ALGEBRA 1 - Medium Session 2019

Titolo nota 31/12/2011

Polinomi.

$$p(x) = a_n x^n + a_{n-1} x^{n-1} \text{ ---- } + a_1 x + a_0$$

$a_0, \dots, a_n$ sono i coff., con $a_n \neq 0$

n = "grado del polinomio"

Proprietà dei polinomi dipendono da dove prendono i coefficienti, in un anello A.

Def. Anello è un insieme $(A, +, \cdot)$ tale che per "+" esiste l'opposto e per "$\cdot$" esiste l'elemento neutro (1)

$0 \in A$, $1 \in A$, $a \in A \Rightarrow -a \in A$

$1 \cdot a = a$

$A[x]$ = "Insieme di polinomi a coeff. in A"

Ex. Se A è un anello allora $A[x]$ è un anello

Esempi: $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{C}$ sono tutti anelli

$\mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}[x], \mathbb{C}[x]$ sono tutti anelli

$\mathbb{Z}/n\mathbb{Z}$ è un anello

Tutto quanto funziona bene se A è un dominio:

cioè se $a, b \in A$ $\quad a \cdot b = 0 \Rightarrow a = 0$ oppure $b = 0$

$\mathbb{Z}/n\mathbb{Z}$ è dominio $\iff$ ($n \mid ab \Rightarrow n \mid a$ o $n \mid b$)

$\Updownarrow$

n è un primo.

Cosa può succedere di male?

Es. $p(x) = (x-3)\cdot(x-4) = x^2 - 7x + 12 \pmod{12}$

$= x^2 - 7x$

3, 4 sono radici di $p(x)$ → 0, 7 sono radici di $p(x)$

$p(x)$ ha come radici (almeno) 0, 3, 4, 7 ma il grado di $p(x)$ è 2.

Th. A è un dominio allora se $p(x)$ ha grado n, $p(x)$ ha al più n radici.

Lemma (Ruffini) (A dominio) $\quad p(a) = 0$ allora $(x-a) \mid p(x)$, cioè esiste $q(x) \in A[x]$ t.c. $p(x) = (x-a)\,q(x)$.

Pf. $(n=2)$ Supponiamo a_1, a_2, a_3 sono tre radici distinte di $p(x)$. Allora $p(a_1)=0$

$$p(x) = (x-a_1)\, q_1(x)$$

$$0 = p(a_2) = \underbrace{(a_2-a_1)}_{\neq 0} \underbrace{q_1(a_2)}_{=0}$$

A è un dominio

$\Rightarrow a_2 - a_1 = 0$ NO

oppure $q_1(a_2)=0$ ✓

$$q_1(x) = (x-a_2)\cdot a$$

$$0 = p(a_3) = (a_3-a_1)(a_3-a_2)\cdot a$$

$\neq 0$ $\neq 0$

$$p(x) = a(x-a_1)(x-a_2) \equiv 0$$

$$\deg(f\cdot g) = \deg(f) + \deg(g)$$ ← vero solo per A dominio

$$\deg(f\circ g) = \deg(f)\cdot \deg(g)$$

$$\deg(f+g) \leq \max\{\deg f, \deg g\}$$

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

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

(Se A è un dominio) Irriducibilità e fatt. unica

$p(x) \in A[x]$ è irriducibile (in $A[x]$) se $\nexists$ $q_1, q_2 \in A[x]$ $\partial q_1 \geq 1$, $\partial q_2 \geq 1$

$$p(x) = q_1(x)\, q_2(x)$$

Th. (fatt. unica) $p(x) = q_1(x)^{\alpha_1} q_2(x)^{\alpha_2} \cdots q_k(x)^{\alpha_k}$ $q_1, \dots, q_k$ sono irriducibili

e la fatt. è unica

Es. pol. irriducibili:

in $\mathbb{C}[x]$ $\{(x-\alpha),\ \alpha \in \mathbb{C}\}$ $\leftrightarrow$ Th. fond. algebra $p(x) \in \mathbb{C}[x]$ $\Rightarrow \exists\ \alpha$ $p(\alpha) = 0$

in $\mathbb{R}[x]$ $\{(x-\alpha),\ \alpha \in \mathbb{R}\} \cup \{(x-\alpha)(x-\bar{\alpha}),\ \alpha \in \mathbb{C}\setminus\mathbb{R}\}$

