ALGEBRA 1 - 14 DIC 2018

Note Title 12/14/2018

Riprendiamo gli "shift" di estensioni

$$\begin{tikzcd}[column sep=small]
 & EF \arrow[dl, dash] \arrow[dr, dash, "\sigma \in G"] & \\
E & & F \\
 & E \cap F \arrow[ul, dash, "G'"'] \arrow[ur, dash] & \\
 & K \arrow[uul, dash] \arrow[uur, dash] \arrow[u, dash] &
\end{tikzcd}$$

$G' \cong G$

E/K normale

$\Rightarrow EF/F$ normale

$G = Gal(EF/F)$

$\sigma \in G \qquad \sigma \mapsto \sigma|_E \in Gal(E/K)$

$$Gal(EF/F) \xrightarrow{rest} Gal(E/K)$$

è un omomorfismo iniettivo.

(Se $\sigma|_E = id$, dal momento che $\sigma \in Gal(EF/F)$

anche $\sigma|_F = id \Rightarrow \sigma = id$)

$Im(res)$ è $Gal(E/L)$

dove L è l'insieme dei punti fissi.

$L = E \cap F$

$$\begin{tikzcd}[column sep=small]
 & EF \arrow[dl, dash, "H"'] \arrow[dr, dash, "K"] \arrow[dd, dash, "G"] & \\
E & & F \\
 & K \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

E/K normale

F/K normale

$H = Gal(EF/E)$

$K = Gal(EF/F)$

$$G = Gal(EF/K) \longrightarrow Gal(F/K) \times Gal(E/K)$$

$$\sigma \mapsto (\sigma|_E, \sigma|_F)$$

σ omomorfismo iniettivo.

$\mathrm{Im}\,\sigma = \mathrm{Gal}(EF/E\cap F)$.

$$\begin{tikzcd}[column sep=small]
 & EF \arrow[dl, dash, "H"'] \arrow[dr, dash, "K"] & \\
E \arrow[dr, dash, "K'"'] & & F \arrow[dl, dash, "H'"] \\
 & E\cap F \arrow[d, dash] & \\
 & K &
\end{tikzcd}$$

$H \cong H'$

$K \cong K'$

$H \cap K = \{id\}$

$$\mathrm{Gal}(EF/F) \cong H \times K \cong H' \times K'$$

CAMPI CICLOTOMICI

$\mathbb{Q}(\zeta_n)$ $\quad \zeta_n$ radice n-esima primitiva di 1.

<u>Prop</u> $\quad [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$

(Caso particolare: $n = p$ primo,
$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \phi(p) = p-1$).

<u>Dim.</u> Osserviamo che $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ è un'estensione normale. Infatti, il pol. min. $f(x)$ di ζ_n divide $X^n - 1$ e quindi tutte le sue radici sono potenze di $\zeta_n \to \in \mathbb{Q}(\zeta_n)$.

Vorrei vedere che $\deg f(x) = \phi(n)$.

Un automorfismo $\varphi : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$

deve mandare un elemento di ordine moltiplicativo n in un elemento di ordine n

Quindi le possibilità sono ζ^k con $(k,n)=1$ $(\zeta=\zeta_n)$ quindi al più $\phi(n)$. $(\deg f(x) \leq \phi(n))$.

Per vedere l'uguale, faccio vedere che $\forall k$ con $(k,n)=1$ ζ^k è radice di $f(x)$.

Fattorizzo k

$$k = p_1 p_2 \cdots p_s \quad \text{con } p_i \text{ eventualmente ripetuti.}$$

$$(p_i, n) = 1 \quad \forall i.$$

$$\zeta \to \zeta^{p_1} \to (\zeta^{p_1})^{p_2} = \zeta^{p_1 p_2} \to \cdots \to \zeta^{p_1 \cdots p_s} = \zeta^k$$

Mi basta far vedere che, se $(p,n)=1$ e ζ è radice di $f(x)$, allora anche ζ^p è radice di $f(x)$.

Scriviamo $\quad X^n - 1 = f(x)\, g(x)$

Supponiamo, per assurdo, che ζ^p non sia radice di $f(x)$ $\to$ radice di $g(x)$ $\quad g(\zeta^p)=0$.

