# Costruzioni con riga e compasso

Giacomo Mezzedimi

16 Febbraio 2015

In questo articolo illustreremo quali costruzioni sono possibili utilizzando solamente riga e compasso; in particolare ci concentreremo su quali poligoni regolari sono effettivamente costruibili.

*Regole del gioco*: Ho una retta con punto iniziale 0 e punto unitá 1. Posso tracciare una retta per due punti giá dati oppure tracciare una circonferenza con centro in un punto giá dato e raggio pari alla distanza di due punti giá dati.

**Proposizione 1.** *Data una retta e un suo punto, si puó costruire la perpendicolare in quel punto.*

*Dimostrazione.* Segue da Fig. 1. □

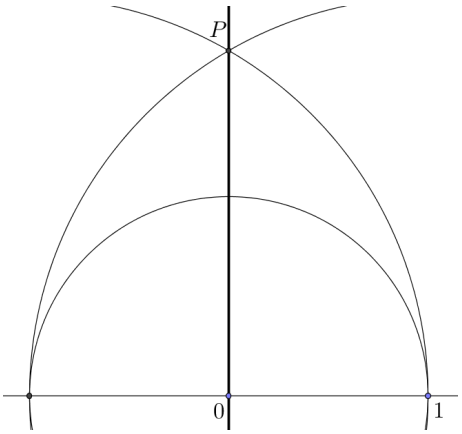


Figura 1: Perpendicolare a una retta per un punto

**Proposizione 2.** *Data una retta, si puó costruire la parallela per un punto non su essa.*

*Dimostrazione.* Basta costruire la perpendicolare della perpendicolare. □

**Proposizione 3.** *Se su una retta ho $a$ e $b$, allora posso costruire anche $a+b$ e $b-a$.*

*Dimostrazione.* Puntando il compasso su $b$ e prendendo come raggio il segmento $\overline{0a}$, si ottengono $a+b$ e $b-a$ come intersezione fra la retta e la circonferenza. □

Denotiamo con $\mathbb{K}$ l'insieme dei numeri costruibili sulla retta data.

**Corollario.** $(\mathbb{K}, +)$ *é un gruppo.*

**Proposizione 4.** *Dati $a$ e $b$, si possono costruire $a \cdot b$ e $\frac{b}{a}$.*

*Dimostrazione.* Segue da Fig. 2 e Fig. 3 per Talete. □

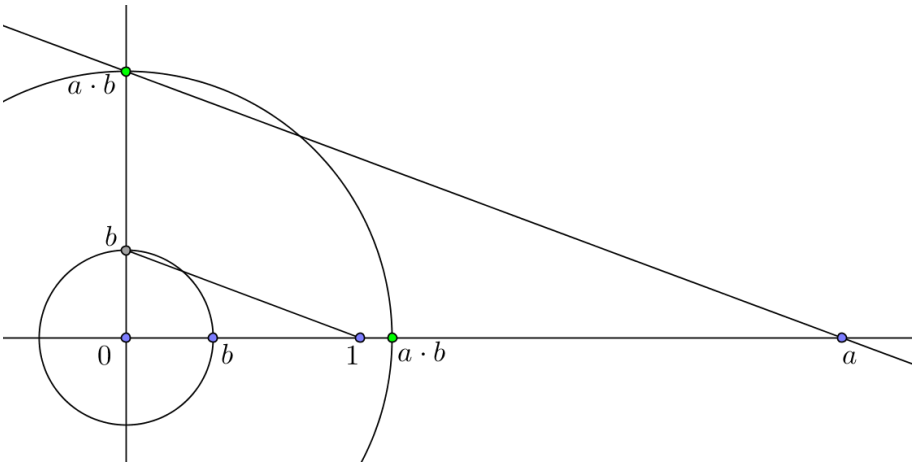


Figura 2: Moltiplicazione di due numeri dati

**Corollario.** $(\mathbb{K}, +, \cdot)$ *é un campo.*

**Proposizione 5.** *Sulla retta $\mathbb{K}$ posso ottenere tutti i razionali e tutte le radici quadrate.*

*Dimostrazione.* Per quanto visto si possono costruire i razionali; le radici quadrate si costruiscono come in Fig. 4:

