in modo essenzialmente unico come prodotto di polinomi di 1° grado o di 2° grado con $\Delta < 0$.

\Rightarrow in $\mathbb{R}[x]$ un polinomio di grado > 2 è sempre riducibile.

Ma ciò non significa che abbia radici reali: le ha se e solo se (teor. di Ruffini) nella scomposizione del polinomio compareno fattori irriducibili di 1° grado.

I due problemi:

- ricerca di fattori di 1° grado di $a(x)$
- ricerca di radici reali di $a(x)$

sono equivalenti.

Se nella scomposizione di $a(x)$ in fattori irriducibili un fattore compare n volte si dice che ha molteplicità (algebrica) n.

Ad es. in

$$a(x) = x^3 (2x+1) (2x^2+2x+1)^2$$

si dice che x ha molteplicità 3,

$$2x+1 \quad " \quad " \quad 1$$

$2x^2+2x+1$ ha molteplicità 2.

Se il fattore ha grado 1 si estende la terminologia alle corrispondenti radici. Così direi che $a(x)$ ha la radice $x=0$ con molteplicità algebrica 3 e la radice $x=-\frac{1}{2}$ " " " 1.

$(\mathbb{Z}, +, \cdot, 0, 1, >)$

Nozione di divisibilità

algoritmo della divisione

algoritmo euclideo
debole divisione
successive per
la determinazione
di M.C.D.(a,b):
ESISTENZA!

rappresentazione
di un intero \mathbb{Z}
in base $m \in \mathbb{Z}$,
 $m > 1$

esistenza e
calcolo di
m.c.m.(a,b)

visibilità
e risoluzione
delle equazioni
lineari di ordine

numeri
primi

teoria di
fattorizzazione
unica di un
numero intero
come prodotto
di irriducibili
= primi

$(\mathbb{R}[x], +, \cdot, 0, 1, \text{grado})$

Nozione di divisibilità

algoritmo della
divisione

T. di
Ruffini

algoritmo
euclideo
per il
calcolo di
M.C.D.(a(x), b(x))

Esistenza

esistenza e
calcolo di
m.c.m.(a(x), b(x))

polim. irriduc.
polin. (primi)

Teor. di
fattorizz.
unica di
a(x) $\in \mathbb{R}[x]$
in polinomi
irriducibili

(R9)