**Università degli Studi di Verona**

DIPARTIMENTO DI INFORMATICA
Corso di Laurea in Matematica Applicata

Tesi di laurea triennale

# Costruzioni geometriche con riga e compasso

Candidato:
**Orazio Alibrandi**
**Matricola VR478719**

Relatore:
**Prof.ssa Francesca Mantese**

**Anno Accademico 2023–2024**

...

# Indice

# Introduzione

In questo elaborato tratteremo uno degli argomenti più importanti per gli sviluppi degli studi della geometria nell'antica Grecia, ossia le costruzioni con riga e compasso. Gli antichi matematici greci si interessarono a questa tecnica, e scoprirono come costruire somme, differenze, prodotti, rapporti e radici quadrate di lunghezze date. Col passare degli anni, approfondirono le loro ricerche, affrontando una serie sempre crescente di problemi, talvolta risolvendoli, talvolta riscontrando delle difficoltà. Ad esempio, dato un angolo qualsiasi, trovarono come dividerlo in due angoli uguali, ma non riuscirono a dividerlo in tre angoli uguali. In molti tentarono di risolvere questi problemi, ma solo utilizzando altre tecniche di costruzione riuscirono nel loro intento. Solamente nel diciottesimo secolo Pierre Wantzel, e successivamente Ferdinand Von Lindemann, dimostrarono l'impossibilità dei cosiddetti "tre problemi classici dell'antichità", ossia la trisezione dell'angolo, la quadratura del cerchio e la duplicazione del cubo, mentre Carl Friedrich Gauss dimostrò una condizione sufficiente per la costruzione di poligoni a $n$ lati regolari. Nelle seguenti pagine, definiremo cos'è un numero costruibile con riga e compasso ed illustreremo alcuni esempi di costruzione di poligoni regolari come esagono e quadrato. Dopodiché, procederemo con l'enunciare e dimostrare i principali teoremi di estensioni algebriche e della Teoria di Galois che sfrutteremo successivamente per dimostrare il Criterio di Costruibilità di Gauss per le costruzioni con riga e compasso, che stabilisce quali poligoni regolari sono costruibili in un numero finito di passi. In secondo luogo, discuteremo i tre problemi classici dell'antichità e dimostreremo che non sono risolvibili con il solo utilizzo delle tecniche sopra citate. Infine, introdurremo le costruzioni con il metodo origami, che rispetto alle precedenti offrono numerose possibilità in più, con la quale possiamo risolvere due dei tre problemi classici. Infine, enunceremo il Criterio di Costruibilità con Origami per evidenziarne le differenze con le costruzioni classiche.

# 1 Informazioni preliminari

In questa sezione iniziale, menzioniamo delle definizioni fondamentali e alcuni risultati utili che useremo nel corso dell'elaborato. Le seguenti informazioni possono essere trovate all'interno del libro *Abstract algebra* di *Israel Nathan Herstein* [5].

### Anelli

**Definizione 1.1.** Un anello $(R, +, \cdot)$ è un insieme non vuoto $R$ su cui sono definite due operazioni $+, \cdot : R \times R \longrightarrow R$ che godono delle seguenti proprietà:

- $R_1 : (R, +)$ è un gruppo abeliano con elemento neutro $0_R$
- $R_2 : (R, \cdot)$ gode della proprietà associativa e possiede un elemento neutro $1_R$
- $R_3$ : Leggi distributive
  - $a(b + c) = ab + ac$
  - $(a + b)c = ac + bc$ per $a, b \in R$

  R è detto commutativo se $(R, \cdot)$ gode della proprietà commutativa.

**Definizione 1.2.** Un campo è un anello commutativo tale che $R^* = R \setminus \{0_R\}$. In altre parole, $(R \setminus \{0_R\}, \cdot)$ è un gruppo abeliano.

**Definizione 1.3.** Sia $(R, +, \cdot)$ un anello (campo). Un sottoinsieme non vuoto $S \subset R$ si dice sottoanello (sottocampo) se $(S, +, \cdot)$ è un anello (campo).

### Ideali

**Definizione 1.4.** Dato un anello $R$, un sottoinsieme non vuoto $I \subset R$ è un ideale (bilatero) di $R$ se gode delle proprietà:

$(i)$ se $a, b \in I$, allora $a + b \in I$

$(ii)$ se $a \in I$ e $r \in R$, allora $ra, ar \in I$.

