Senior 2017 - N1 Advanced Anér

Titolo nota

Anello: insieme A con $+$ $-$ $\cdot$, tipo $\mathbb{Z}$

$\forall x, y \in A$ avete $x+y$, $x-y$, $x \cdot y$

esiste 0, esiste 1

Campo: anello in cui posso sempre dividere per elementi $\neq 0$

<u>Esempi</u> $\mathbb{Z}$, $\mathbb{Z}\left[\frac{\sqrt{-7}+1}{2}\right]$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}[x]$ sono anelli

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{R}(x)$ sono campi

Un dominio è un anello in cui vale la seguente: se $x, y \neq 0$ anche $xy \neq 0$. Es: $\mathbb{Z}$, $\mathbb{R}[x]$ domini

---

Sia $\mathbb{K}$ un campo e $p(x) \in \mathbb{K}[x]$ monico

$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$. Supponiamo

$p(x)$ irriducibile, $\deg p = n \geq 2$

Se p non ha radici in $\mathbb{K}$, le inventiamo!

Inserisco α e impongo $p(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$

ottengo $\mathbb{K}[\alpha] = \left\{ \text{scritture del tipo } \sum_{i=0}^{k} \lambda_i \alpha^i \text{ con } \lambda_i \in \mathbb{K},\ k \in \mathbb{N} \right\}$ a meno di multipli di $p(\alpha)$

OSS Ogni elemento di $\mathbb{K}[\alpha]$ ha rappr. con $k \leq n-1$ (divisione euclidea)

OSS $\mathbb{K}[\alpha]$ è un anello

OSS $\mathbb{K}[\alpha]$ è anche un campo: sia $q(\alpha) \neq 0$ in $\mathbb{K}[\alpha]$

vuol dire che $q(x)$ non è un multiplo di $p(x)$

$p(x)$ irrid. $\rightsquigarrow$ $q(x), p(x)$ coprimi $\rightsquigarrow$ Bezout

$\exists$ trovo $a(x)\ b(x) \in \mathbb{K}[x]$: $a(x) \cdot p(x) + b(x)\, q(x) = 1$

OSS $\mathbb{K}[\alpha]$ è uno spazio vettoriale di dimensione n su $\mathbb{K}$, cioè

$\mathbb{K}$ sp. vett.
1. Posso sommare elementi di $\mathbb{K}[\alpha]$ tra loro
2. Posso moltiplicare $q(\alpha)^{\in \mathbb{K}[\alpha]}$ per uno scalare $\lambda \in \mathbb{K}$

dim n
3. $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ sono una base

$\mathbb{K}[\alpha]$ è un'estensione algebrica di grado n di $\mathbb{K}$

Prendiamo un dominio A (se servirà, $\mathrm{Frac}(A) = \mathbb{K}$ il campo delle frazioni)

$p(x) \in A[x]$ monico irriducibile (anche in $\mathbb{K}[x]$)

Aggiungo α come prima, ma $A[\alpha]$ sarà ora solo un anello, che è un dominio $A[\alpha] \subseteq \mathbb{K}[\alpha]$

$$
\begin{array}{ccc}
A & \subseteq & A[\alpha] \\
\cap & & \cap \\
\mathbb{K} & \subseteq & \mathbb{K}[\alpha]
\end{array}
$$

campo delle frazioni

campo delle frazioni

Def Dato $A \subseteq \mathbb{L}$ A anello $\mathbb{L}$ campo, $\beta \in \mathbb{L}$, β è intero su A se esiste un polinomio $p(x)$ monico a coefficienti in A ($p(x) \in A[x]$) t.c. $p(\beta)=0$

Esempio/giustificazione $A=\mathbb{Z}$, $\mathbb{L}=\mathbb{Q}$, allora gli interi su $\mathbb{Z}$ dentro $\mathbb{Q}$ sono proprio $\mathbb{Z}$!

$A=\mathbb{Z}$, $\mathbb{L}=\mathbb{C}$, adesso i è intero su $\mathbb{Z}$ perché è radice di x^2+1. $\sqrt{2}$ è intero su $\mathbb{Z}$ (x^2-2)

$\frac{\sqrt{-7}+1}{2}$ è intero su $\mathbb{Z}$ (x^2-x+2)

TEO Gli interi su $\mathbb{Z}$ contenuti in $\mathbb{C}$ sono un anello (e contengono tutto $\mathbb{Z}$).

