Senior 2017 - A1 MEDIUM Anér

Note Title 9/4/2017

$p(x) = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n$

Def. Un anello è un insieme con due operazioni, $+$ e $\cdot$, con le proprietà che vi aspettate, in particolare

- oltre a $+$ ho anche $-$
- non assumo la divisione

Esempi $\mathbb{Z}$ è l'anello degli interi

$\boxed{\mathbb{Q}, \mathbb{R}, \mathbb{C}}$ sono anelli (di un tipo particolare)

$\mathbb{Z}/n\mathbb{Z}$ è un anello

Esempio/costruzione Se A è un anello, posso definire $A[x] \overset{\text{definizione}}{=} \{$polinomi in x con coefficienti in $A\}$

Def Un campo è un anello in cui ogni elemento $\neq 0$ ammette un inverso molt.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono campi

OSS In $\mathbb{Z}$ vale la legge di annullamento del prodotto: se m e $n \neq 0$, allora $mn \neq 0$

<u>OSS</u> $\mathbb{Z}/10\mathbb{Z}$, per esempio, non ha questa proprietà

$\mathbb{Z}$ è un <u>dominio</u>

<u>Esempio</u> $\mathbb{R}[x]$ è un dominio, come $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{C}[x]$

Posso costruire le frazioni con num. e den. $(\neq 0)$ in un dominio A, e questo sarà un campo $C(A)$

<u>Filosofia</u> A è un dominio, e_i ed e_f elementi di A.

$$\begin{array}{ccccc} A & & C(A) & & \\ \cup & & \cup & & \\ e_i & = & f_1 & = f_2 = f_3 = \dots = f_n = & e_f \end{array}$$

<u>Domanda</u> Esistono anelli $\mathbb{Z} \subsetneq A \subsetneq \mathbb{Q}$?

- $A = \{$ frazioni del tipo $\frac{n}{2^k}\}$ razionali diadici

- $A = \{$ " " " $\frac{n}{2^k \cdot 3^h}\}$

<u>x CASA</u> Gli anelli "tra $\mathbb{Z}$ e $\mathbb{Q}$" sono tutti così: Dato $S \subseteq$ numeri primi, costruiamo

$A = \mathbb{Z}[S^{-1}] = \{$fraz. in cui il den. si fattorizza in $S\}$

Esempio Polinomi di Laurent

$\mathbb{C}[x, x^{-1}] = \{$ scritture del tipo

$a_{-m} x^{-m} + a_{-m+1} x^{-m+1} + \dots + a_0 + \dots + a_n x^n \}$

$= \{$ frazioni algebriche della forma $\frac{p(x)}{x^m} \}$

$$\mathbb{C}[x] \subset \mathbb{C}[x, x^{-1}] \subset C(\mathbb{C}[x]) = \mathbb{C}(x)$$

Se A è un dominio, anche $A[x]$ è un dominio cioè se $p(x), q(x)$ sono polinomi non nulli a coeff. in A, anche $p(x) \cdot p(x) \neq 0 \Rightarrow$ guardo i coefficienti direttivi.

Divisione euclidea

1° caso (noto) i coeff. in un campo C ad esempio $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

$p(x), q(x) \in C[x]$ voglio trovare $r(x)$ e $s(x)$ t.c. $p(x) = q(x) \cdot s(x) + r(x)$ e $\deg r < \deg q$ (oppure $r(x) = 0$)

$p(x) = a_n x^n + \dots + a_0$

$q(x) = b_m x^m + \dots + b_0$

supponiamo $n > m$

divido $\frac{a_n}{b_m}$, e comincio a sottrarre

$\left(\frac{a_n}{b_n}\right) \cdot x^{n-m} \cdot q(x)$ a $p(x)$

2° caso coeff. in un dominio: allargo gli orizzonti e lavoro nel campo delle frazioni (e comunque tutti i denominatori saranno potenze di b_m)

3° caso coeff. in un anello, se il divisore è monico tutto va bene!

Cosa fare con pol. in più variabili?