**Definizione 1.5.** Sia $(R, +, \cdot)$ un anello e sia $I$ un ideale di $R$. Poiché $(I, +) \lhd (R, +)$, possiamo considerare il gruppo quoziente $(R/I, +)$ dato dai laterali di $R$ modulo $I$: $a = \{x \in R | x - a \in I\} = a + I$.

**Definizione 1.6** (Phi di Eulero)**.** Per ogni $n \in \mathbb{N}$, denotiamo con $\varphi(n)$ il numero degli $0 < a < n$ che sono primi con $n$, ovvero

$$\varphi(n) = |\mathbb{Z}/n\mathbb{Z}^*|$$

Otteniamo una funzione $\varphi(n) : \mathbb{N} \to \mathbb{N}$ che si calcola come segue:
Se $n = p_1^{r_1} \cdot ... \cdot p_m^{r_m}$ è la scomposizione di $n$ in fattori primi, allora

$$\varphi(n) = n(1 - \tfrac{1}{p_1}) \cdot ... \cdot (1 - \tfrac{1}{p_m}).$$

**Definizione 1.7.** Siano $R$ e $S$ anelli. Un'applicazione $f : R \to S$ si dice omomorfismo se

(i) $f(a + b) = f(a) + f(b)$ per $a, b \in R$

(ii) $f(a \cdot b) = f(a)f(b)$ per $a, b \in R$

(iii) $f(1_R) = 1_S$.

**Definizione 1.8.** Un ideale $I$ di un anello $R$ è detto massimale se è un elemento massimale dell'insieme ordinato formato dagli ideali propri di $R$ rispetto all'inclusione "$\subseteq$". In altre parole $I$ è massimale se e solo se per ogni ideale $A$ di $R$ con $I \subset A \subset R$ si ha $I = A$ oppure $A = R$.

**Oss.** Se $R$ è commutativo, $I$ è massimale se e solo se $R/I$ è un campo.

**Definizione 1.9.** Un elemento non invertibile $p \in R$ si dice irriducibile se possiede soltanto divisori banali, cioè se $p = xy$, allora $x \in R^*$ oppure $y \in R^*$.

## Polinomi

**Teorema 1.1.** *Sia $f \in K[x]$ un polinomio di grado $n \geq 0$. Allora $f$ possiede al più $n$ zeri su $K$.*

**Proposizione 1.1.**

1. *Ogni polinomio $f = a_0 + a_1 x \in K[x]$ di grado 1 è irriducibile con un unico zero $\alpha = -a_1^{-1} a_0$.*
2. *Se $f \in K[x]$ è irriducibile di grado $n > 1$, allora non possiede zeri.*
3. *Se $f \in K[x]$ ha grado $n \in \{2, 3\}$, $f$ è irriducibile se e solo se non ammette zeri.*

**Definizione 1.10.** Per ogni $0 \neq f \in \mathbb{Q}[x]$ esiste un $\alpha \in \mathbb{Q}$ tale che $\alpha f \in \mathbb{Z}[x]$ con coefficienti coprimi. Un polinomio $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ per il quale $a_0, ..., a_n$ sono coprimi si dice primitivo.

**Teorema 1.2** (Criterio di Eisenstein)**.** *Sia $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ un polinomio primitivo di grado $n > 0$. Se esiste un numero primo $p$ tale che*

1. *$p$ non divide $a_n$*
2. *$p$ divide $a_0, ..., a_{n-1}$*
3. *$p^2$ non divide $a_0$.*

*allora $f$ è irriducibile.*

**Teorema 1.3** (Criterio di sostituzione)**.** *Sia $K$ un campo e sia $f = \sum_{i=0}^{n} a_i x^i \in K[x]$. Sostituendo $x$ con $a + bx$, dove $a, b \in K$ e $b \neq 0$, otteniamo il polinomio*

$$\tilde{f} = \sum_{i=0}^{n} a_i (a + bx)^i \in K[x].$$

*$f$ è irriducibile se e solo se lo è $\tilde{f}$.*

**Definizione 1.11.** Se $K, F$ sono campi e $K \subset F$ è un sottocampo, diciamo che F è un'estensione di $K$. In tal caso $F$ è uno spazio vettoriale su $K$ tramite la moltiplicazione per scalari

$$K \times F \to F, \qquad (\alpha, x) \mapsto \alpha x.$$

La dimensione di $F$ su $K$ si dice grado dell'estensione e si indica con

$$[F : K] = dim_K F.$$

L'estensione $K \subset F$ è finita se $[F : K] < \infty$.
Un elemento $\alpha \in F$ si dice algebrico se esiste $f \in K[x] conf \neq 0$ e $f(\alpha) = 0$. Altrimenti, $\alpha$ si dice trascendente su $K$.