↓ pol di secondo grado con $\Delta < 0$

Dim. Fattorio fatt. su $\mathbb{C}$ e poi uso che $p(x)$ è a coeff. reali per cui $p(\alpha) = 0 \Rightarrow \overline{p(\alpha)} = 0 \Rightarrow p(\bar{\alpha}) = 0$

$$(x-\alpha)(x-\bar{\alpha}) = x^2 - (\alpha+\bar{\alpha})x + \alpha\bar{\alpha} = x^2 - 2\mathrm{Re}\,\alpha \cdot x + |\alpha|^2$$

$$p(x) = (x-r_1)^{d_1} \cdots (x-r_k)^{d_k} \cdot (x-\alpha_1)(x-\bar{\alpha}_1)^{e_1} (x-\alpha_2)(x-\bar{\alpha}_2) \cdots$$

in $\mathbb{Q}$, in $\mathbb{Z}$ $p(x)$ irriducibile può essere di qualsiasi grado.

Lemma di Gauss $p(x) \in \mathbb{Z}[x]$, riducibile in $\mathbb{Q}[x]$, allora è riducibile in $\mathbb{Z}[x]$.

$$p(x) = r_1(x)\, r_2(x) \qquad r_1, r_2 \in \mathbb{Q}[x]$$

$\exists\ q \in \mathbb{Q}$ t.c. $q r_1(x) \in \mathbb{Z}[x]$

$\frac{1}{q} r_2(x) \in \mathbb{Z}[x]$

$$p(x) = (q\, r_1(x)) \cdot \left(\frac{1}{q} \cdot r_2(x)\right).$$

Derivata di un polinomio

$D(p)(x)$ $\qquad D(p) \in A[x]$

(i) $D(p+q) = D(p) + D(q)$

(ii) $D(p \cdot q) = D(p) \cdot q + D(q) \cdot p$ (derivata formale)

(iii) $D(a \cdot p) = a\, D(p) \qquad a \in A$

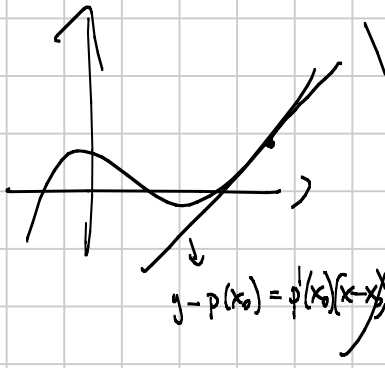
(iv) $D(x) = 1$

Corollario $\cdot\ D(x^n) = n \cdot x^{n-1}$

$D(a x^n) = a \cdot n\, x^{n-1}$ (per induzione usando (iii) e (ii))

$$D(a_n x^n + \cdots + a_1 x + a_0) = n a_n x^{n-1} + (n-1) \cdot a_{n-1} \cdot x^{n-2} + \cdots + a_1$$

Bonus $\qquad D(p)(x) = p'(x) = \lim_{h \to 0} \frac{p(x+h) - p(x)}{h}$



Conseguenze per polinomi

(I) Se $x-\alpha \mid p'(x)$ e $x-\alpha \mid p(x)$

$\Rightarrow (x-\alpha)^2 \mid p(x)$.

(II) se $(m \geq 1)$ $(x-\alpha)^m \,||\, p(x) \Rightarrow (x-\alpha)^{m-1} \,||\, p'(x)$

$p(x) = (x-\alpha)^m \cdot q(x) \leftarrow (x-\alpha) \nmid q(x)$, in pratica $q(\alpha) \neq 0$

$p'(x) = \left((x-\alpha)^m\right)' \cdot q(x) + (x-\alpha)^m \cdot q'(x)$

$= m \cdot (x-\alpha)^{m-1} \cdot q(x) + (x-\alpha)^m \cdot q'(x)$

$= (x-\alpha)^{m-1} \left[m \cdot q(x) + (x-\alpha) q'(x) \right]$

↓ valuto in α

$m \cdot q(\alpha) + 0$

$\text{rad}(n) = p_1 p_2 \cdots p_k$

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_n}$

$\text{rad}(p(x)) = p_1(x) \cdots p_k(x)$ sono i fattori irr. DISTINTI di p.