Questo dice che ζ è radice del polinomio

$$g(X^p)$$

$$\Rightarrow \quad g(X^p) = f(x)\, h(x)$$

$$\Rightarrow \quad (g(x))^p \equiv g(X^p) \equiv f(x)\, g(x) \pmod p$$

Ne segue che ogni radice modulo p di $f(x)$ è radice modulo p di $g(x)$

$X^n - 1 = f(x) g(x)$ $\qquad X^n - 1 \equiv f(x) g(x) \pmod p$

Ma $X^n - 1 \bmod p$ non ha radici multiple: la derivata è nX^{n-1} $(p \nmid n)$, assurdo

Quindi la tesi è dimostrata

$$G = Gal\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right).$$

$$\sigma \in G \implies \sigma(\zeta_n) = \zeta_n^k \qquad (k, n) = 1$$

$$\sigma = \sigma_k$$

$$\sigma_k \xrightarrow{\lambda} \bar{k} \in (\mathbb{Z}/n\mathbb{Z})^*$$

λ è un omomorfismo, $\sigma_k \circ \sigma_h(\zeta_n) = \sigma_k(\zeta_n^h) = \zeta_n^{kh}$

λ è iniettivo. $\sigma_k = id \iff \bar{k} = \bar{1}$.

λ è surgettivo (G e $(\mathbb{Z}/n\mathbb{Z})^*$ hanno lo stesso ordine)

Conclusione: $G \cong (\mathbb{Z}/n\mathbb{Z})^*$.

<u>Oss.</u> Se $(m, n) = 1$

1. $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$
2. $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

<u>Dim.</u> 1. $\subseteq$ ovvio. $\supseteq$ $\zeta_m \cdot \zeta_n$ è una radice primitiva mn-esima

2.

$$\begin{tikzcd}[column sep=small]
& \mathbb{Q}(\zeta_{mn}) \arrow[dl, dash, "H\quad \phi(n)"'] \arrow[dr, dash, "\phi(m)\quad K"] \arrow[dd, dash, "\phi(mn)"] & \\
\mathbb{Q}(\zeta_m) \arrow[dr, dash, "\phi(m)"'] & & \mathbb{Q}(\zeta_n) \arrow[dl, dash, "\phi(n)"] \\
& \mathbb{Q} &
\end{tikzcd}$$

$H \cap K = Id$

$HK = G$

(G per questioni di ordine)

$(L = \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n))$ $L = \mathbb{Q}$.

ζ_{15} pol min.

$$\frac{(x^{15}-1)(x-1)}{(x^5-1)(x^3-1)}$$

Gruppo di Galois di un binomio

$$f(x) = x^n - a \in \mathbb{Q}[x]$$

Supponiamo $f(x)$ irriducibile.

F = campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

$$F = \mathbb{Q}(\alpha, \zeta_n)$$

α è una radice di $f(x)$.

$|K| = \phi(n)$ $\qquad$ $|H| = n$

$$\begin{tikzcd}[column sep=small]
& F \arrow[dl, dash, "K"'] \arrow[dr, dash, "H"] \arrow[dd, dash, "G"] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash, "n"'] & & \mathbb{Q}(\zeta_n) \arrow[dl, dash, "\phi(n)"] \\
& \mathbb{Q} &
\end{tikzcd}$$

IPOTESI: $\quad (n, \phi(n)) = 1$

$H \triangleleft G$ $\qquad$ (corr di Galois)

$H \leftrightarrow \mathbb{Q}(\zeta_n)$

$K < G$

$H \cap K = \{id\}$ $\qquad HK = G$ (cardinalità)

$\Rightarrow G \cong H \rtimes_\phi K$

$K \cong (\mathbb{Z}/n\mathbb{Z})^*$ $\qquad K = \{\tau_k \mid (k,n)=1\}$

$\tau_k(\zeta_n) = \zeta_n^k$

$\sigma \in H \Rightarrow \sigma(\alpha) = \zeta_n^i \alpha \quad 0 \leq i < n.$

$\sigma_1(\alpha) = \zeta_n^1 \alpha = \zeta_n \alpha$

$\sigma_1^2(\alpha) = \sigma_1(\zeta_n \alpha) = \sigma_1(\zeta_n)\sigma_1(\alpha)$