**Teorema 1.4** (Teorema di Lindemann)**.** *$\pi$ è trascendente su $\mathbb{Q}$.*

**Lemma 1.1** (Lemma del Grado)**.** *Sia $K \subset F$ un'estensione finita e sia $L$ un campo intermedio (cioè $K \subset L$ e $L \subset F$ sono estensioni di campi). Allora*

$$[F : K] = [F : L][L : K].$$

# 2 Costruzioni con riga e compasso

La costruzione con riga e compasso nella geometria euclidea consiste nel tracciare rette e archi attraverso l'utilizzo di una riga e di un compasso non graduati. Ciò significa che non è possibile sfruttare le proprietà di misurazione della riga, né tanto meno mantenere l'apertura del compasso per disegnare più archi. Un punto può essere costruito con riga e compasso secondo la seguente definizione:

**Definizione 2.1.** Sia $M \subset \mathbb{C}$. Denotiamo con $E(M)$ l'insieme di tutti i punti $\alpha \in \mathbb{C}$ che si ottengono da $M$ mediante una delle seguenti operazioni:

- R: Dati due punti, è possibile tracciare una retta passante per essi
- C: Dati due punti, è possibile disegnare una circonferenza centrata in uno e passante per l'altro
- RR: L'intersezione di due rette dà origine a un nuovo punto
- CC: L'intersezione di due circonferenze dà origine a un nuovo punto
- RC: L'intersezione di una retta con una circonferenza dà origine a un nuovo punto

Diremo che $a \in \mathbb{C}$ è costruibile con riga e compasso da $M$ se $a$ è ottenuto da $M$ attraverso un numero finito di costruzioni elementari, cioè esistono $a_1, ..., a_n \in \mathbb{C}$ tali che $a_1 \in E(M)$, $a_2 \in E(M \cup \{a_1\})$, ... ,$a_n \in E(M \cup \{a_1, ..., a_{n-1}\})$ e $a_n = a$.
Diciamo che $a \in \mathbb{C}$ è costruibile se è costruibile con riga e compasso da $M = \{0, 1\}$.

A partire da queste operazioni elementari, si definiscono costruzioni più complesse. Tutti i problemi di costruzione con riga e compasso possono essere riformulati in termini algebrici conducendo alla risoluzione di una equazione. Le operazioni grafiche consentite da riga e compasso, sempre in termini algebrici, si ricollegano alle quattro operazioni e all'estrazione della radice quadrata. Di seguito, sono riportati alcuni esempi esplicativi.

## 2.1 Esempio

*Costruzione di un esagono.*

Per costruire un esagono inscritto in una circonferenza, partiamo da due punti $A$ e $B$ distanti 1 e puntando il compasso su $A$ con apertura $\overline{AB}$, disegniamo la circonferenza $c_1$ passante per $B$. Allo stesso modo, puntando il compasso su $B$ con apertura $\overline{AB}$, disegniamo la circonferenza $c_2$ passante per $A$.

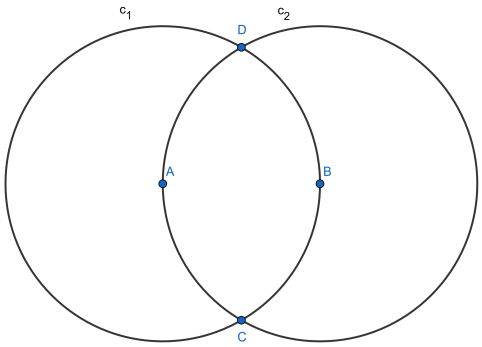


Figura 1: Esagono 1

Dopodiché, usando $B$ e i due punti di intersezione $C$ e $D$, creiamo i nuovi vertici: centrando il compasso su $C$, si fa passare un arco per il punto $A$ e l'intersezione tra l'arco e $c_1$ crea il nuovo punto $E$. Allo stesso modo partendo da $E$ si crea $F$ e partendo da $F$ si crea $G$, come in Figura 2.

