CRITERIO:

Siano $z_1, z_2, \dots, z_m \in \mathbb{C}$ con $z_1 = 0$ $z_2 = 1$

Definiamo $F \overset{def}{=} \mathbb{Q}(z_1, \dots, z_m, \overline{z}_3, \dots, \overline{z}_m)$

Allora

z è costruibile a partire da $z_1, z_2, \dots, z_m$

se e solo se

$z \in F(u_1, u_2, \dots, u_r)$ con $u_1^2 \in F$ e $u_i^2 \in F(u_1, u_2, \dots, u_{i-1})$

Def Un campo come $F(u_1, u_2, \dots, u_r)$ si chiama **torre di radici quadrate** su F

Dim del criterio "$\Leftarrow$" $\mathbb{C}(z_1, \dots, z_m)$ chiuso per coniugio e radici quadrate $\Rightarrow F(u_1, u_2, \dots, u_r) \subseteq \mathbb{C}(z_1, \dots, z_m)$ ◢

"$\Rightarrow$" definiamo

$$C' \overset{def}{=} \{ z \in \mathbb{C} \mid z \text{ appartiene ad una torre di radici quadrate su } F \}$$

$z, z' \in C'$ allora $z \in F(u_1, \dots, u_r)$ e $z' \in F(u'_1, \dots, u'_s)$

torri di rad. quad. da cui otteniamo

$z+z', zz'$ appartengono a $F(u_1, \dots, u_r, u'_1, \dots, u'_s)$ torre di radici quadrate su F

Da questo si deduce che C' è un campo

Inoltre se $z^2 \in C'$, allora $z^2 = F(u_1, \dots, u_r)$ torre di r.q.

e $z \in F(u_1, \dots, u_r, z^2)$ torre di radici quadrate

quindi C' è chiuso per radici quadrate

Infine notiamo che $\overline{F} = \{\overline{z} \mid z \in F\} = F$ ($\overline{z}$: z coniugato)

quindi $z \in C' \Rightarrow z \in F(u_1, \dots, u_r)$ torre di r.q.

$\Rightarrow \overline{z} \in \overline{F}(\overline{u_1}, \dots, \overline{u_r}) = F(\overline{u_1}, \dots, \overline{u_r})$ torre di r.q.

$\Rightarrow \overline{z} \in C'$

Concludiamo che C' è un sottocampo di $\mathbb{C}$ che contiene $z_1, \dots, z_m$ chiuso per radici e per coniugio, ma $\mathbb{Q}(z_1, \dots, z_m)$ è il più piccolo sottocampo di $\mathbb{C}$ con queste proprietà e quindi $\mathbb{Q}(z_1, \dots, z_m) \subseteq C'$

Corollario Sia $F = \mathbb{Q}(z_1, \dots, z_m, \overline{z_1}, \dots, \overline{z_m})$

Se z è costruibile con riga e compasso a partire da $z_1, \dots, z_m$ allora z è algebrico su F con grado una potenza di 2

Dim. z costruibile $\Rightarrow$ $z \in F(u_1, u_2, \dots, u_n)$ torre di r.q.

$$[F(u_1, u_2, \dots, u_n) : F] = 2^t$$

perché $F(u_1, u_2, \dots, u_n)$ si può ottenere con estensioni successive di grado 1 o 2

Siccome $F(z) \subseteq F(u_1, u_2, \dots, u_n)$

abbiamo che

$$[F(u_1, u_2, \dots, u_n) : F] = [F(u_1, u_2, \dots, u_n) : F(z)]\,[F(z) : F]$$

per cui $[F(z) : F]$ divide 2^t

da cui la tesi ∎

TRISECAZIONE DELL'ANGOLO DI 60°

Ricordo che il problema era stato ridotto a questa forma

$\cos\frac{\pi}{9} + i \operatorname{sen}\frac{\pi}{9}$ è costruibile a partire da $\left\{0, 1, \frac{1}{2} + i\frac{\sqrt{3}}{2}\right\}$ "

Osserviamo che:

- $\mathbb{Q}(z_1, z_2, z_3, \overline{z}_3) = \mathbb{Q}(\sqrt{-3})$ e $[\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = 2$
- $\cos\frac{\pi}{9} + i \operatorname{sen}\frac{\pi}{9}$ è costruibile se e solo se $\cos\frac{\pi}{9}$ è costruibile.

