# Corso:Algebra IV I1/Costruzioni con righe e compasso/Criterio per la costruibilità

## 1 Lemmi preliminari

Considereremo sottocampi $F \subseteq \mathbb{C}$ tali che

1. $F$ contiene l'unità immaginaria, cioè $i \in F$ ;
2. $F$ è chiuso rispetto al coniugio, cioè se $z \in F$ , anche $\bar{z} \in F$ .

**Lemma 5.1**

Sia $F \subseteq \mathbb{C}$ un campo che soddisfa le proprietà 1 e 2. Siano $z_1 = x_1 + iy_1$ e $z_2 = x_2 + iy_2$ due elementi di $F$ , allora

1. $x_1, x_2, y_1, y_2 \in F$ ;
2. se $y = \alpha x + \beta$ è l'equazione della retta che passa per $(x_1, y_1)$ e $(x_2, y_2)$ , allora $\alpha, \beta \in F$ .
3. se $(x - x_1)^2 + (y - y_1)^2 = r^2$ è l'equazione della circonferenza di centro $(x_1, y_1)$ e passante per il punto di coordinate $(x_2, y_2)$ , allora $r^2 \in F$ .

*Dimostrazione*

1. $z_1 \in F$ , e siccome $F$ è chiuso per coniugio, anche $\bar{z}_1 = x_1 - iy_1 \in F$ , allora siccome $F$ è chiuso rispetto alla somma e alla differenza, si ha $z_1 + \bar{z}_1 = 2x_1 \in F$ , e $z_1 - \bar{z}_1 = 2iy_1 \in F$ . Di conseguenza, siccome $i \in F$ e $2 \in F$ , anche $x_1, y_1 \in F$ , e lo stesso vale per $x_2, y_2$ .
2. Se $y = \alpha x + \beta$ è la retta che passa per $(x_1, y_1)$ e $(x_2, y_2)$ , segue che $y_1 = \alpha x_1 + \beta$ e $y_2 = \alpha x_2 + \beta$ , allora, facendo la differenza tra queste due condizioni, si ha
$$y_1 - y_2 = \alpha(x_1 - x_2)$$
$$\longrightarrow \alpha = \frac{y_1 - y_2}{x_1 - x_2}$$
quindi $\alpha \in F$ , perché è espressa come somma e differenza e prodotto di elementi che per il punto 1 stanno in $F$ . Di conseguenza, siccome per la prima equazione $\beta = y_1 - \alpha x_1$ si ha anche $\beta \in F$ .

3. Se $(x-x_1)^2+(y-y_1)^2 = r^2$ è l'equazione della circonferenza di centro $(x_1, y_1)$ e passante per $(x_2, y_2)$ , sostituendo le coordinate di $(x_2, y_2)$ nell'equazione segue che
$$r^2 = (x_1 - y_1)^2 + (x_2 - y_2)^2$$
cioè $r^2 \in F$ .

**Lemma 5.2**

Sia $F \subseteq \mathbb{C}$ un campo che soddisfa le proprietà 1 e 2. Sia $z = u + iv \in \mathbb{C}$ , dove $(u, v)$ si ottiene come intersezione di

1. due rette definite a partire da punti in $F$ ,
2. retta e circonferenza definite a partire da punti in $F$ ,
3. due circonferenze definite a partire da punti di $F$ .

Allora $|F(z) : F| \leq 2$ .

*Dimostrazione*

Distinguiamo i tre casi:

1. $(u, v)$ **è punto di intersezione di due rette**, $y = \alpha_1 x+\beta_1$ e $y = \alpha_2 x+\beta_2$ . Per il lemma precedente $\alpha_1, \alpha_2, \beta_1, \beta_2 \in F$ , allora
$$\begin{cases} v = \alpha_1 u + \beta_1 \\ v = \alpha_2 u + \beta_2 \end{cases}$$
e, sottraendo tra loro le due equazioni, ottengo
$$(\alpha_1 - \alpha_2)u = \beta_1 - \beta_2, \longrightarrow u = \frac{\beta_1 - \beta_2}{\alpha_1 - \alpha_2}$$
cioè $u \in F$ . Per la prima equazione anche $v \in F$ . Siccome $F$ contiene l'unità immaginaria, $z \in F$ e quindi $F(z) = F$ e l'estensione ha grado 1.