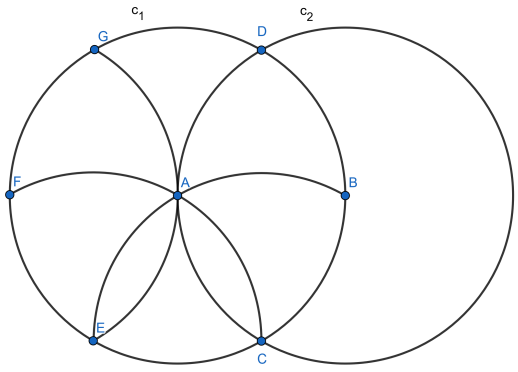


Figura 2: Esagono 2

Adesso, non resta che tracciare le rette che generano i segmenti $\overline{BC}$, $\overline{CE}$, $\overline{EF}$, $\overline{FG}$, $\overline{GD}$ e $\overline{DB}$, ottenendo un esagono.

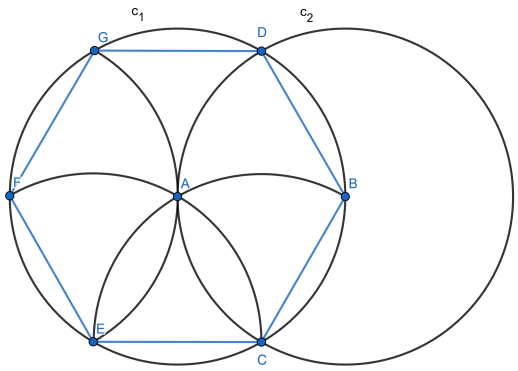


Figura 3: Esagono 4

Per mostrare che queste operazioni portano alla costruzione di un esagono regolare, basta notare che se tracciassimo sei raggi della circonferenza $c_1$ $\overline{AB}, \overline{AC}, \overline{AD}, \overline{AE}, \overline{AF}$ ed $\overline{AG}$, l'esagono risulterebbe formato da 6 triangoli equilateri di lato 1. Ciò ci permette di affermare la regolarità dell'esagono.

Adesso, mostriamo come questo esempio può essere trasformato nella risoluzione di un'equazione. Se consideriamo la circonferenza come il cerchio unitario nel piano complesso, i sei vertici dell'esagono saranno i sei numeri complessi che soddisfano l'equazione:

$$z^6 = 1.$$

Questa equazione ci consente di trovare le radici seste dell'unità, che tratteremo anche nelle sezioni successive. Poste sul piano complesso, queste radici formano un esagono regolare inscritto nel cerchio unitario.

L'equazione $z^6 = 1$ ha sei soluzioni complesse, che possono essere espresse nella forma

$$z_k = e^{\frac{2\pi k}{6} i} = \cos\left(\frac{2\pi k}{6}\right) + i \sin\left(\frac{2\pi k}{6}\right), \quad \text{per } k = 0, 1, 2, 3, 4, 5.$$

Le radici $z_k$ che rappresentano le coordinate dei vertici nel piano complesso corrispondono ai punti

$$z_0 = 1, \quad z_1 = e^{i\frac{\pi}{3}}, \quad z_2 = e^{i\frac{2\pi}{3}}, \quad z_3 = -1, \quad z_4 = e^{i\frac{4\pi}{3}}, \quad z_5 = e^{i\frac{5\pi}{3}}.$$

## 2.2 Esempio

*Costruzione di un quadrato.*

Per costruire un quadrato inscritto in una circonferenza, partiamo sempre da due punti $A$ e $B$ distanti 1 e tracciamo una circonferenza $c_1$ centrata in $A$ passante per $B$ e una circonferenza $c_2$ centrata in $B$ passante per $A$. Le intersezioni delle circonferenze creeranno i punti $C$ e $D$.

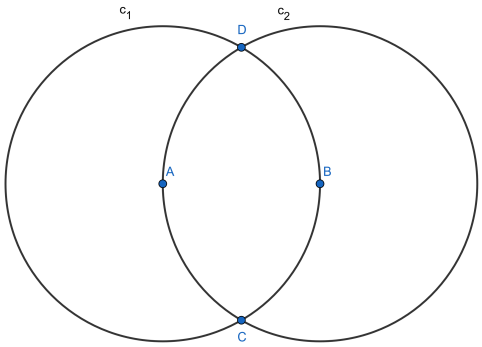


Figura 4: Quadrato 1

Successivamente, tracciamo la retta $p$, passante per $A$ e $B$, e la retta $q$ passante per $C$ e $D$. Dalle intersezioni di queste due rette, nasce il punto $E$ sulla quale centriamo il compasso per disegnare una circonferenza di raggio $\overline{AE}$. Le intersezioni con la retta $q$ generano i punti $F$ e $G$, come mostrato in Figura 5.