$= \zeta_n \zeta_n \alpha = \zeta_n^2 \alpha$

$\sigma_1^k(\alpha) = \zeta_n^k \alpha$

$\rightarrow \operatorname{ord} \sigma_1 = n.$

$H = \langle \sigma_1 \rangle \cong \mathbb{Z}/n\mathbb{Z}.$

Per capire la struttura di G_n devo vedere quanto vale

$$\tau_k \sigma_1 \tau_k^{-1}$$

Ovviamente $\tau_k \sigma_1 \tau_k^{-1}(\zeta_n) = \zeta_n$

$\langle \sigma_1 \rangle \triangleleft \operatorname{Gal}(\quad).$

$\tau_k \in K \qquad \tau_k(\zeta_n) = \zeta_n^k \quad \tau_k(\alpha) = \alpha$

$\tau_k \sigma_1 \tau_k^{-1}(\alpha) = \tau_k \sigma_1(\alpha)$

$= \tau_k(\zeta_n \alpha) =$

$= \tau_k(\zeta_n)\tau_k(\alpha) = \zeta_n^k \cdot \alpha$

Conclusione: $\tau_k \sigma_1 \tau_k^{-1} = \sigma_1^k$.

$$G = \mathbb{Z}/n\mathbb{Z} \rtimes_\phi (\mathbb{Z}/n\mathbb{Z})^*$$

$$(\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$
$$k \longmapsto k$$

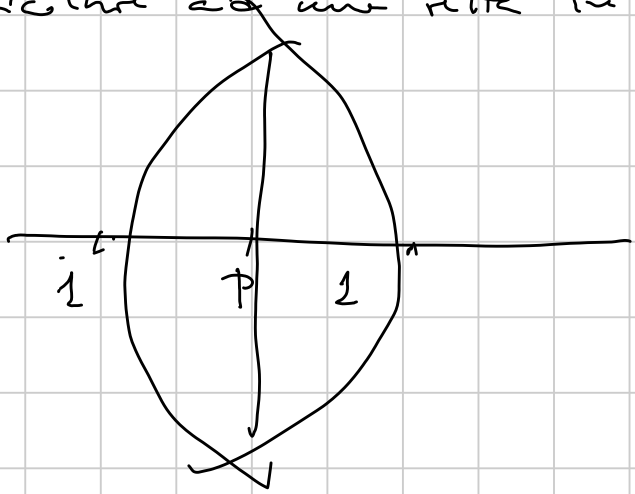
COSTRUZIONI CON RIGA E COMPASSO.

<u>Regole</u>. Si parte con 2 punti 0, 1

$$0 \cdot \quad \cdot 1$$

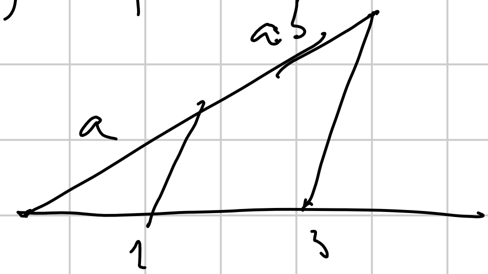
e poi si costruiscono
- rette per due punti già presenti
- circonferenze di centro un punto già presente e raggio la distanza tra due punti già presenti.

Si possono costruire:
- la perpendicolare ad una retta in un punto dato.



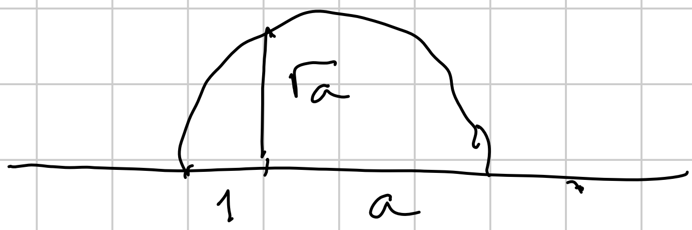
- punto medio

- parallela ad una retta per un punto dato.
- Date le lunghezze a, b
  si può fare $a \pm b$ ab a/b.

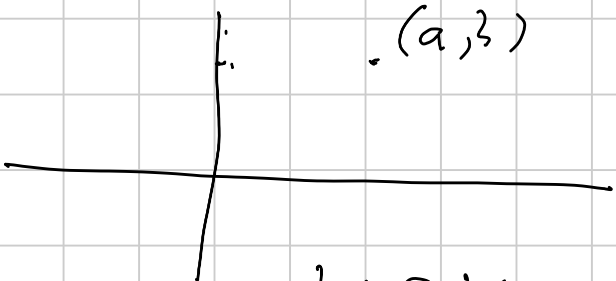


Talete

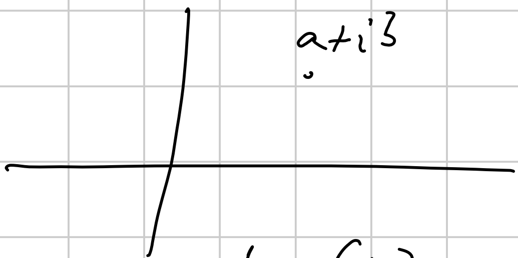
- Data la lunghezza a, si può costruire $\sqrt{a}$



I punti costruibili sull'asse delle x sono un campo, chiuso per radici quadrate.