$\mathbb{C}[x,y]$ $\quad p(x,y) = x^2+y^2 \quad q(x,y) = x^2+xy$

Div. risp. alla x $\quad p(x,y) = q(x,y)\cdot 1 + (y^2 - xy)$

Div. risp. alla y $\quad p(x,y) = q(x,y)\cdot \frac{y}{x} + (x^2 - xy)$

Problema $p(x,y)$ coeff. reali; $\forall n \in \mathbb{N}$ $p(n,n^2) = 0$. Allora p è un multiplo di $y-x^2$.

Divido p per $y-x^2$ usando y come var. principale

$$p(x,y) = s(x,y)\cdot(y-x^2) + r(x,y)$$

$r(x,y)$ ha grado 0 in $y \rightsquigarrow r(x,y) = R(x)$

$R(n) = 0$ $\forall n$ naturale, ma un polinomio a coeff. reali non ha infinite radici!

$R(x) \equiv 0$ e abbiamo finito.

Teo Un polin. $p(x) \in \mathbb{R}[x]$ di grado n ha al massimo n radici distinte.

$p(x)$ se α è radice divido per $(x-\alpha)$, il resto ha grado 0, è un numero, e deve essere 0
$p(x) = (x-\alpha) \cdot p_1(x)$. Prendo β un'altra radice (diversa da α). Poiché $\beta - \alpha \neq 0$, serve $p_1(\beta)=0$
e parte l'induzione...

OSS Lo stesso argomento vale in un campo qualsiasi e perfino in un dominio!

Ma non in un non-dominio!
Se A non è un dominio (esempio $A = \mathbb{Z}/10\mathbb{Z}$)
prendo $a, b \neq 0$ con $a \cdot b = 0$ (esempio $a=2$ $b=5$
$a \cdot b = 10 = 0$)

considero $(x-a)(x-b)$: ha radici
$a, b, 0, a+b$ (nel nostro esempio $2, 5, 0, 7$)

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

Artefatto $(x-y) \mid [p(x) - p(y)]$ dove
$p(t) \in \mathbb{R}[t]$ è un pol. in una variabile

Infatti: $p(t) = a_n t^n + \dots + a_0$

$p(x) - p(y) = a_n(x^n - y^n) + \dots + a_1(x-y)$

Problema x casa $p(t), q(t) \in \mathbb{R}[t]$; $[p(x)-p(y)] \mid [q(x)-q(y)]$. Allora $\exists\, r(t) \in \mathbb{R}[t]$ t.c. $q(t) = r(p(t))$

Un polinomio $p(x)$ in $A[x]$ è irriducibile se non esistono $p_1(x), p_2(x)$ di grado >0 t.c. $p(x) = p_1(x) \cdot p_2(x)$ (supponiamo A dominio)

Teo Ogni polinomio in $A[x]$ ammette un'unica fattorizzazione in irriducibili a meno di permutazioni e riscalamenti dei fattori, per i seguenti A: $\mathbb{Z}$, campi. Vero anche per $A[x,y]$, $A[x,y,z]$, ...

Esempi
- $\mathbb{C}[x]$ qui avrò fattori di grado 1
- $\mathbb{R}[x]$ // // // 1 o 2
- $\mathbb{Q}[x]$ // // // // qualsiasi
- $\mathbb{Z}[x]$ // // // // qualsiasi

Lemma di Gauss Se $p(x) \in \mathbb{Z}[x]$ è un polin.

a coeff. interi (e quindi razionali), allora la fattoriz. in irriducibili in $\mathbb{Z}$ e in $\mathbb{Q}$ sono uguali a meno di riscalamento.

<u>Esempio</u> $(2x+1)(x+2) = 2x^2+5x+2 = \left(x+\frac{1}{2}\right)(2x+4)$

Quindi passando da $\mathbb{Z}$ a $\mathbb{Q}$ le possibilità di fattorizzazione non migliorano

---

Radici razionali di $p(x) \in \mathbb{Z}[x]$: come cercarle?