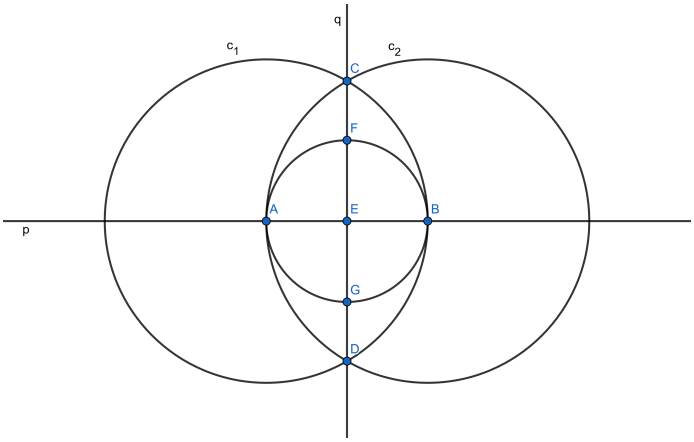


Figura 5: Quadrato 2

Facciamo passare la retta $r$ attraverso $A$ ed $F$ e la retta $s$ attraverso $A$ e $G$. Dalle intersezioni di queste rette con $c_1$ troviamo i nuovi punti $H, I, J$ e $K$, che saranno i vertici del nostro quadrato.

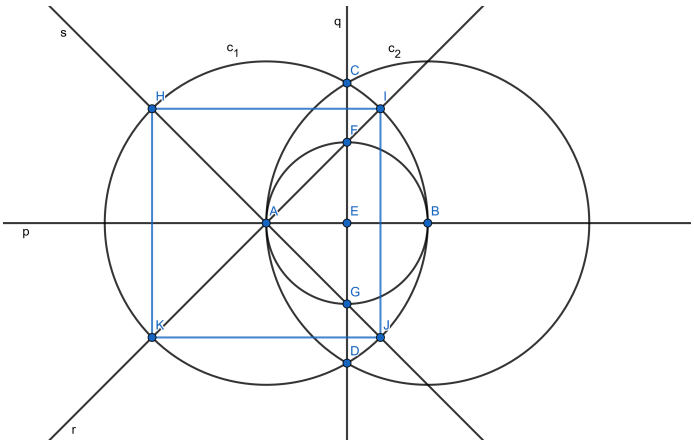


Figura 6: Quadrato 3

Mostriamo ora di aver creato un quadrato. Innanzitutto osserviamo che le rette $p$ e $q$ sono perpendicolari per costruzione e che i punti $A$ sulla retta $p$ e $F, G$ sulla retta $q$ sono equidistanti dal punto $E$. Gli angoli $\measuredangle EAF$ e $\measuredangle EFA$ sono dunque uguali e insieme formano un angolo di 90°. Allo stesso modo, gli angoli $\measuredangle GAE$ e $\measuredangle EGA$ sono uguali e insieme formano un angolo di 90°. Di conseguenza, l'angolo $\measuredangle GAF$ è un angolo di 90° e le rette $r$ e $s$ sono ortogonali. Osserviamo ora che i vertici del quadrato sono posizionati sulla circonferenza $c_1$. Essendo $r$ e $s$ ortogonali, i vertici sono fra loro equidistanti e ne deriva che i lati sono tutti uguali. Ciò ci permette di concludere che il poligono appena costruito è un quadrato.

L'equazione associata a questo esempio, sempre considerando la circonferenza come il cerchio unitario nel piano complesso, sarà

$$z^4 = 1.$$

Questa equazione ci consente di trovare le radici quarte dell'unità che, poste sul piano complesso, formano un quadrato inscritto nel cerchio unitario.