2. $(u, v)$ **è punto d'intersezione tra la retta di equazione** $y = \alpha x+\beta$ **e la circonferenza di equazione** $(x-a)^2+(y-b)^2 = r^2$ .Allora $\alpha, \beta, a, b, r^2 \in F$ per il lemma precedente. Sostituendo le coordinate di $(u, v)$ nelle due equazioni ottengo
$$\begin{cases} v = \alpha u + \beta \\ (u - a)^2 + (v - b)^2 = r^2 \end{cases}$$
e sostituendo la prima equazione nella seconda ottengo
$$(u - a)^2 + (\alpha u + \beta - b)^2 = r^2$$
Quest'equazione è di secondo grado e ha coefficienti in $F$ . Allora $|F(u) : F| \leq 2$ .Inoltre $v = \alpha u + \beta, \longrightarrow v \in F(u)$ , si ha che $i \in F$ , quindi $z = u + iv \in F(u)$ , quindi $|F(z) : F| \leq 2$ .

3. $(u, v)$ **si ottiene come punto di intersezione di due circonferenze**,

$$\mathcal{C}_1 : x^2 + y^2 + ax + by + c = 0$$

$$\mathcal{C}_2 : x^2 + y^2 + \alpha x + \beta y + \gamma = 0$$

Allora $(u, v)$ soddisfa l'equazione ottenuta sottraendo $\mathcal{C}_1$ a $\mathcal{C}_2$ , cioè

$$(a - \alpha)x + (b - \beta)y + c - \gamma = 0$$

che è l'equazione di una retta, e quindi ci si riconduce al caso 2.

## 2 Condizione necessaria e sufficiente per la costruibilità

**Teorema 5.2**

Un numero complesso $z \in \mathbb{C}$ è costruibile se e solo se esiste una catena di campi della forma $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$ , dove $z \in K_r$ , e $|K_{i+1} : K_i| \leq 2$ .

*Dimostrazione*

$1 \longrightarrow 2$ : Supponiamo che $z$ sia costruibile, allora esiste una successione

$$0,\ 1,\ z_1 = i,\ z_2, \ldots, z_s = z$$

dove gli $z_i$ sono numeri complessi tali che $z_{i+1}$ si ottiene come punto di intersezione di retta-retta, retta-circonferenza o circonferenza-circonferenza, definite a partire dagli elementi precedenti della successione, cioè a partire dai punti $0, 1, z_1, \ldots, z_i$ .

Definiamo

$$E_0 = F_0 := \mathbb{Q}$$

$$E_1 = F_1 := \mathbb{Q}(i).$$

$$Supponendo\, di\, aver\, definito\, E_i,\ definiamo$$

$$F_{i+1} = E_i(z_{i+1});\ E_{i+1} = F_{i+1}(\bar{z}_{i+1})$$

Supponiamo di aver dimostrato che $E_i$ contenga l'unità immaginaria e sia chiuso per coniugio. Allora vogliamo provare che

1. $|F_{i+1} : E_i| \leq 2$
2. $|E_{i+1} : F_{i+1}| \leq 2$
3. anche $E_{i+1}$ soddisfa le proprietà 1 e 2.

L'affermazione $I$) è vera perché $E_i$ e $z_{i+1}$ soddisfano le ipotesi del lemma 2. L'unita' immaginaria $i$ è contenuta in ogni $E_j$ . Per dimostrare le affermazioni I) e II) distinguiamo due casi:

