Se p è un pol. irriduc.

$\Rightarrow$ $\mathbb{K}[X]/(p)$ un campo.

contiene $\mathbb{K}$ come sottocampo

$\mathbb{R}[X]/(X^2+1) =: \mathbb{C}$.

1) Algor. di divisione $\Rightarrow$ ogni cl. d'equiv. ha uno e un solo rappr di grado $<$ deg p.

2) Se considero $\mathbb{K}[X]/(p)$ come $\mathbb{K}$-sp. vettoriale

$$\dim_{\mathbb{K}} \mathbb{K}[X]/(p) = \deg p. \text{ perché}$$

se $d = \deg p$ $\{[1], [X], \dots [X^{d-1}]\}$ è una base su $\mathbb{K}$.

<u>OSS.</u> la molt. per $[X]$.

è un endomorfismo (invertibile perché $[X] \neq 0$ e $\mathbb{K}[X]/_{(p)}$ è un campo) di questo sp. vett.

Qual'è la sua matr. rispetto alla base $[1], \ldots$?

ABUSO: $[1] = 1 \quad [X] = X \ldots$

$$\begin{pmatrix} 0 & & & -a_d \\ 1 & & & \vdots \\ 0 & 1 & & \\ \vdots & & \ddots & \\ & & 1 & -a_1 \end{pmatrix} \qquad [X][X^{d-1}] = X^d$$

$$p(X) = X^d + a_1 X^{d-1} + \ldots + a_d$$

$$[X^d] = -a_1[X^{d-1}] - \ldots - a_d[1]$$

__Es.__ $p(x) = x^4 + 1$

$\mathbb{Q}[x] / (x^4+1)$ base $1, x, x^2, x^3$

$$x \longrightarrow \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

$p(x) = x^2 + 1$ nella base $1, x$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

__OSS.__ in $\mathbb{K}[x] / (p(x))$

$[x]$ è una radice di p

Es.

1) X^2+1 in $\mathbb{R}[X]/(X^2+1)$

$[X]$ anche $-[X]$ radice

2) X^3-3 $\mathbb{Q}[X]/(X^3-3)$

$[X]$ è una radice ma non ci sono altre radici dell' equazione X^3-3.

$X^3-3 \quad | \; X-[X]$

$\rightsquigarrow$ pol. di grado 2 che non ha radici in $\mathbb{Q}[x]/_{x^3-3}$.

in ulteriore estensione (di grado 2) si trova un campo, che ha dimens. $= 6$ come sp. vett. su $\mathbb{Q}$ su cui x^3-3 ha 3 radici.

$[X] = \xi$. $\mathbb{Q}[X]/(X^3-3) = K'$

$\xi \in K'$ risolve $\xi^3 = 3$

$X^3 - 3$ è divisibile per

$X - \xi$ in K'.

$$X^3 - 3 = (X-\xi)\underbrace{(X^2+\xi X+\xi^2)}_{\text{irriduc. in } K'}$$

$\rightsquigarrow$ $K'[X]/(X^2+\xi X+\xi^2) = K''$

é un nuovo campo

$\mathbb{Q} \subseteq K' \subseteq K''$.

K' ha dim 3 come sp. vett. su $\mathbb{Q}$,

K'' dim 2 come sp. su K'

e dim 6 come sp. su $\mathbb{Q}$.

in K'' l'eq. x^3-3 ha

3 radici.

<u>OSS</u>. In questo modo si possono costruire tutti i campi finiti

<u>Es.</u> $\mathbb{F}_2$

x^2+x+1 è irr. in $\mathbb{F}_2$.

$\mathbb{F}_2[x]/(x^2+x+1)$ è un campo

$\supseteq \mathbb{F}_2$ con 4 elementi.

<u>Es.</u> $\mathbb{F}_3$ x^2+1 è irrid.

$\mathbb{F}_3[x]/(x^2+1)$ campo con 9 elementi.

in $\mathbb{F}_5$ x^2+1 ha radice 4.

<u>Es</u>, per ogni p esiste un pol. irriducibile di grado 2

$\Rightarrow \forall p$ esiste un campo con p^2 elementi.

Si può dimostrare (non facile) $\forall n, p$ esiste un pol. di grado n irriduc. su $\mathbb{F}_p$

$\rightsquigarrow$ esiste un campo con p^n elementi.

Cosa succede se p non è irriducibile?

(analogo n non primo che anello è $\mathbb{Z}/(n)$?)

<u>Def</u>. A_1, A_2 anelli commutativi con unità.

$A_1 \times A_2$ come ins. il prod. cartesiano.

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$
$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$$

Es. mostr. che è un anello commutativo con unità $(1,1)$ //

osservare che $e_1 = (1,0)$ e $(0,1) = e_2$ sono divisori di 0.

e che $e_1^2 = e_1 \quad e_2^2 = e_2$

$$e_1 \cdot e_2 = 0.$$

TEOR.