$p(x) = a_n x^n + \dots + a_0$ e $\frac{a}{b}$ è radice di p

$(a,b)=1$, allora $a \mid a_0$ e $b \mid a_n$

Per dim. che p è irriducibile ho i seguenti mezzi:

- ridurre modulo n (modulo un primo): se $p(x)$ considerato modulo n è irriducibile, allora a maggior ragione p sarà irriducibile. Al contrario

$p(x)$ a coeff. interi. $\quad p(x) = q(x) \cdot r(x)$ a coeff. interi

$p(x) \equiv q(x) \cdot r(x) \mod n$ (cioè come polinomi a coeff. in $\mathbb{Z}/n\mathbb{Z}$)

<u>Esempio</u> $x^3 - 4$ è irriducibile: infatti è irrid. mod 7 (se si fattorizzasse avrebbe un fattore lineare, ma allora 4 sarebbe residuo cubico mod 7, assurdo!)

- Eisenstein. Preliminare: $\mathbb{Z}/n\mathbb{Z}$ non è un dominio se n non è un primo, ma $\mathbb{Z}/p\mathbb{Z}$ è un campo!

Sia $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$

p primo $\quad p \nmid a_n, \; p \mid a_{n-1}, \dots a_1, a_0$

$p^2 \nmid a_0$. $\quad$ Allora f è irriducibile.

<u>Esempio</u> $\quad x^{10} - 10$.

<u>Dim</u> Suppongo per assurdo $f(x) = g(x) \cdot h(x)$ in $\mathbb{Z}[x]$

mod p ho $\quad a_n x^n \equiv g(x) \cdot h(x) \pmod p$

Per la fattorizzazione unica in $\mathbb{Z}/p\mathbb{Z}[x]$ (infatti $\mathbb{Z}/p\mathbb{Z}$ è un campo) ho che

$$g(x) \equiv b x^m \qquad h(x) \equiv c x^l \qquad \text{mod } p$$

$m, l > 0$. Allora $p \mid$ termini noti di g e h, il cui prodotto è a_0, che però non è div. per p^2.

- Terza via: ridurre a un numero finito di tentativi e provarli tutti. Dato $p(x) \in \mathbb{Z}[x]$, un suo divisore ha grado limitato da $\deg p$, ma i coefficienti?

<u>PASSO 1</u> Capire quanto grandi (in modulo) sono le radici complesse di p, usando i coeff. di p

Per semplificare, supponiamo p monico $p(x) = x^n + a_{n-1}x^{n-1} + \dots a_0$

Se $\alpha \in \mathbb{C}$ è radice di p, serve per la triangolare

$$|\alpha|^n \leq |a_{n-1}||\alpha|^{n-1} + \dots + |a_1|\cdot|\alpha| + |a_0|$$

<u>PASSO 2</u> Stimare i moduli dei coeff. di un div. di p avendo una stima sui moduli delle radici di p

$q(x) = x^m + b_{m-1}x^{m-1} + \dots + b_0$ divide p.

Le radici di q sono anche radici di p, in modulo $< N$

$b_0 =$ prodotto radici $\quad |b_0| < N^m$

$b_{m-1} =$ somma radici $\quad |b_{m-1}| < m \cdot N$

Bezout per polinomi in $C[x]$ $\quad C$ un campo.

$p(x), q(x)$ pol. senza fattori irriducibili in comune.

Allora esistono $a(x), b(x) \in C[x]$ per cui

$$a(x)\cdot p(x) + b(x)\cdot q(x) = 1$$

Si usa la divisione euclidea, quindi <u>serve</u> dividere per i coefficienti che di volta in volta si presentano

<u>Esempio</u> $p(x) = x^2 - 2 \qquad q(x) = x$

$$p(x) = q(x)\cdot x \underbrace{-2}_{r(x)} \qquad q(x) = (-2)\cdot \frac{-1}{2}x + 0$$

$$-\frac{1}{2}p(x) + \frac{1}{2}x\,q(x) = 1 \rightsquigarrow -p(x) + x\,q(x) = 2$$