- $Z_{i+1} \in E_i$ , e quindi $F_{i+1} = E_i(z_{i+1}) = E_i$ . Per ipotesi, $E_i$ è chiuso per coniugio, quindi $\bar{z}_{i+1} \in E_i$ , segue anche che $E_{i+1} = E_i$ ; per quest'ultimo fatto, ovviamente si ha $|E_{i+1} : F_{i+1}| = 1 \leq 2$ e $E_{i+1}$ soddisfa le proprietà 1 e 2, e valgono quindi le affermazioni II) e III).
- $Z_{I+1}$ HA GRADO 2 SU $E_I$ , segue che $z_{i+1}$ ha un polinomio minimo della forma $x^2 + \alpha x + \beta \in E_i[x]$ , cioè $z_{i+1}$ risolve l'equazione $z^2 + \alpha z + \beta = 0$ . Passando ai coniugati, segue che $\bar{z}_{i+1}$ è radice del polinomio $z^2 + \bar{\alpha} z + \bar{\beta}$ a coefficienti in $E_i[x]$ , e quindi anche in $F_{i+1}[x]$ . Allora rimane vero che $|E_{i+1} : F_{i+1}| \leq 2$ , perché $E_{i+1} = F_{i+1}(\bar{z}_{i+1})$ , e vale l'affermazione II).

La chiusura per coniugio di $E_{i+1}$ segue dal fatto che

$$E_{i+1} = F_{i+1}(\bar{z}_{i+1}) = E_i(z_{i+1}, \bar{z}_{i+1})$$

quindi, un generico elemento di $E_{i+1}$ è della forma

$$(\alpha + \beta z_{i+1}) + (\gamma + \delta z_{i+1})\bar{z}_{i+1},\ \alpha, \beta, \delta, \gamma \in E_i$$

e quindi anche il coniugato di questo elemento sta ancora in $E_{i+1}$ ( $\bar{\alpha}, \bar{\beta}, \bar{\delta}, \bar{\gamma}$ stanno ancora in $E_i$ perché $E_i$ è chiuso rispetto al coniugio).

Provando le affermazioni I), II), e III) abbiamo costruito una catena di estensioni

$$E_0 = F_0 = \mathbb{Q} \subseteq E_1 = F_1 = \mathbb{Q}(i) \subseteq F_2 \subseteq E_2 \subseteq F_3 \subseteq E_3 \subseteq \cdots \subseteq F_t \subseteq E_t$$

come nell'enunciato.

$2 \longrightarrow 1$ : viceversa, dobbiamo dimostrare che se esiste una catena di campi

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$$

dove $z \in K_r$ e $|K_{i+1} : K_i| \leq 2$ allora $z$ è costruibile.

Basta dimostrare il seguente fatto: **se $F$ è un sottocampo di $\mathbb{C}$ , tutti gli elementi di $F$ sono costruibili ed esiste $E$ tale che $|E : F| = 2$ , allora tutti gli elementi di $E$ sono costruibili**. Vogliamo quindi mostrare che ogni $\alpha \in E \setminus F$ è costruibile. Siccome $|E : F| = 2$ , dato $\alpha \in E \setminus F$ , segue che $F(\alpha) = E$ , e $\alpha$ sarà lo zero di un polinomio della forma $x^2 + bx + c$ a coefficienti in $F$ . Posto $\Delta = b^2 - 4c$ , si ha $\delta \in F$ e $\alpha = \frac{-b \pm \sqrt{\delta}}{2}$ , e $\alpha$ è costruibile se $\sqrt{\delta}$ è costruibile, quindi non è restrittivo supporre che $\alpha^2 \in F$ . Pongo $\alpha^2 = a$ , **e mostriamo che $\sqrt{a}$ è costruibile**. Distinguiamo due casi:

CASO 1: $A \in \mathbb{R}, A > 0$ . Allora $\sqrt{a}$ è costruibile con le seguenti operazioni:

- traccio la circonferenza $\mathcal{C}$ con centro in $((a+1)/2, 0)$ passante per $(0, 0)$ ;
- costruisco la retta $\mathcal{R}$ passante per $(1, 0)$ e parallela all'asse delle y (per fissare le idee suppongo che $(a+1)/2 > 1$ ).
- chiamo $P$ il punto di intersezione tra $\mathcal{C}$ ed $\mathcal{R}$ di ascissa positiva, e ne determino le coordinate.