$p(x) = p_1(x)^{\alpha_1} \cdots p_k(x)^{\alpha_k}$

(I) + (II) $\Rightarrow \text{rad}(p(x)) = \dfrac{p(x)}{\text{mcd}(p(x), p'(x))}$

↓ in verità con irriducibile nel posto di $(x-\alpha)$.

Esempi:

1) Dimostrare che il numero di radici distinte di $p(x)$ e $p(x)+1$ è ALMENO $\deg p + 1$

1bis) Qual è il numero minimo di radici distinte di $p(x), p(x)+1, p(x)+2, \dots, p(x)+k$?

2) Trovare se esistono soluzioni di $p(x)^3 - q(x)^2 = 1$ p, q non costanti

2bis) Idem con $= 2x+1$

3) (RMM 18) Dire se esistono $p, q \in \mathbb{R}[x]$ non costanti tali che

$$p(x)^{10} + p(x)^9 = q(x)^{21} + q(x)^{20}$$

Cosa utile: per induzione trovare $D(p(x)^k)$

1. in $\mathbb{R}[x]$ x^n x^n+1

in $\mathbb{C}[x]$ radici distinte 0, $e^{\frac{ik\pi}{n}}$ k dispari $k < 2n$ $k = 1, 3, \dots, 2n-1$

ALmeno $\deg p + 1$ radici

(i) $p(x) = (x-\alpha_1)^{d_1} \cdots (x-\alpha_k)^{d_k}$ $\quad K + J \geq \deg p + 1$

$p(x)+1 = (x-\beta_1)^{e_1} \cdots (x-\beta_J)^{e_J}$

$$p'(x) = (x-\alpha_1)^{d_1-1} \cdots (x-\alpha_h)^{d_h-1} \cdot (x-\beta_1)^{e_1-1} \cdots (x-\beta_j)^{e_j-1} \cdot q(x)$$

$$\partial p - 1 = \sum (d_i - 1) + \sum (e_i - 1) + \partial q$$

$$\geq \left(\sum d_i\right) - h + \left(\sum e_i\right) - j$$

$$= 2\partial p - h - j$$

$$h + j \geq \partial p + 1 .$$

(ii) $$\operatorname{rad}\left(p(x)(p(x)+1)\right) = \frac{p(x)(p(x)+1)}{MCD\left(p(x)(p(x)+1),\ p'(x)(2p(x)+1)\right)}$$

$$= \frac{p(x)(p(x)+1)}{MCD\left(p(x)(p(x)+1),\ p'(x)\right)}$$

$$\partial \sqcup = 2\partial p - \partial\left(MCD\left(\quad, p'(x)\right)\right)$$

$$\geq 2\partial p - (\partial p - 1) = \partial p + 1$$

1bis) $p(x) = (\quad)^{d_1} \cdots (\quad)^{\cdots}$

$p(x)+1 = (\quad)^{e_1} \cdots (\quad)^{\cdots}$

$p(x)+k = (\quad)^{f_1} \cdots (\quad)^{\cdots}$

$$p'(x) = (\quad)^{d_1-1} \cdots (\quad)^{e_1-1} \cdots (\quad)^{f_1-1} \cdots \cdot q(x)$$

$$\partial p - 1 \geq -r_0 + \left[d_i - r_1 + \sum e_1 - r_2 + \sum f_i \cdots\right.$$

$$\geq -(r_0 + r_1 - - - + r_k) + (k+1)\,\partial p$$

$$r_0 + r_1 \cdot - - - r_k \geq \underline{k\,\partial p + 1}$$

$$x^n \qquad x^{n+1} \qquad x^{n+2} \quad \cdot - - \quad x^{n+k}$$

2) $p(x)^3 - q(x)^2 = 1$ $\quad p, q$ non costanti.