Vale che:

$$\cos(3\theta) = \cos 2\theta \cos\theta - \operatorname{sen} 2\theta \operatorname{sen}\theta$$

$$= (2\cos^2\theta - 1)\cos\theta - 2\cos\theta \underbrace{\operatorname{sen}\theta \operatorname{sen}\theta}_{\operatorname{sen}^2\theta}$$

$$= 2\cos^3\theta - \cos\theta - 2\cos\theta(1-\cos^2\theta)$$

$$= 2\cos^3\theta - \cos\theta - 2\cos\theta + 2\cos^3\theta$$

$$= 4\cos^3\theta - 3\cos\theta$$

In questo caso $\theta = \frac{\pi}{9}$ $\cos(3\theta) = \cos(\frac{\pi}{3}) = \frac{1}{2}$

per cui $\cos\left(\frac{\pi}{9}\right)$ è radice del polinomio

$$p(x) = 4x^3 - 3x - \frac{1}{2}$$

Claim: $p(x)$ è irriducibile in $\mathbb{Q}[x]$

Dim. del claim:

$p(x)$ è irriducibile $\iff$ $p(\frac{1}{2}x) = \frac{1}{2}x^3 - \frac{3}{2}x - \frac{1}{2}$ è irriducibile

$p(\frac{1}{2}x)$ è irriducibile $\iff$ $q(x) = x^3 - 3x - 1$ irriducibile

$q(x)$ è riducibile $\iff$ $q(x)$ ha radici in $\mathbb{Q}$

(perché $\deg q(x) = 3$)

$q(x)$ ha radici in $\mathbb{Q}$ $\iff$ $q(x)$ ha radici in $\mathbb{Z}$

($q(x)$ è monico a coeff in $\mathbb{Z}$ (teorema delle radici razionali))

Problema:

dimostrare che se $p(x) \in \mathbb{Z}[x]$ monico

$p(x)$ ha radici intere se e solo se $p(x)$ ha radici razionali

[Concludendo:

$p(x)$ è irriducibile $\iff$ $q(x) = x^3 - 3x - 1$ non ha radici in $\mathbb{Z}$]

Se α fosse una radice di $q(x)$ in $\mathbb{Z}$ allora $\alpha^3 - 3\alpha = \alpha(\alpha^2 - 3) = 1$

$\Longrightarrow$ α divide 1 $\Rightarrow$ $\alpha = \pm 1$

ma $q(1) = -3$ $\quad$ $q(-1) = +1$

$q(x)$ non ha radici in $\mathbb{Z}$ $\Longrightarrow$ $p(x)$ è irriducibile

■ del Claim

$p(x)$ è il polinomio minimo di $\cos\frac{\pi}{9}$ su $\mathbb{Q}$ $\Rightarrow$

$\Rightarrow [\mathbb{Q}(\cos\frac{\pi}{9}) : \mathbb{Q}] = 3$

Se $\cos\frac{\pi}{9}$ fosse costruibile allora avremmo che

$$\left[\mathbb{Q}(\sqrt{-3})(\cos\tfrac{\pi}{9}) : \mathbb{Q}(\sqrt{-3})\right] = 2^t$$