DIM
- ogni $n \in \mathbb{Z}$ è radice di $x-n$;
- Se α è radice di $p(x)$, $-\alpha$ è radice di $\pm p(-x)$;
- Se α è radice di $p(x)$ e β radice di $q(x)$, $\alpha+\beta$ di chi è radice? E $\alpha\beta$?

Caso semplice (?) $\alpha=\sqrt{2}$ $\beta=i$ $\quad \pm\sqrt{2}\pm i$ è radice di chi?

$(x-\sqrt{2})^2 = i^2 \qquad x^2-2\sqrt{2}x+2=-1 \qquad x^2+3=2\sqrt{2}x$

$(x^2+3)^2 = 8x^2$ e ricomponendo ...

Caso generale $p(x)=(x-\alpha_1)\dots(x-\alpha_n)$ $\qquad \alpha=\alpha_1$

$q(x)=(x-\beta_1)\dots(x-\beta_m)$ $\qquad \beta=\beta_1$

Sembra una buona idea cercare un polin. che ha $\alpha_i+\beta_j$ come radici, per tutti gli i e j...

$$\tau(x) := \prod_{\substack{1\le i\le n\\ 1\le j\le m}} (x-\alpha_i-\beta_j)$$ ha $\alpha+\beta$ come radice. Ma è in $\mathbb{Z}[x]$?

Idea: Considero la "stessa espressione" nell'anello polinomiale $\mathbb{Z}[x, A_1 \dots A_n, B_1 \dots B_m]$

$R(x) = \prod (x-A_i-B_j)$ è simmetrico nei B_j

$\rightsquigarrow$ vive in $\mathbb{Z}[x, A_1 \dots A_n, s_1(B_j..) \dots s_m(B_j)]$

è simm. negli A_i $\rightsquigarrow$ vive in $\mathbb{Z}[x, s_1(A_i) \dots s_n(A_i), s_1(B_j) \dots s_m(B_j)]$

---

① Trovare le soluzioni razionali di
$$x^3+3y^3 = x^2+2y^2$$

② Dim che $x^3+y^3=9$ ha molte ∞ soluzioni razionali

③ $\begin{cases} x+y = z+u \\ 2xy = zu \end{cases}$ ha tante soluzioni intere con x e $y>0$ (e wlog $x>y$)

Trovare, al variare di queste, $\inf \frac{x}{y}$.

Polinomi ciclotomici

$x^n - 1$ si può fattorizzare come $\prod_{d \mid n} \Phi_d(x)$, dove $\Phi_d(x)$ è il polinomio monico, di grado $\varphi(d)$, le cui radici sono le radici d-esime primitive di 1 in $\mathbb{C}$

Domanda Come sono fatti i coefficienti? Vedremo che

1) La lista di coefficienti è simmetrica: infatti $x^{\varphi(n)} \cdot \Phi_n\left(\frac{1}{x}\right)$ ha le stesse radici di $\Phi_n(x)$ e (a parte il caso $n=1$) è anche monico

2) Il secondo coefficiente è davvero 0, 1 o -1.

$$\Phi_n(x) = x^{\varphi(n)} + a_{\varphi(n)-1} \, x^{\varphi(d)-1} + \ldots + 1 \quad \boxed{n \geq 2}$$

3) $n \in \mathbb{N}_0$ $\quad n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ chiamo radicale di n $\mathrm{rad}(n) = p_1 \cdot \ldots \cdot p_k$. Confrontare $\Phi_n(x)$ e $\Phi_{\mathrm{rad}(n)}(x)$. (Suggerimento: $\varphi(n) = \varphi(\mathrm{rad}(n)) \frac{n}{\mathrm{rad}(n)}$)

$\Phi_n(x)$ è irriducibile su $\mathbb{Z}$. Per assurdo $\Phi_n(x) = f(x) \cdot g(x)$, $f, g \in \mathbb{Z}[x]$, monici (Gauss)

supponiamo f irriducibile.