$\partial p = 2d$

$\partial q = 3d$

$$3\,p(x)^2\,p'(x) - 2q(x)\,q'(x) = 0$$

$$3\,p(x)^2\,p'(x) = 2q(x)\,q'(x)$$

r irriducibile $\quad r \mid p \Rightarrow r \mid q'$, con molteplicità doppia rispetto a p, (poiché $r \nmid q$ da eq.)

$\Rightarrow \quad p^2 \mid q' \qquad \partial(p^2) \leq \partial q'$

$4d \leq 3d - 1 \quad \Rightarrow \quad d \leq -1.$

radici distinte di p^3 sono al più $2d$

" " " q^2 " " $3d$

$$6d + 1 \leq 5d$$

$$d \geq -1$$

2bis) PreIMO 2018 /p

$$p(x)^3 - q(x)^2 = 2x + 1 \qquad \partial p = 2d \quad \partial q = 3d$$

$$3\,p(x)^2\,p'(x) - 2q'(x)\,q(x) = 2$$

$$3\,p(x)^3 p'(x) - 2q'(x)q(x)p(x) = 2p(x) \qquad (\text{Lavoro "mod } q(x)")$$

$$3(2x+1)\,p'(x) \equiv 2p(x)$$

$(p(x)^3 \equiv 2x+1$ dall'equazione$)$

$$2p(x) - 3(2x+1)p'(x) \equiv 0 \quad (q(x))$$

$$q(x) \mid 2p(x) - 3(2x+1)p'(x)$$

$$\Downarrow$$

$$= 2d$$

$$\partial q = 3d$$

$$2a_n x^n + \dots - 3(2x+1)\cdot(n\cdot a_n x^{n-1} + \dots)$$

$$x^n(2a_n - 6n a_n) = a_n\cdot(2-6n)x^n \neq 0$$

$\lightning$

3) RIPRI'18

$$(p(x)+1)\,p(x)^9 = p(x)^{10} + p(x)^9 = q(x)^{21} + q(x)^{20} = p(x)^{20}(p(x)+1)$$

p, q non costanti. $\in \mathbb{R}[x]$

$$p'(x)\,p(x)^8(10p(x)+9) = q'(x)\,q(x)^{19}(21q(x)+20)$$

$\partial q = 10n$

$\partial p = 21n$

$$\left(D(p(x)^k) = k\cdot p(x)^{k-1}\cdot p'(x)\right.$$

$$\left.D(y^k) = k\,y^{k-1}\cdot y' = k\,p(x)^{k-1}\cdot p'(x)\right)$$

$$p'(x)\,p(x)^9\left(10\,p(x)+y\right) = q'(x)\,q(x)^{19}\cdot p(x)\left(21\,q(x)+20\right)$$

$$p'(x)\,q^{20}(x)\left(q(x)+1\right)\left(10\,p(x)+y\right) = q'(x)\,\cancel{q(x)^{19}}\,p(x)\left(p(x)+1\right)\left(21\,q(x)+20\right)$$

$$p'(x)\,q(x)\left(q(x)+1\right)\left(10\,p(x)+y\right) = p(x)\left(p(x)+1\right)q'(x)\left(21\,q(x)+20\right)$$

se faccio il conto dei gradi: a sinistra $2\partial q + 2\partial p - 1$, in entrambi i membri.

$$p(x)\left(p(x)+1\right) \mid q(x)\left(q(x)+1\right)q'(x)$$

$$2\partial p \le 2\partial q + \partial p - 1$$

$$\partial p \le 2\partial q - 1 \quad ?$$

$$21n \le 2\cdot 10n - 1$$

$$20n - 1 \quad ?$$

$$n \le -1. \quad \lightning$$

Theorem (Mason-Stothers, Teorema ABC). $a, b, c \in A[x]$

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

$\leftarrow$ a, b, c coprimi

$$\partial\left(\mathrm{rad}(abc)\right) \ge \max\{\partial a, \partial b, \partial c\} + 1$$

APPLICAZIONI!

1) $a(x) = p(x) \qquad b(x) = 1 \qquad c(x) = p(x)+1$

$rad(abc) = rad(p(x)(p(x)+1)) = \#$ rad. dist. di $p(x)$ e $p(x)+1$

$\geq \max(\partial a, \partial b, \partial c) + 1 = \partial p + 1$

2) $a = p^3 \qquad b = -q^2 \qquad c = p^3 - q^2$

Supponga che $\partial c < \partial a$.