L'equazione $z^4 = 1$ ha sei soluzioni complesse, che possono essere espresse nella forma

$$z_k = e^{\frac{2\pi k}{4} i} = \cos\left(\frac{2\pi k}{4}\right) + i \sin\left(\frac{2\pi k}{4}\right), \quad \text{per } k = 0, 1, 2, 3.$$

Le radici $z_k$ che rappresentano le coordinate dei vertici nel piano complesso corrispondono ai punti

$$z_0 = 1, \quad z_1 = i, \quad z_2 = -1, \quad z_3 = -i.$$

Inoltre, dimostriamo il seguente Lemma:

**Lemma 2.1.** *I numeri costruibili formano un campo intermedio* $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{C}$.

*Dimostrazione.* Prima di tutto, dimostriamo che, data la retta $r$ passante per due punti $A, B$, possiamo costruire la retta $s$ parallela a $r$ passante per $C$ e la retta $t$ ortogonale a $r$ passante per $C$. Tracciamo due circonferenze: $c_1$ centrata in $A$ passante per $C$ e la circonferenza $c_2$ centrata in $B$ passante per $C$. La retta $t$ passerà per le intersezioni $C$ e $D$ delle circonferenze. Ora, tracciamo una circonferenza $c_3$ centrata in $C$ passante per $A$ e dal punto di intersezione $E$ tra $c_1$ e $r$ tracciamo una circonferenza $c_4$ passante per $A$. L'intersezione tra $c_3$ e $c_4$ ci darà l'altro punto $F$ per cui far passare la retta $s$.

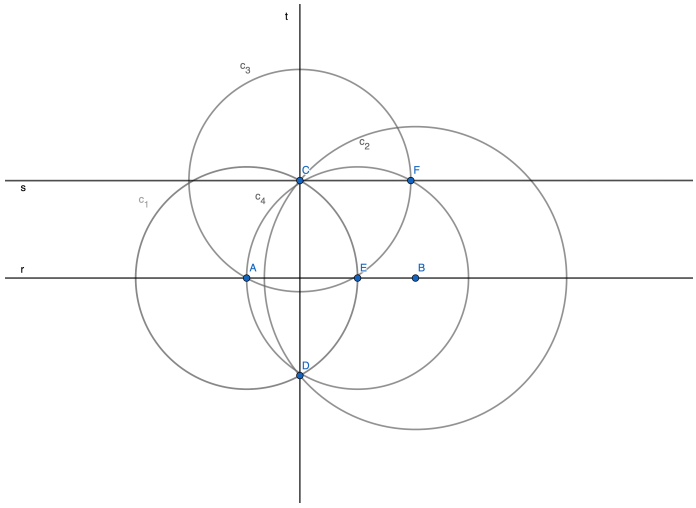


Figura 7

Ora, dimostriamo i seguenti punti:

1. Siano $a, b \in \mathbb{K}$. Allora anche $a + b, -a \in \mathbb{K}$, e $|a| \in \mathbb{K} \cap \mathbb{R}$. Infatti,
   - $-a$ è costruibile, poiché ottenuto tracciando la retta $r$ passante per $a$ e 0
   - $a + b$ è costruibile per la regola del parallelogramma: basta tracciare la retta $u$ parallela a $s$ passante per $a$, la rette $s$ passante per 0 e $b$ e la retta $t$ parallela a $r$ passante per $b$.
   - $|a|$ è costruibile poiché è l'intersezione tra l'asse reale e la circonferenza passante per $a$.