$\mathbb{Q}(z_1, z_2, z_3, \bar{z}_3)$

ma è impossibile perchè avremmo che

$$[\mathbb{Q}(\sqrt{-3})(\cos\tfrac{\pi}{9}) : \mathbb{Q}] = [\mathbb{Q}(-\sqrt{3})(\cos\tfrac{\pi}{9}) : \mathbb{Q}(\sqrt{-3})][\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = 2^{t+1}$$

e

$$[\mathbb{Q}(\sqrt{3})(\cos\tfrac{\pi}{q}) : \mathbb{Q}] = 2^{t+1} = [\mathbb{Q}(\sqrt{3})(\cos\tfrac{\pi}{q}) : \mathbb{Q}(\cos\tfrac{\pi}{q})]\,[\underbrace{\mathbb{Q}(\cos\tfrac{\pi}{q}) : \mathbb{Q}}_{\text{''}3}]$$

arrivando all'assurdo che 3 divide 2^{t+1}

Possiamo concludere che $\cos\frac{\pi}{q}$ non è costruibile su $(0,1,\frac{1}{2}+i\frac{\sqrt{3}}{2})$ e l'angolo di 60° non è trisecabile con riga e compasso.

[Altri problemi classici]

DUPLICAZIONE DEL CUBO CON RIGA E COMPASSO

"È possibile costruire con riga e compasso un cubo di lato di volume 2 a partire da un cubo di volume 2?"

Traduciamo il problema con il nostro linguaggio

"A partire da $z_1 = 0$ e $z_2 = 1$ è possibile costruire con riga e compasso $\sqrt[3]{2}$?"

Osserviamo che

- $\mathbb{Q}(z_1, z_2) = \mathbb{Q}$
- $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

da cui si ricava che la risposta è NO.

COSTRUZIONE POLIGONI REGOLARI CON RIGA E COMPASSO

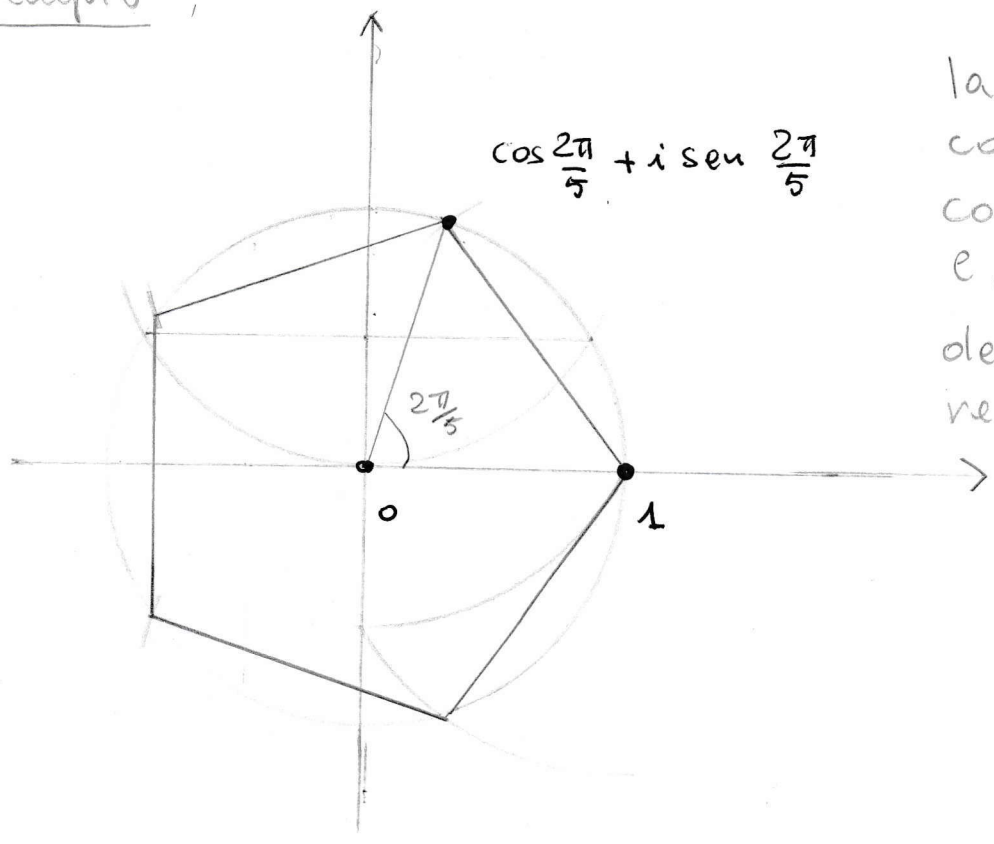
Consideriamo ora il caso di <u>poligoni con p lati dove p è primo</u>. Il problema è:

"È possibile costruire un poligono regolare con p lati usando riga e compasso partendo da un segmento unitario?"