$\partial p = 2d$

$\partial q = 3d$

$\partial c < 6d$

$\partial(rad(abc)) \geq 6d + 1$

$\partial(rad(p^3(-q^2)\cdot(p^3-q^2))) \leq \partial(rad(p)) + \partial rad(q) + \partial rad(p^3-q^2)$

$\left(\begin{array}{l} rad(ab) \leq rad(a)\cdot rad(b) \\ rad(p^k) = rad\, p \end{array}\right)$

$\leq 2d + 3d + \partial rad(p^3 q^2)$

$\partial rad(p^3 - q^2) \geq d + 1 \left(= \frac{\partial p}{2} + 1\right) \geq 2$

$\partial(p^3 - q^2) \geq d + 1 = \left(\frac{\partial p}{2} + 1\right)$

provare a vedere se si riesce ad ottenere la costante $d+1$.

3) $p^{10} + p^9 = q^{21} + q^{20}$

$c \qquad a \qquad b$

$\partial q = 10d$

$\partial p = 21d$

$rad(abc) \geq \partial a + 1 = 210d + 1$

$rad(q^{21}\cdot q^{20}\cdot p^9\cdot(p+1)) \leq \partial q + 2\partial p = 10d + 42d.$

Achtung !! bisogna avere a,b,c coprimi.

Fermat per polinomi: $\nexists\ p,q,r \in \mathbb{R}[x]$ t.c. $p(x)^3 + q(x)^3 = r(x)^3$

Dim. (ABC per polinomi)

$W = ac' - ca'$ $\quad \partial a \le d$, $\partial c \le d$ $\Rightarrow \partial W \le 2d-1$ $\quad a+b=c$, $a'+b'=c'$

$r^k \| a \Rightarrow r^{k-1} \mid W$

$r^k \| c \Rightarrow r^{k-1} \mid W$

$r^k \| b \Rightarrow r^{k-1} \mid W$

$ac' - ca' =$

$= (c-b)c' - c(c'-b') =$

$= -bc' + b'c$

poiché a,b,c sono coprimi

$r^k \| abc \Rightarrow r^{k-1} \mid W$ $\qquad W = \prod r_i^{(k_i-1)} \cdot q$

$$rad(abc) = \prod r_i = \frac{\prod r_i^{k_i}}{\prod r_i^{k_i-1}} = \frac{abc}{W} \cdot q$$

$$\partial rad(abc) \ge \partial(abc) - \partial W$$

$$\ge 3\max\{\partial a, \partial b, \partial c\} - (\max\{\partial a, \partial b, \partial c\} - 1)$$

$$= \max\{\partial a, \partial b, \partial c\} + 1$$

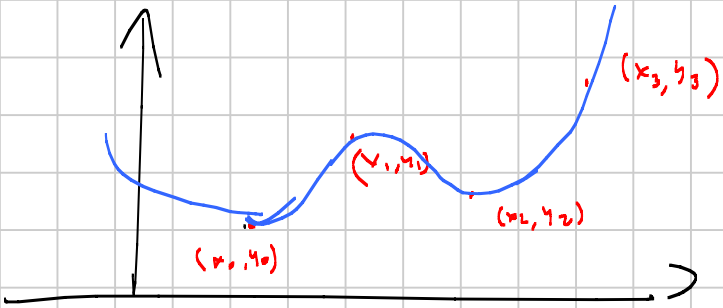
$a+b=c$ $\qquad \frac{a}{c} + \frac{b}{c} = 1$ $\qquad \frac{a'c - c'a}{c^2} + \frac{b'c - c'b}{c^2} = 0$.

o

Interpolazione:

Domanda: date coppie di punti $(x_0, y_0) \dots (x_n, y_n)$ con x_i distinti $(x_i, y_i \in \mathbb{R})$.

Esiste una funzione polinomiale p che "passa" per questi punti? Quanto "facile" risulta a farla?