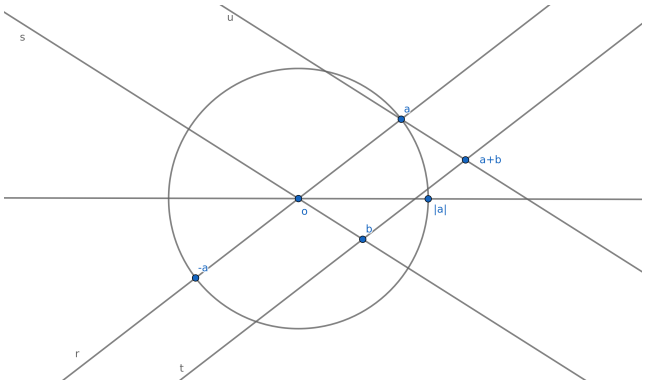


Figura 8

2. Per $|a| \cdot |b| \in \mathbb{K}$, se $b \neq 0$, anche $\frac{1}{b} \in \mathbb{K}$. Partiamo dai punti $0, 1, |a|, |b|$. Costruiamo la retta $\beta$ che taglia in due la circonferenza e due circonferenze $c_1$ e $c_2$ centrate in 0 e passanti rispettivamente per 1 e $|a|$. Le intersezioni con $\beta$ danno origine ai punti $p$ e $q$. Tracciamo una retta $r$ passante per $p$ e $|b|$ e una retta $s$ parallela a $r$ passante per $q$. L'intersezione di $r$ con l'asse reale dà origine al punto $c$. Per il Teorema di Talete, $\frac{|q|}{|p|} = \frac{|c|}{|b|}$ e poiché $|p| = 1, |q| = |a|$, segue che $c = |a| \cdot |b|$. Costruiamo la retta $t$ parallela a $s$ e passante per 1. Chiamiamo $d$ l'intersezione tra $\beta$ e $t$, per il quale facciamo passare la circonferenza $c_3$ centrata in 0. Per il Teorema di Talete, $\frac{|q|}{|p|} = \frac{|1|}{|b|}$, perciò $|d| = \frac{1}{|b|}$.

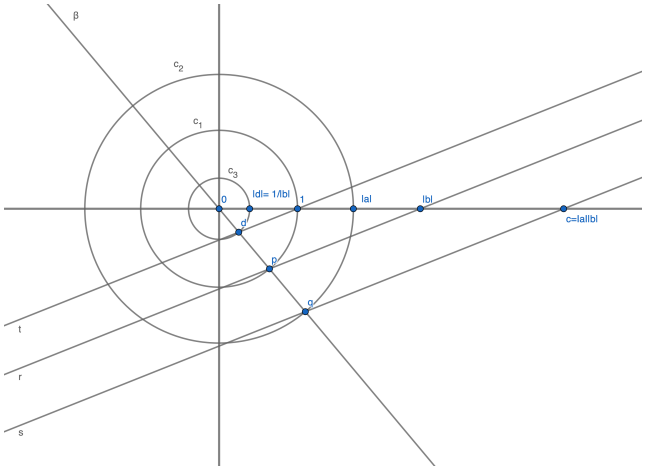


Figura 9

3. Per $ab \in \mathbb{K}$, $\frac{1}{b} \in \mathbb{K}$ se $b \neq 0$. Infatti, siano $a = |a|(\cos\alpha + i\sin\alpha)$ e $b = |b|(\cos\beta + i\sin\beta)$. Allora, applicando i punti precedenti 1. e 2., otteniamo

che $ab = |a||b|(\cos(\alpha+\beta) + i\sin(\alpha+\beta))$ e $\frac{1}{b} = \frac{1}{|b|}(\cos(-\beta + i\sin(-\beta))$, come mostrato in Figura 10.

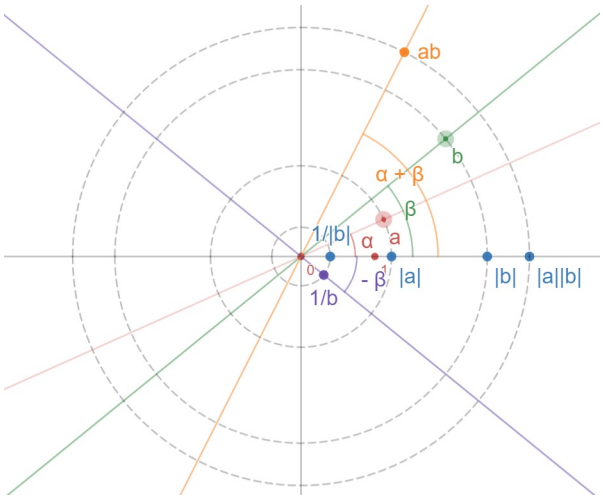


Figura 10

4. Costruzione di $\sqrt{a}$ con $a = |a|(\cos\alpha + i\sin\alpha)$: costruiamo $\sqrt{|a|}$: partiamo costruendo $-|a|$ come visto in 1. e troviamo il punto medio $p$ tra $-|a|$ e 1 attraverso l'intersezione di due circonferenze $c_1$ centrata in $-|a|$ passante per 1 e $c_2$ centrata in 1 passante per $-|a|$. Tracciamo una circonferenza centrata in $p$ passante per 1 e la sua intersezione con l'asse immaginario dà origine al punto $q$. Il triangolo $-|a|q1$ è rettangolo con $h = |q|$ e quindi $|a|1 = h^2 = |q|^2$. Quindi $|q| = \sqrt{|a|}$.