<u>equivalentemente</u>

"È possibile costruire con riga e compasso $\omega_p \overset{def}{=} \cos 2\pi/p + i \operatorname{sen} 2\pi/p$ a partire da 0 e 1?"

<u>Esempio</u>:



la classica costruzione con riga e compasso del pentagono regolare

Osserviamo che

- $\mathbb{Q}(0,1) = \mathbb{Q}$
- ω_p è radice di $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \dots + x + 1)$
- $x^{p-1} + x^{p-2} + \dots + x + 1$ è irriducibile (vedi esercizi ottava settimana) e quindi è il polinomio minimo su $\mathbb{Q}$ di ω_p
- $[\mathbb{Q}(\omega_p) : \mathbb{Q}] = p - 1$

Sappiamo anche che se ω_p è costruibile allora

$$[\mathbb{Q}(\omega_p) : \mathbb{Q}] = 2^t$$

ottenendo $p = 1 + 2^t$

> Se p primo non è nella forma $1+2^t$ il poligono regolare con p lati non è costruibile con riga e compasso (esempio: $p=7$ l'ettagono)

Claim: se p primo e $p = 1 + 2^t$ per qualche primo allora t è una potenza di 2

Dim. del claim se $t = uv$ con u dispari, $u > 1$

$$x^u + 1 = (x+1)(x^{u-1} - x^{u-2} + x^{u-3} - \dots + 1)$$

da cui:

$$(2^t + 1) = (2^{uv} + 1) = (2^v + 1)(2^{(u-1)v} - 2^{(u-1)v-1} + \dots + 1)$$

e questo implica $2^t + 1$ non è primo

Concludendo $2^t + 1$ primo $\Rightarrow t = 2^h$

Conclusione: w_p costruibile $\Rightarrow p = 1 + 2^{2^h}$

Def: i primi del tipo $1 + 2^{2^h}$ si dicono primi di Fermat

Primi di Fermat conosciuti: 3, 5, 17, 257 e 65537

CONGETTURA: non ci sono altri primi di Fermat

[noi abbiamo ottenuto w_p costruibile $\Rightarrow p$ di Fermat
vale anche il viceversa ?]

I casi $p = 3, 5$ corrispondono alle classiche costruzioni del triangolo equilatero e del pentagono regolare $\Rightarrow w_3, w_5$ sono costruibili

Noi vedremo ora il caso $p=17$

In realtà vale il viceversa nel caso generale

(p primo di Fermat $\Rightarrow$ ω_p costruibile)

ma riprenderemo l'argomento più in avanti

COSTRUZIONE DEL POLIGONO REGOLARE CON 17 LATI

In questa parte $p=17$. Osserviamo che:

- $q(x) = x^{16} + x^{15} + \dots + 1$ è irriducibile (e separabile)
- $U = \{\text{radici di } x^{17}-1\} = \{1, \omega_p, \omega_p^2, \dots, \omega_p^{16}\} \cong \mathbb{Z}_{17}$ (U è un gruppo ciclico)
- $\mathbb{Q}(\omega_p)$ è il campo di spezzamento di $q(x) \Rightarrow$ $\mathbb{Q}(\omega_p)$ è un estensione di Galois $\Rightarrow$

$$|Gal(\mathbb{Q}(\omega_p)/\mathbb{Q})| = [\mathbb{Q}(\omega_p) : \mathbb{Q}] = 16$$