Ci sono due casi:

(1) Esiste un primo $q \nmid n$, ξ radice di f, con ξ^q radice di g

(2) Per ogni primo $q \nmid n$, ξ radice di f, anche ξ^q radice di f

(un attimo! Perché $\Phi_n(x)$ non ha radici doppie? Perché $x^n - 1$ non ha radici doppie (criterio della derivata)

Se vale (2) allora $f = \Phi_n$: (2) $\Rightarrow$ $\forall m$ coprimo con n, $\forall \xi$ radice di f, anche ξ^m è radice di f. Fine del caso (2)

Se vale (1) la faccenda è più complicata.
ξ^q è radice di g, considero il polinomio $g(x^q)$: questo ha ξ come radice, ma allora $f(x)$ è un divisore $g(x^q)$. $g(x^q) = f(x) \cdot h(x)$ in $\mathbb{Z}[x]$

$$f(x) \cdot h(x) = g(x^q) \equiv [g(x)]^q \pmod q$$

[Attenzione! $x^q - x$ non è il polinomio nullo in $\mathbb{Z}/q\mathbb{Z}[x]$, benché sostituendo a x ogni classe mod q venga 0

Riscrivo: $f(x) \cdot h(x) \equiv (g(x))^q \pmod q$

Prendo un fattore irriducibile di f mod q

$F(x) \equiv \ell(x) \cdot i(x)$ ed $\ell(x)$ è irrid. mod q.

$$\ell(x) \cdot i(x) \cdot h(x) \equiv [g(x)]^q \pmod q$$

$\ell(x)$ deve essere un fattore di $g(x) \pmod q$

$$g(x) \equiv \ell(x) \cdot m(x) \pmod q$$

$$\Phi_n(x) = F(x) \cdot g(x) \equiv [\ell(x)]^2 \cdot i(x) \cdot m(x) \pmod q$$

$$x^n - 1 = \left[\prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x)\right] \cdot [\ell(x)]^2 \cdot i(x) \cdot m(x) \pmod q$$

$$\frac{d}{dx}(x^n - 1) = n x^{n-1} \not\equiv 0 \pmod q$$

perché $q \nmid n$ per ipotesi

3) Claim $\Phi_n(x) = \Phi_{rad(n)}\left(x^{\frac{n}{rad(n)}}\right)$

Infatti sono entrambi monici, e hanno le stesse radici: basta, per ragioni di grado, controllare che ogni radice n-esima ξ primitiva di 1 annulla $\Phi_{rad\, n}\left(x^{\frac{n}{rad\, n}}\right)$

$\xi^{\frac{n}{rad\, n}}$ è una radice dell'unità di ordine $rad(n)$

$\to$ tesi

2) Def: la funzione μ di Möbius $: \mathbb{N}_0 \to \{0, -1, 1\}$ è definita così: se $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$

$$\mu(n) = \begin{cases} 0 & \text{se qualche } \alpha_i \geq 2; \\ \text{altrimenti} & \begin{cases} 1 & \text{se } k \text{ pari} \\ -1 & \text{se } k \text{ dispari} \end{cases} \end{cases}$$

Proprietà:

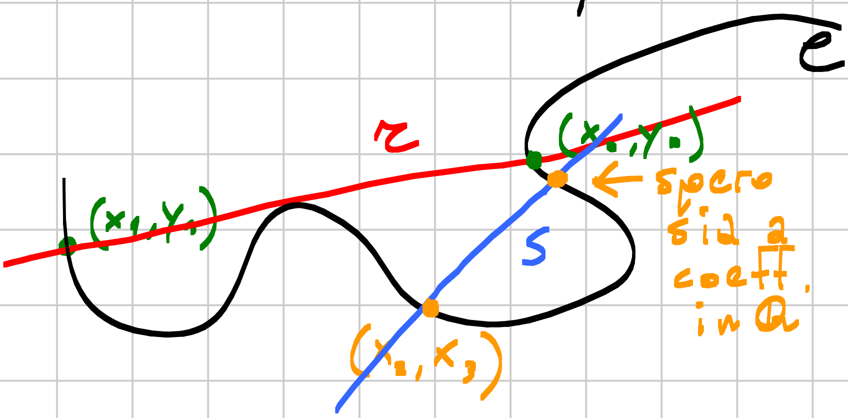
- $\mu(1) = 1$
- $\sum_{d \mid n} \mu(d) = 0$ se $n \geq 2$

Sorpresona: $\Phi_n(x) = x^{\varphi(n)} - \mu(n) \cdot x^{\varphi(n)-1} + \ldots$

Induzione: chiamo c_n la somma delle radici n-esime primitive di 1. Allora vale anche

- $c_1 = 1$
- $\sum_{d \mid n} c_d =$ somma tutte le radici n-esime di $1 = 0$ se $n \geq 2$

Idea per trovare punti razionali su curve: usare rette con equazioni a coeff. in $\mathbb{Q}$.