Vandermonde

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$$

$$\begin{cases} p(x_0) = y_0 \\ \vdots \\ p(x_n) = y_n \end{cases} \qquad \begin{cases} a_d x_0^d + \dots + a_1 x_0 + a_0 = y_0 \\ \vdots \\ a_d x_n^d + \dots + a_1 x_n + a_0 = y_n \end{cases}$$

$$V \Rightarrow \begin{pmatrix} x_0^d & \dots & x_0 & 1 \\ x_1^d & x_1^{d-1} & \dots & x_1 \; 1 \\ & \ddots & & \\ x_n^d & x_n^{d-1} & \dots & x_n \; 1 \end{pmatrix} \begin{pmatrix} a_d \\ a_{d-1} \\ \vdots \\ a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} y_0 \\ \vdots \\ y_n \end{pmatrix}$$

Se $d+1 \geq n+1$ ci sono almeno d funzioni tutte

Se $d+1 < n+1$ sicuramente non posso risolvere per

QUALSIASI $y_0, \dots, y_n$

IL CASO INTERESSANTE È $d_{n+1} = n+1$

$$V \begin{pmatrix} a_n \\ | \\ a_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow a_n = \dots = a_0 = 0$$

$$\downarrow$$

$$p(x_0) = 0$$
$$p(x_1) = 0 \quad \Rightarrow \quad p \equiv 0$$
$$\vdots$$
$$p(x_n) = 0$$

II metodo (costruttivo interpolante (Lagrange))

$n = 3$ (x_0, y_0) (x_1, y_1) (x_2, y_2)

$$p_0(x) = \frac{(x - x_1)(x - x_2)}{(x_0 - x_1)(x_0 - x_2)} \qquad p_2(x) = \frac{(x - x_0)(x - x_1)}{(x_2 - x_0)(x_2 - x_1)}$$

$$p_1(x) = \frac{(x - x_0)(x - x_2)}{(x_1 - x_0)(x_1 - x_2)}$$

Lemma $p_i(x_j) = 0$ se $i \neq j$ $\quad p_i(x_i) = 1$

$$p(x) = y_0 p_0(x) + y_1 p_1(x) + y_2 p_2(x)$$

$$p(x_0) = y_0 \underbrace{p_0(x_0)}_{1} + \cancel{y_1 p_1(x_0)}^{0} + \cancel{y_2 p_2(x_0)}^{0} = y_0$$

$$p(x_1) = y_1$$
$$p(x_2) = y_2$$

$$c\frac{(x-a)(x-b)}{(c-a)(c-b)} + b\frac{(x-c)(x-a)}{(b-c)(b-a)} + a\frac{(x-b)(x-c)}{(a-c)(a-b)} = x$$

$$p(x) = 1\cdot P_c(x) + 1\cdot P_b(x) + 1\cdot P_a(x) \equiv 1$$

$\partial\, p(x) \le n$

$\partial\, \tilde{p}(x) \le n$

$p(x) - \tilde{p}(x) = 0$ 在 $x_0, \dots, x_n$

(x_0, y_0) $\quad p(x) = y_0$

(x_1, y_1) $\quad p(x) = y_0 + (x-x_0)\cdot\frac{(y_1-y_0)}{(x_1-x_0)}$

(x_2, y_2) $\quad p(x) = y_0 + (x-x_0)\frac{(y_1-y_0)}{(x_1-x_0)} + (x-x_0)(x-x_1)\cdot q$

$x_0, \longrightarrow x_n = 1, 2, \dots, n+1$

$\partial\, p \le n$

$p(-1)$	$p(0)$	$p(1)$	$p(2)$	$p(3)$	$\cdots$	$p(n)$	$p(n+1)$
1		$p(1)-p(0)$	$p(2)-p(1)$			$p(n)-p(n-1)$	
2			$p(2)-2p(1)+p(0)$	$\cdots$			
$\vdots$							
n	c	c	c	c	c	c	c

$c_n \cdot n!$

$q(k) = p(k+1) - p(k)$

Dato k diff. finite $\quad q(n) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} p(n+i)$

se $\quad k > \partial p \quad q \equiv 0$

$k = \partial p \quad q = c_{\partial p} \cdot (\partial p)!$