Esempio Proviamo con $\mathbb{C}[x,y]$ $p(x,y)=x$
$q(x,y)=y$. Esistono $a(x,y)$, $b(x,y)$ t.c.

$$a(x,y)\cdot x + b(x,y)\cdot y = 1 \ ?$$ NO perché

a sinistra manca il termine noto
porre $(x,y)=(0,0)$

- $p = x-1$ $\quad q = y-1$

$$a(x,y)(x-1) + b(x,y)(y-1) = 1 \ ?$$

No perché ponendo $(x,y)=(1,1)$

In generale se esistono x_0, y_0 complessi t.c. $p(x_0,y_0)=q(x_0,y_0)=0$
allora non esistono $a(x,y), b(x,y)$ come sopra!

Teo (Hilbert Nullstellensatz) Se $p(x,y)$ e $q(x,y)$ non si annullano simultaneamente su una coppia di complessi (x_0,y_0), allora esistono $a(x,y)$ e $b(x,y)$ come in Bezout. Vale anche per più polinomi e più variabili. Esempio p_1, p_2, p_3, p_4 polinomi in $\mathbb{C}[x,y,z]$. Allora o esiste (x_0,y_0,z_0) che annulla tutti i p_i, oppure esistono polinomi $a_1 \dots a_4 \in \mathbb{C}[x,y,z]$ t.c. $a_1\cdot p_1 + a_2\cdot p_2 + a_3\cdot p_3 + a_4 p_4 = 1$

serve coeff. in $\mathbb{C}$: coeff. reali non funziona!

$p(x,y) = x^2+y^2+1$ Esiste $a(x,y)$ t.c. $a(x,y)\cdot p(x,y)=1$
No perché p ha zeri complessi, anche se

non reali!

Caso ancora più semplice: una variabile: $p(x) = x^2+1$

Serve un campo per cui vale il teorema fond. dell'algebra! (E in effetti basta).

Derivate $p(x) = a_n x^n + \dots + a_0$

$$p'(x) = \frac{d}{dx} p(x) = n \cdot a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1$$

Proprietà fondamentali

(1) Linearità (A) $\frac{d}{dx}\left[p(x) + q(x)\right] = \frac{d}{dx} p(x) + \frac{d}{dx} q(x)$

(B) λ è una costante nell'anello

$$\frac{d}{dx}\left(\lambda \cdot p(x)\right) = \lambda \left(\frac{d}{dx} p(x)\right)$$

(2) Regola di Leibniz: $\frac{d}{dx}\left(p(x) \cdot q(x)\right) = \left[\frac{d}{dx} p(x)\right] \cdot q(x) + p(x) \cdot \left[\frac{d}{dx} q(x)\right]$

(3) $\frac{d}{dx} x = 1$

Proprietà (1), (2), (3) determinano $\frac{d}{dx}$ univocamente

La derivata abbassa il grado $\rightsquigarrow$ permette dim. per induzione sul grado. Ci sono anche altre operazioni che abbassano il grado...

① Divido per $(x-\alpha)$ dove α è una radice

② Tolgo il termine noto e divido per x

③ $p(x+1) - p(x)$ ha grado minore

① $\dfrac{p(x)}{(x-\alpha)} = \dfrac{p(x) - p(\alpha)}{x - \alpha}$

② $\dfrac{p(x) - a_0}{x} = \dfrac{p(x) - p(0)}{x - 0}$

③ $\dfrac{p(x+1) - p(x)}{(x+1) - x}$

$p(x) \in \mathbb{C}[x]$. α è radice doppia di $p(x)$ se e solo se α è radice di $p(x)$ e anche di $p'(x)$

Scrivo $p(x) = (x-\alpha) \cdot q(x)$. Allora

$$p'(x) = 1 \cdot q(x) + (x-\alpha) \cdot q'(x)$$

<u>A che serve?</u> Se ad esempio vogliamo che $p(x)$ sia il $\square$ di un polinomio, è necessario che ogni radice di p compaia almeno 2 volte ...