$K_x \oplus K$



$K(i)$

Punti "nuovi" ad ogni passo della costruzione
intersezione di:
due rette
una retta e una circonferenza
due circonferenze

$$\begin{cases} ax+by=c \\ a'x+b'y=c' \end{cases} \qquad \begin{cases} ax+by=c \\ x^2+y^2+\alpha x+\beta y+\gamma=0 \end{cases} \qquad \begin{cases} x^2+y^2+\alpha x+\beta y+\gamma=0 \\ x^2+y^2+\alpha' x+\beta' y+\gamma'=0 \end{cases}$$

Tutti sistemi di grado ≤ 2

Se al passo n-esimo ho costruito i punti
$P_1 = (a_1, b_1)$, ... , $P_s = (a_s, b_s)$

e considero $K_{n+1} = \mathbb{K}(a_1, b_1, \dots, a_s, b_s)$

allora un nuovo punto $\in K_{n+1}$
con $[K_{n+1} : K] \leq 2$

CONCLUSIONE : Un punto $P = (a+ib) \in \mathbb{C}$ è costruibile $\iff$ $a+ib \in F$ dove F si può ottenere da $\mathbb{Q}$ con una catena

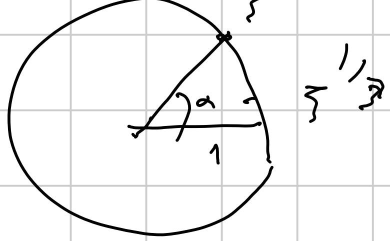
$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \dots \subseteq F_{s-1} = F_s = F$$
$$[F_i : F_{i-1}] = 2.$$

Cor. α è costruibile $\Longrightarrow$ α algebrico su $\mathbb{Q}$ di grado potenza di 2.

Conseguente classiche:

- π non è costruibile (non è algebrico)

- non è possibile trisecare un angolo generico.



$X^3 - \xi = 0$
se è irriducibile non si può.

- simultaneamente, non si può fare la duplicazione del cubo. cubo di vol. 1 → cubo di vol. 2

$$X^3 - 2 = 0.$$

- Pol. regolari $\overbrace{}^{\text{con } n \text{ lati}}$ ~ costruzione di radici n-esime di 1

Condizione necessaria : $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = 2^t$

$$\| \\ \phi(n)$$

$$n = 2^a p_1^{a_1} \cdots p_s^{a_s}$$

$$\phi(n) = 2^{a-1} \cdot (p-1)\cancel{p_1^{a_1-1}} \cdots (p_s-1)\cancel{p_s^{a_s-1}}$$

(1 se $a=0$)

$$a_1 = a_2 = \cdots = a_s = 1$$

$$p_i - 1 = 2^{t_i}$$

$$p_i = 2^{t_i} + 1$$

$2^m + 1$ è primo

$\Rightarrow m = 2^n$

(se $m = dk$ per k dispari

$2^{dk} + 1 = 2^{dk} + 1^k$ è divisibile per $2^d + 1$.

Numeri di Fermat

$$F_n = 2^{2^n} + 1$$

$F_0 = 3$ $F_1 = 5$ $F_2 = 17$ $F_3 = 257$ $F_4 = 65537$

primi

$F_5 = 4294967297$

NON E' PRIMO.

$$2^{2^5}+1 \equiv 0 \pmod p$$

$$2^{2^6}-1 = (2^{2^5}+1)(2^{2^5}-1) \equiv 0 \pmod p$$

$$\mathrm{ord}_p\, 2 = 2^6.$$

$$\Rightarrow 2^6 \mid p-1 \qquad p \equiv 1 \pmod{64}$$

$$641 \mid F_5.$$

La Condizione è sufficiente? SI

Le estensioni con radici n-esime dell'unità sono abeliane

Se $|G| = 2^n$ allora esiste una catena di sottogruppi

$$\{1\} = G_0 < G_1 < G_2 < \dots < G_n = 2^n$$
$$|G_i| = 2^i$$
$$|G_{i+1}/G_i| = 2.$$

e questa corrisponde ad una catena di sottoestensioni K_i con $[K_i : K_{i-1}] = 2$.