1. Si costruisce la circonferenza che ha per diametro il segmento $\overline{0(a+1)}$.

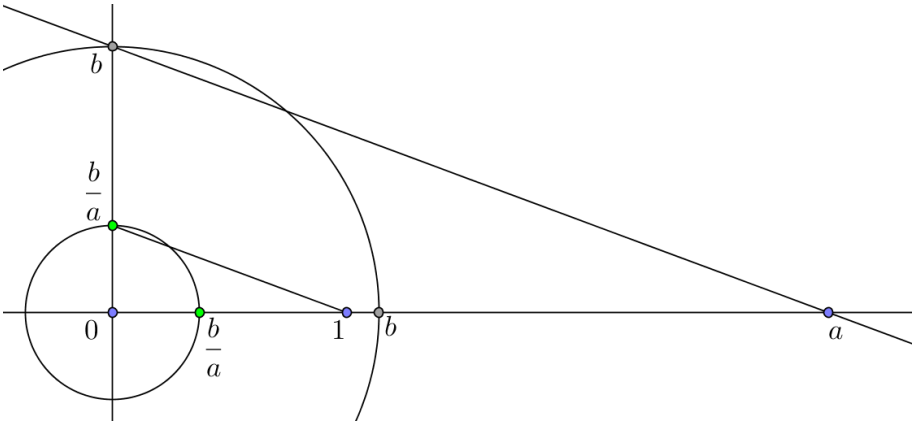


Figura 3: Divisione di due numeri dati

2. Sia $P$ il punto di intersezione fra la circonferenza e la perpendicolare alla retta per 1; allora $\overline{1P} = \sqrt{\left(\frac{a+1}{2}\right)^2 - \left(\frac{a+1}{2} - 1\right)^2} = \sqrt{a}$.
3. Si porta $P$ sulla retta, ottenendo il punto $1 + \sqrt{a}$; a questo punto basta togliere 1.

□

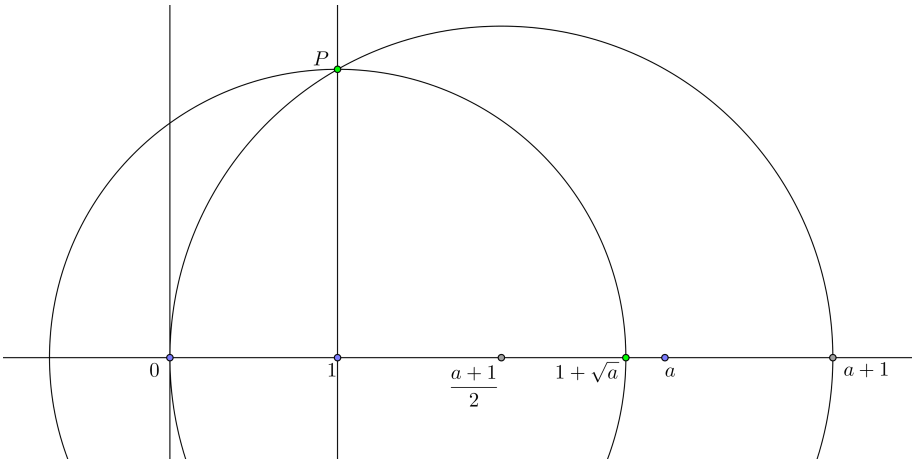


Figura 4: Radice quadrata di un numero

Ad ogni passaggio, i punti "nuovi"si ottengono tramite l'intersezione di due rette, di una retta e di una circonferenza, e di due circonferenze.
Studiamo ogni caso separatamente:

- Due rette hanno equazioni a coefficienti in $\mathbb{K} \Rightarrow$ le coordinate dell'intersezione stanno in $\mathbb{K}$, poiché se le rette sono $y = ax + b$ e $y = \alpha x + \beta$, l'intersezione é $P = (\frac{\beta - b}{a - \alpha}, a \cdot \frac{\beta - b}{a - \alpha} + b)$.
- L'intersezione di retta e circonferenza a coefficienti in $\mathbb{K}$ sta in un'estensione di grado $\leq 2$ di $\mathbb{K}$, poiché é soluzione di un'equazione di grado 2.
- Per la Fig. 5, il caso dell'intersezione fra due circonferenze é analogo al caso precedente.

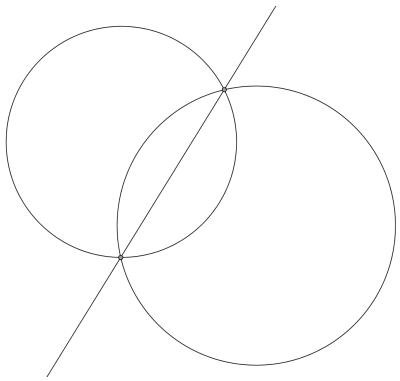

Figura 5: Intersezione fra due circonferenze

Denotiamo con $\mathbb{F}$ il campo dei numeri algebrici su $\mathbb{Q}$ ottenibili da $\mathbb{Q}$ tramite una successione di estensioni di grado $\leq 2$.