$$p(x) = (x-\alpha_1)(x-\alpha_2) \cdot \ldots \cdot (x-\alpha_n)$$

$$\frac{d}{dx} p(x) = \sum_{i=1}^{n} (x-\alpha_1) \cdot \ldots \cdot (x-\alpha_{i-1}) \cdot 1 \cdot (x-\alpha_{i+1}) \cdot \ldots \cdot (x-\alpha_n)$$

$$= \sum_{i=1}^{n} \frac{p(x)}{x-\alpha_i}$$

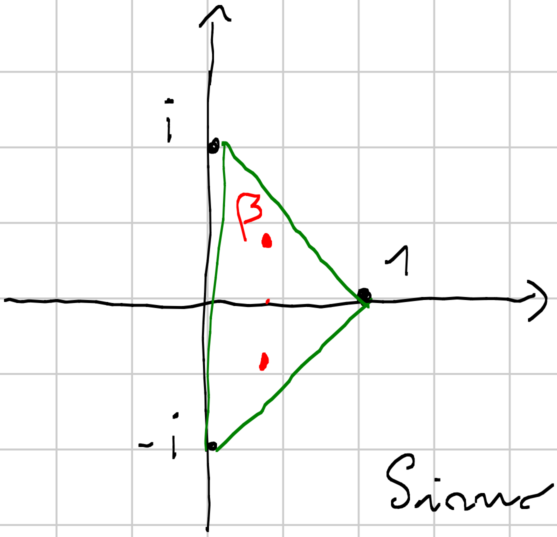
Esempio in $\mathbb{C}$

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

$p'(x) = 3x^2 - 2x + 1$

le radici di p' sono

$\frac{1}{3} \pm \frac{\sqrt{2}}{3} i$



Le radici di p' sono nell'inv. convesso di quelle di p (dentro $\mathbb{C}$)

Verifichiamolo!

Siano $\alpha_1, \ldots, \alpha_n$ le radici di p

Sia β una radice di p'.

OSS 0 è radice di $p'(x+\beta)$. WLOG (con le dovute verifiche...) $\beta = 0$ a meno di traslare

$$p'(x) = \sum_{i=1}^{n} \frac{p(x)}{x-\alpha_i}$$ pongo $x = 0$

$$0 = \sum \frac{p(0)}{-\alpha_i} = -p(0) \cdot \sum \frac{1}{\alpha_i}.$$

Trattiamo il caso $p(0) \neq 0$, ossia $\beta = 0$ non è già radice di p.

$$\sum \frac{1}{\alpha_i} = 0 \qquad \sum \frac{\overline{\alpha_i}}{\overline{\alpha_i} \cdot \alpha_i} = 0$$ coniugo tutto

$$\sum \frac{\alpha_i}{|\alpha_i|^2} = 0$$ Se $\sum \frac{1}{|\alpha_i|^2} = 1$ ho finito,

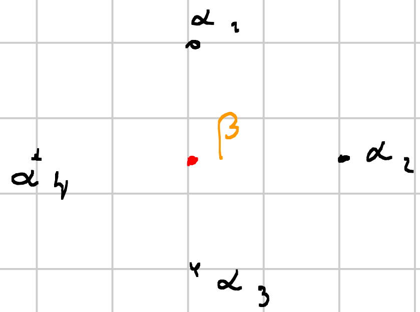
altrimenti divido!

$$\sum_{i=1}^{n} \alpha_i \cdot \boxed{\frac{\frac{1}{|\alpha_i|^2}}{\sum_{j=1}^{n} \frac{1}{|\alpha_j|^2}}} = 0$$ >0

la somma dei coeff ora è 1

Risultato: $\beta = 0 = \sum_{i=1}^{n} \lambda_i \alpha_i$ con $\lambda_i > 0$, $\sum \lambda_i = 1$

Esempio



$$\beta = \frac{1}{2}\alpha_1 + \frac{1}{2}\alpha_3$$
$$= \frac{1}{2}\alpha_2 + \frac{1}{2}\alpha_4$$