$\mathcal{C}$ ha equazione

$$(x-(a+1)/2)^2+y^2=((a+1)/2)^2$$

e ponendo $r=(a+1)/2$ :

$$(x-r)^2+y^2=r^2$$
$$x^2+r^2-2rx+y^2=r^2$$

e il punto di intersezione tra $\mathcal{C}$ e la retta $\mathcal{R}: x=1$ ottengo

$$y^2=2r-1, \longrightarrow y^+=\sqrt{2r-1}=\sqrt{2(a+1)/2-1}=\sqrt{a}$$

$P$ ha coordinate $(1,\sqrt{a})$ .

- costruisco la retta $\mathcal{L}$ passante per $P$ e parallela all'asse x.
- il punto di intersezione tra $\mathcal{L}$ e l'asse y ha coordinate $(0,\sqrt{a})$ .

CASO 2: $A\in\mathbb{C}$ , cioè $a=re^{i\theta}=r(\cos\theta+i\sin\theta)$ . $\sqrt{a}$ è costruibile con le seguenti operazioni:

- considero la circonferenza $\mathcal{C}$ centrata nell'origine e passante per $P=(r\cos\theta, r\sin\theta)$ (posso farlo perché per ipotesi $a\in F$ ).
- chiamo $Q$ il punto di intersezione tra $\mathcal{C}$ e l'asse x, cioè $Q=(r,0)$ .
- chiamo $\mathcal{R}$ la retta passante per $Q$ e $P$ .
- Traccio la retta $\mathcal{L}$ ortogonale a $\mathcal{R}$ passante per il punto medio tra $P$ e $Q$ .
- ho individuato il punto $T$ intersezione di $\mathcal{C}$ ed $\mathcal{L}$ , che ha coordinate $(r\cos(\theta/2),\ r\sin(\theta/2))$ cioe' $re^{i\theta/2}$ e' costruibile.

Osservo che $\sqrt{a}=\sqrt{r}e^{i\theta/2}$ , e siccome abbiamo appena mostrato che $b=re^{i\theta/2}$ è costruibile, allora possiamo costruire $a=1/\sqrt{r}*b$ dove $\sqrt{r}$ è costruibile per il caso 1.

**Corollario 5.2**

Sia $z\in\mathbb{C}$ , se $z$ è costruibile allora $|\mathbb{Q}(z):\mathbb{Q}|=2^n$ con $n\geq 0$ .

*Dimostrazione*

Se $z$ è costruibile, esiste un campo $K_r\supseteq\mathbb{Q}$ con $z\in K_r$ e $|K_r:\mathbb{Q}|=2^s$ . Siccome $K_r\supseteq\mathbb{Q}(z)\supseteq\mathbb{Q}$ , $|\mathbb{Q}(z):\mathbb{Q}|\mid 2^s$ e quindi è una potenza di 2.

# 3 Tre problemi classici

Discutiamo i seguenti problemi classici:

1. QUADRATURA DEL CERCHIO: **si vuole costruire con riga e compasso un quadrato di area pari a quella di un cerchio dato**.Assumiamo che il cerchio abbia raggio 1, allora per risolvere il problema bisognerebbe costruire con riga e compasso $\sqrt{\pi}$ . Questo non e' possibile perché $\sqrt{\pi}$ è trascendente su $\mathbb{Q}$ , mentre per la proposizione precedente $z$ è costruibile solo se $|\mathbb{Q}(z) : \mathbb{Q}| = 2^n$, $n \geq 0$ .
2. DUPLICAZIONE DEL CUBO: **costruire con riga e compasso un cubo di volume doppio del volume di un cubo dato**. Assumiamo che il cubo dato abbia lato 1, allora bisognerebbe costruire con riga e compasso $\sqrt[3]{2}$ , ma $\sqrt[3]{2}$ ha grado 3 su $\mathbb{Q}$ , e quindi non è costruibile perché non soddisfa le ipotesi del corollario.
3. TRISEZIONE DELL'ANGOLO DI $\pi/3$ : **costruire un angolo pari a un terzo di quello dato**. Posso costruire $\cos(\pi/3) + i\sin(\pi/3) = 1/2 + i\sqrt{3}/2$ con le seguenti operazioni:#*costruisco la circonferenza di centro l'origine e raggio 1;#*costruisco la retta $\mathcal{R}$ passante per $(1/2, 0)$ e parallela all'asse y.#*il punto $(1/2, \sqrt{3}/2)$ è uno dei punti di intersezione tra $\mathcal{C}$ e $\mathcal{R}$ .Tuttavia non posso costruire $e^{i\pi/9}$ , perché questa è una radice primitiva 18-esima dell'unità, il cui polinomio minimo ha grado $\varphi(18) = 6$ , e non è una potenza di 2.