$(x_0,y_0),(x_1,y_1)$ a coeff. in $\mathbb{Q}$

r ha equaz. a coeff. in $\mathbb{Q}$

parto da (x_2,y_2), traccio una retta s (tutto in $\mathbb{Q}$)

OSS Se $\mathcal{C}$ è di secondo grado funziona!

Con questo metodo trovo tutti i punti razionali di una conica: ne trovo uno P (il primo, il punto base), e poi per ogni retta s a equazione in $\mathbb{Q}$ passante per P, ne trovo un altro, e così li ottengo tutti;

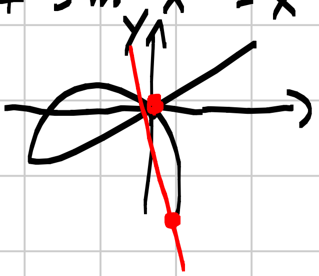
<u>OSS</u> Per una cubica, se ho 2 sol. razionali, la retta che le congiunge interseca una terza volta la cubica in un (nuovo?) punto razionale

① $\mathcal{C}: x^3+3y^3-x^2-2y^2=0$ $\qquad$ $(0,0)$ è radice.

Considero $r: y=mx$ $\quad$ ($m\in\mathbb{Q}$ è la generica retta razionale per l'origine

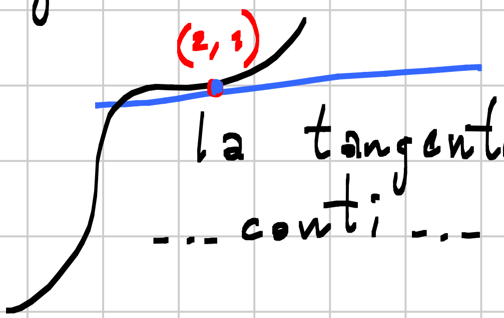
poi a parte considero $r: x=0$)

$$x^3+3m^3x^3-x^2-2m^2x^2=0=x^2\left([1+3m^3]x-2m^2-1\right)$$



② Trovare $\overset{\text{tanti}}{\text{pti}}$ razionali su x^3+y^3-9.

Usare $(2,1),(1,2)$ e la retta $x+y=3$ che li congiunge, non funziona!

Provo con 

la tangente a $\mathcal{C}$ per $(2,1)$

... conti ... nuovo punto razionale!

x CASA: trovare un argomento per dire che ci sono ∞ pti razionali.

<u>OSS</u> il punto all'∞ in direzione $x=-y$ sembra

essere singolare. Provo a usare le rette

$$y = -x + k \; .$$

$$y^3 + x^3 - 9 = k^3 - 3k^2 x + 3k x^2 - 9 = 0$$ non è di primo grado in X

$$\Delta = 9k^4 - 12k^4 + 108k = -3k^4 + 108k$$

$$\begin{cases} x+y = u+z \\ 2xy = uz \end{cases} \qquad t^2 - (u+z)t + (uz) = t^2 - (x+y)t + 2xy$$

$$\Delta = (x+y^2) - 8xy = x^2 - 6xy + y^2 = y^2 \cdot \left(\left[\frac{x}{y}\right]^2 - 6\left[\frac{x}{y}\right] + 1 \right)$$

$$t := \frac{x}{y} \qquad s := \sqrt{\Delta}$$

ci ritroviamo a cercare punti razionali per

$t^2 - 6t + 1 = s^2$. Vogliamo trovare punti di questa iperbole con t piccolo

- trovo un punto razionale P_0 sull'iperbole
- trovo il punto di min. reale M per t (il più piccolo $t > 1$ per cui $t^2 - 6t + 1 \geq 0$)
- tracciamo una retta razionale per P_0 e passante vicino a M