- se $\eta \in Gal(\mathbb{Q}[\omega_p] : \mathbb{Q})$ allora
  - $\eta(U) = U$ ($\eta(1)=1$ e η permuta le radici di $q(x)$)
  - $\eta : U \to U$ isom. di gruppi (η automorfismo di campo)

- $\eta(\omega_p)$ caratterizza η (i.e $\eta(\omega_p)=\eta'(\omega_p) \Rightarrow \eta=\eta'$)

- Siccome U è ciclico

$$\eta(\omega_p)=\underbrace{\omega_p^k}_{\text{possibili generatori di } U} \quad \text{con} \quad k=1,\dots,6$$

(In particolare se $\eta(\omega_p)=\omega_p$ allora $\eta=Id_U$)

- $\bar{\eta} \in Gal\left(\mathbb{Q}(\omega_p)/\mathbb{Q}\right)$ tale che $\bar{\eta}(\omega_p)=\omega_p^3$

genera tutto $Gal\left(\mathbb{Q}(\omega_p)/\mathbb{Q}\right)$ cioè

$Gal\left(\mathbb{Q}(\omega_p)/\mathbb{Q}\right)$ è ciclico di ordine 16

(provare per esercizio)

- Trovo una sequenza di gruppi di indice 2 e i corrispondenti sottocampi di $\mathbb{Q}(\omega_p)/\mathbb{Q}$

$$Gal\left(\frac{\mathbb{Q}(\omega_p)}{\mathbb{Q}}\right)=\langle\bar{\eta}\rangle \overset{\text{ind 2}}{\supseteq} \langle\bar{\eta}^2\rangle \overset{\text{ind 2}}{\supseteq} \langle\bar{\eta}^4\rangle \overset{\text{ind 2}}{\supseteq} \langle\bar{\eta}^8\rangle \overset{\text{ind 2}}{\supseteq} \{Id\}$$

Corrispondenza Galois

$$\downarrow \gamma_{MN} \qquad \downarrow \gamma_{MN} \qquad \downarrow \gamma_{MN} \qquad \downarrow \gamma_{MN} \qquad \downarrow \gamma_{MN}$$

$$\mathbb{Q} \subseteq E_1 \subseteq E_2 \subseteq E_3 \subseteq \mathbb{Q}(\omega_p)$$

estensione grado 2 | est. grado 2 | est. grado 2 | est grado 2

Sfruttando la seguente proposizione:

Proposizione: Sia $F \subseteq K$ estensione di campi con
$[K:F]=2$ e $\mathrm{char} F \neq 2$
Allora esiste $d \in K$ tale che $d^2 \in F$ e $F(d)=K$

otteniamo che $\mathbb{Q} \subseteq E_1 \subseteq E_2 \subseteq E_3 \subseteq \mathbb{Q}(\omega_p)$

è una torre di radici quadrate su $\mathbb{Q}$ che contiene $\omega_p = \omega_{17}$

$\Rightarrow$ ω_{17} è costruibile

[concludiamo con la dim della proposizione]

Dim della proposizione Esiste $c \in K \setminus F$

Siccome $[K:F]=2$ allora c è di grado 2 su F e $K = F(c)$

Inoltre esistono $a_1, a_2 \in F$ tali che $c^2 + a_1 c + a_2 = 0$

Se $a_1 = 0$ c è proprio il d che stò cercando

Se $a_1 \neq 0$ definisco $d \overset{def}{=} c + \frac{a_1}{2}$

osserviamo che
- $c + \frac{a_1}{2} \notin F$
- $\left(c + \frac{a_1}{2}\right)^2 + \left(a_2 - \frac{a_1^2}{4}\right) = 0$
  $\left(c + \frac{a_1}{2}\right)^2 = d^2$, $\left(a_2 - \frac{a_1^2}{4}\right) \in F$

Quindi $[F(d):F]=2$ e $F(d)=K$ ∎

Problema: vale la proposizione per $\mathrm{char} F = 2$