# 4 Costruzione di poligoni regolari

**Teorema 5.3**

Sia $p > 2$ un numero primo, allora il poligono regolare con $p$ lati è costruibile se e solo se $p$ è della forma $2^{2^s} + 1$ , $s \in \mathbb{N}$ .

*Dimostrazione*

Il poligono regolare con $p$ lati è costruibile se e solo se è costruibile una radice primitiva $p$ -esima dell'unità.

$1 \longrightarrow 2$ : per ipotesi, la radice primitiva $\omega = \cos(2\pi/p) + i\sin(2\pi/p) = e^{i2\pi/p}$ è costruibile, allora $|\mathbb{Q}(\omega) : \mathbb{Q}| = 2^m$, $m \in \mathbb{N}$ per il corollario. Inoltre $\omega$ ha come polinomio minimo $\phi_p(x)$ e $\mathrm{gr}(\phi_\mathrm{p}(\mathrm{x})) = \varphi(\mathrm{p}) = \mathrm{p} - 1$ , quindi $|\mathbb{Q}(\omega) : \mathbb{Q}| = p - 1$ . Eguagliando le due espressioni di $|\mathbb{Q}(\omega) : \mathbb{Q}|$ segue quindi che $p - 1 = 2^m$ , cioè $p = 2^m + 1$ . **Proviamo che** $m = 2^s$ .

Se $m$ non è una potenza di 2, potrò scrivere $m = k * l$ con $k$ numero dispari. Il polinomio $x^k + 1$ ammette $-1$ come radice quindi

$$x^k + 1 = (x + 1) * f(x),\ f(x) \in \mathbb{Z}[x]$$
$$\longrightarrow p = 2^m + 1 = 2^{kl} + 1 = (2^l)^k + 1 = (2^l + 1) * f(2^l)$$

ma questo contraddice il fatto che $p$ sia primo. Rimane provato che $m$ è una potenza di 2.

$2 \longrightarrow 1$ : per ipotesi $p = 2^{2^s} + 1$ , considero $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$ con $\omega$ radice primitiva $p$ -esima dell'unità. Il gruppo $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$ è abeliano di ordine $2^{2^s}$ (anzi ciclico perché $p$ è primo). Allora esiste una catena di sottogruppi $G = G_0 \supseteq G_1 \supseteq G_2 \cdots \supseteq G_s = 1$ , dove $G_{i+1}$ è normale in $G_i$ e $o(G_i/G_{i+1}) = 2$ . Per il teorema della corrispondenza di Galois, considerando i campi intermedi $(G_i)'$ , trovo una catena di campi $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_r = \mathbb{Q}(\omega)$ con $|K_{i+1} : K_i| = 2$ , e questo significa che $\omega$ è costruibile per il teoerma che fornisce un criterio per la costruibilita' (il primo teorema della sezione).

Più in generale, se considero un poligono regolare con $n$ lati, esso è costruibile se è costruibile una radice $n$ -esima primitiva dell'unità $\omega$ , e $\omega$ ha grado $\varphi(n)$ sopra $\mathbb{Q}$ . Ora $\omega$ è costruibile se e solo se $n = 2^k * p_1 * p_2 * \cdots * p_s$ , dove $p_i \neq p_j$ per $i \neq j$ e $p_i = 2^{2^{s_i}} + 1$ .

# 5 Fonti per testo e immagini; autori; licenze

## 5.1 Testo

- **Corso:Algebra IV I1/Costruzioni con righe e compasso/Criterio per la costruibilità** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Costruzioni_con_righe_e_compasso/Criterio_per_la_costruibilit%C3%A0?oldid=48059 *Contributori:* Toma.luca95, Irene, ScimmiaSpaziale e Mmontrasio

## 5.2 Immagini

## 5.3 Licenza dell'opera