**Proposizione 6.** *$\sigma : \mathbb{F} \times \mathbb{F} \hookrightarrow \mathbb{C} | (a, b) \to a + ib$ é un'immersione e $a + ib \in \mathbb{C}$ sta in un'estensione ottenibile tramite una successione di estensioni di grado $\leq 2 \Leftrightarrow (a, b) \in \mathbb{F} \times \mathbb{F}$.*

*Dimostrazione.* Che $\sigma$ sia un'immersione é evidente. Inoltre, se $(a, b) \in \mathbb{F} \times \mathbb{F}$, allora $a + ib \in \mathbb{Q}(a, b, i) = \mathbb{Q}(a)(b)(i)$, che é un'estensione successione di estensioni di grado $\leq 2$.
Viceversa, se $a + ib$ sta in un'estensione successione di estensioni di grado $\leq 2$, lo stesso vale per $a - ib$, e dunque anche per $(a + ib) + (a - ib) = 2a$ e $(a + ib) - (a - ib) = 2ib$, e dunque per $a$ e $b$. □

Dunque d'ora in poi considereremo il piano $\mathbb{F} \times \mathbb{F}$ come gli elementi del piano complesso che stanno in estensioni di $\mathbb{Q}$ successioni di estensioni di grado $\leq 2$.
Condizione necessaria é dunque che il grado sia una potenza di 2.

**Proposizione 7.** *La duplicazione del cubo é impossibile con riga e compasso.*

*Dimostrazione.* Bisogna ottenere $\alpha = \sqrt[3]{2}$, che é il lato del cubo doppio; ma $\alpha$ non si puó ottenere perché $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ non é potenza di 2. □

**Proposizione 8.** *Se $\theta \neq k\frac{\pi}{2}$, non si puó trisecare l'angolo $\theta$ con riga e compasso.*

*Dimostrazione.* Si puó trisecare $\theta \Leftrightarrow$ si puó costruire $w = \sqrt[3]{2}$, con $z = e^{i\theta}$.
Ma se $\theta \neq k\frac{\pi}{2}$, $w^3 - z$ é il polinomio minimo di $z$, e come prima 3 non é potenza di 2. □

**Proposizione 9.** *Non si puó realizzare la quadratura del cerchio con riga e compasso.*

*Dimostrazione.* Per realizzarla dovremmo costruire $\sqrt{\pi}$, impossibile perché $\pi$ é trascendente su $\mathbb{Q}$. □

**Definizione 1.** *Un primo $p$ si dice* ***primo di Fermat*** *se esiste $k$ tale che $p = 2^{2^k} + 1$.*

**Proposizione 10.** *Un $n$-agono regolare é costruibile con riga e compasso $\Leftrightarrow$ $n = 2^\alpha \cdot p_1 \cdot \ldots \cdot p_m$, dove $p_i = 2^{2^{k_i}} + 1$ é un primo di Fermat $\forall i$.*

*Dimostrazione.* Per costruire l'$n$-agono, mi basta costruire $\zeta_n = e^{i\frac{2\pi}{n}}$.
$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, dunque una condizione necessaria é che $\phi(n) = 2^t$ per $t \in \mathbb{N}$.
Ora:

$$n = 2^\alpha \cdot p_1^{\beta_1} \cdot \ldots \cdot p_m^{\beta_m} \Rightarrow \phi(n) = 2^{\alpha-1} \cdot (p_1 - 1)p_1^{\beta_1 - 1} \cdot \ldots \cdot (p_m - 1)p_m^{\beta_m - 1},$$

dunque $\beta_1 = \ldots \beta_m = 1$. Inoltre $p_i - 1 = 2^{e_i}$ per un certo $e_i$ $\forall i$.
Ma $p = 2^e + 1$ primo $\Rightarrow e = 2^k$, altrimenti si scomporrebbe non banalmente.
Vediamo che questa é anche condizione sufficiente.
Devo trovare $\mathbb{Q} \subseteq \mathbb{K}_1 \subseteq \ldots \subseteq \mathbb{Q}(\zeta_n)$ tali che $[\mathbb{K}_{i+1} : \mathbb{K}_i] = 2$ $\forall i$, ma esistono perché $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$, essendo abeliano, ha sottogruppi di ogni possibile ordine. □