Se $p = p_1 \cdot p_2 \quad p_1, p_2$ primi tra loro $\Rightarrow$

$$\mathbb{K}[X]/(p_1 p_2) = \mathbb{K}[X]/(p_1) \times \mathbb{K}[X]/(p_2)$$

Analogo per $\mathbb{Z}$

es. $\mathbb{Z}/(55) = \mathbb{Z}/(5) \times \mathbb{Z}/(11)$

$$\mathbb{Z}/(12) = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

Dim. del CRT

$$\mathbb{K}[x]/(p_1 \cdot p_2) \longrightarrow \mathbb{K}[x]/(p_1) \times \mathbb{K}[x]/(p_2)$$

$$[q]_{p_1 p_2} \longmapsto \left([q]_{p_1}, [q]_{p_2}\right)$$

$q - q'$ div per $p_1 p_2 \Rightarrow$ è div per p_1

- - - p_2

verifica immediata che è un om. di anelli.

INIETTIVO

$[q]_{p_1 p_2} \longrightarrow 0$ vuol dire

$[q]_{p_1} = 0$ $[q]_{p_2} = 0$ cioè

q è div. per p_1 e per p_2.

Se un pol. è divisibile per due pol. primi tra loro $\Rightarrow$ è divis. per il prodotto.

SURIETTIVO: $\deg(p_1 p_2) = \deg p_1 + \deg p_2$

$\leftarrow \dim_{\mathbb{K}} \mathbb{K}[x]/(p_1 p_2)$

0. $\deg(p_1 p_2) = \deg p_1 + \deg p_2$

$\dim_{\mathbb{K}} \mathbb{K}[x]/(p_1 p_2)$ $\quad \dim \mathbb{K}[x]/p_2$

$= \dim \mathbb{K}[x]/(p_1)$

$$\dim_{\mathbb{K}} \left(\mathbb{K}[x]/(p_1) \times \mathbb{K}[x]/(p_2) \right) =$$

$$\dim_{\mathbb{K}} \mathbb{K}[x]/(p_1 p_2).$$

$\Rightarrow$ è una appl. lin. iniettiva

Tra sp. stessa dim $\Rightarrow$ SUR.

$\mathbb{Z}/_{n_1 n_2}$ ha $n_1 n_2$ el.

$\mathbb{Z}/_{n_1} \times \mathbb{Z}/_{n_2}$ .. ..

$\square$

Per induzione

<u>Corollario</u> $p_1, \ldots, p_k \in \mathbb{K}[x]$

a due a due primitive loro.

$$\Rightarrow \mathbb{K}[x]/_{(p_1 \cdots p_k)} = \mathbb{K}[x]/_{p_1} \times \ldots \times \mathbb{K}[x]/_{p_k}$$

<u>Dim.</u>

Si appl. il Teor. prec. a

p_1 e $p_2 \cdot \ldots \cdot p_k$

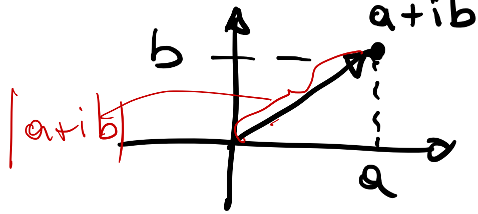
dopo k passi...

Alcune altre osserv. e notazioni su $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$

gli el. si scrivono $a+ib = z$

$a, b \in \mathbb{R}$ $\quad i = [x]$ soddisfa

$i^2 = -1$.



a si dice la parte reale di z

b - - - immaginaria di z

Coniugato di un numero compl.

$z = a+ib \qquad \bar{z} = a - ib$.

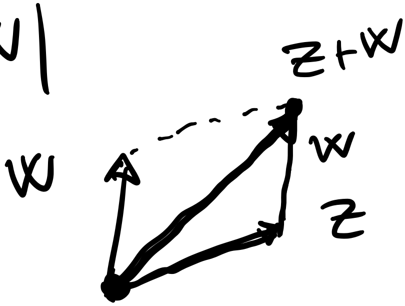
$$|z| = \sqrt{z\bar{z}} = \sqrt{a^2+b^2}$$

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

Proprietà di $| \ |$

$$|z+w| \le |z| + |w|$$

(dis. triangolare)



$$|zw| = |z||w|$$

si verifica

$$|zw|^2 = |z|^2 |w|^2$$

$z = a + ib$

$w = c + id$

$$zw = (ac - bd) + i(ad + bc)$$

FATELO!

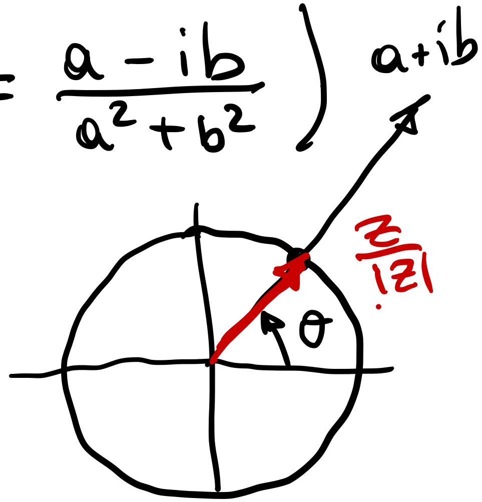
$$(ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2).$$

Rappresentazione polare

$$z = a + ib = \underbrace{\sqrt{a^2+b^2}}_{|z|} \underbrace{\left(\frac{a}{\sqrt{a^2+b^2}} + i \frac{b}{\sqrt{\dots}} \right)}_{\text{numero compl. di modulo 1}}$$

(<u>OSS.</u> $z\bar{z} = |z|^2$, poiché $|z|^2 \neq 0$ se $z \neq 0$, $z \cdot \dfrac{\bar{z}}{|z|^2} = 1$

cioè $z^{-1} = \dfrac{\bar{z}}{|z|^2} = \dfrac{a - ib}{a^2+b^2}$)



se $z \neq 0$ è def. θ (a meno di multipli di 2π)

t.c. $\dfrac{a}{\sqrt{a^2+b^2}} = \cos\theta$

$$\frac{b}{\sqrt{a^2+b^2}} = \sin\theta$$

ogni numero compl si scrive

$$\underbrace{\rho}_{\text{modulo}}(\cos\underbrace{\theta}_{\text{arg}} + i\sin\theta) \quad \rho \in \mathbb{R}_{\geq 0}$$

$\theta \in \mathbb{R}$ a meno di mult. di 2π

θ non è def. se $\rho = 0$

In termini di questa rappr.

$$\big(\rho_1(\cos\theta_1 + i\sin\theta_1)\big)\big(\rho_2(\cos\theta_2 + i\sin\theta_2)\big)$$

$$= \rho_1\rho_2\Big[\underbrace{(\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2)}_{\cos(\theta_1+\theta_2)} + i\underbrace{(\cos\theta_1\sin\theta_2 + \cos\theta_2\sin\theta_1)}_{\sin(\theta_1+\theta_2)}\Big]$$

nel prod. di numeri complessi si fa il prodotto dei moduli e si sommano gli argomenti.

RADICI DELL'UNITÀ.

$x^n = 1$. ha n radici.

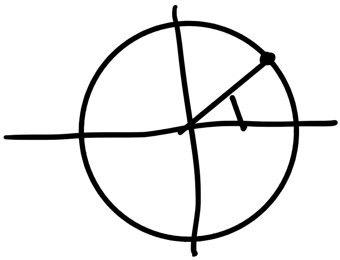
$\Downarrow$ perché $|x^n| = \underbrace{|x|}_{\in \mathbb{R}_{\geq 0}}{}^n = 1$

$|x| = 1$

$$(\cos\theta + i\sin\theta)^n = 1$$

$$\|$$

$$\cos(n\theta) + i\sin(n\theta)$$



es $\theta = \frac{2\pi}{n}$

Se $\mu = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)$

$1, \mu, \mu^2, \dots \mu^{n-1}$ sono le n radici

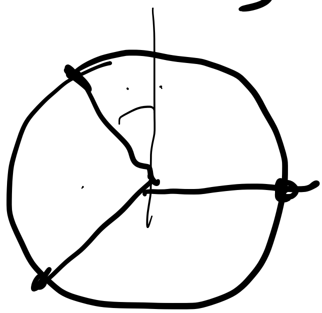
stanno sui vertici di un n-gono regolare. $\mu^k = \left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right)$

<u>Es.</u> $n=3$ $\qquad \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$

$-\frac{1}{2} + i\frac{\sqrt{3}}{2}$

1

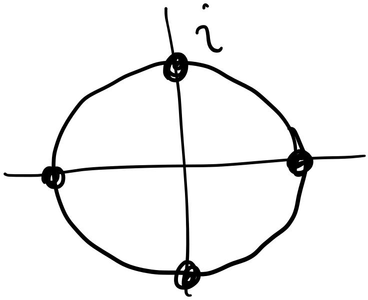
$-\frac{1}{2} - i\frac{\sqrt{3}}{2}$



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

$n = 4$

$1, i, -1, -i$



TEOR. (FOND. DELL'ALGEBRA)

$\mathbb{C}$ è un campo alg. chiuso.
(è la chiusura alg. di $\mathbb{R}$)

Se $p \in \mathbb{C}[X]$ $\deg p > 0$

$\Rightarrow$ p ha una radice in $\mathbb{C}$.

Eq. ogni polinomio p si scompone nel prodotto di polinomi di primo grado

$$p(x) = \prod_{i=1}^{k} (x - \alpha_i)^{m_i}$$

$\alpha_1 \dots \alpha_k$ radici distinte

$m_1 \dots m_k$ le loro molteplicità

$$\sum_{i=1}^{k} m_i = \deg p .$$