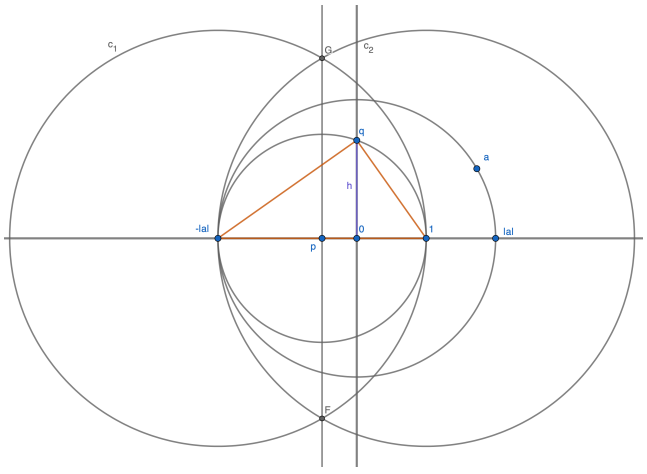


Figura 11

# 3 Estensioni di Campi

Come visto finora, tutte le costruzioni devono essere realizzate tramite un numero finito di passi e la creazione di nuovi punti è possibile attraverso l'intersezione di due rette, due circonferenze o di una retta e una circonferenza. Data una costruzione con riga e compasso di un poligono a $n$ lati, possiamo verificare che sia regolare, come fatto negli esempi precedenti. Per determinare a priori la costruibilità o meno di un poligono a $n$ lati è necessario avere una classificazione algebrica dei campi di numeri costruibili. A tal fine, enunciamo i seguenti teoremi:

**Teorema 3.1.** *Sia $r \in \mathbb{C}$ un numero costruibile. Allora $\exists\ k \in \mathbb{N}_0$ tale che $[\mathbb{Q}(r) : \mathbb{Q}] = 2^k$.*

*Dimostrazione.* Innanzitutto, mostriamo che una retta e una circonferenza, se costruiti partendo da punti razionali, hanno a loro volta coefficienti razionali:

Siano due punti $(x_1, y_1), (x_2, y_2) \in \mathbb{Q}$. La retta passante per questi punti avrà equazione

$$\frac{(x - x_1)}{(x_2 - x_1)} = \frac{(y - y_1)}{(y_2 - y_1)}.$$

Riarrangiando l'equazione, si ottiene

$$(y_2 - y_1)x + (x_2 - x_1)y - (y_2 - y_1)x_1 - (x_2 - x_1)y_1 = 0,$$

da cui si deduce che la retta ha coefficienti in $\mathbb{Q}$.

Per la circonferenza, senza perdere di generalità, assumiamo sia centrata in $(x_1, y_1)$ e passante per $(x_2, y_2)$, entrambi in $\mathbb{Q}$. L'equazione della stessa è data da

$$(x - x_1)^2 + (y - y_1)^2 = (x2 - x1)^2 + (y2 - y1)^2.$$

Riarrangiando l'equazione, si ha

$$x^2 + y^2 - 2x_1x - 2y_1y + x_1^2 + y_1^2 - (x2 - x1)^2 - (y2 - y1)^2 = 0,$$

da cui si deduce che la circonferenza ha coefficienti in $\mathbb{Q}$.

Supponiamo ora che $r \in \mathbb{C}$ sia costruibile. Ciò implica che possiamo costruire $r$ attraverso un numero finito di passi che comprendono intersezioni di rette e circonferenze. Separiamo adesso i casi possibili:

- Intersezione di due rette: supponiamo di avere $a, b, c, d, e$ ed $f \in \mathbb{Q}$.

  Consideriamo due rette $l$ e $m$, dove $l$ è data da

  $$ax + by + c = 0$$

  e $m$ è data da

$$dx + ey + f = 0.$$

Dalla loro intersezione, otteniamo il punto $r$

$$\left(\frac{ce - bf}{bd - ae}\frac{af - cd}{bd - ae}\right)$$

che è un altro punto nel campo $\mathbb{Q}$, e quindi $[\mathbb{Q}(r) : \mathbb{Q}] = 1$;

- Intersezione di due circonferenze: supponiamo di avere $a, b, c, d, e$ ed $f \in \mathbb{Q}$. Consideriamo le circonferenze $c_1$ e $c_2$, dove $c_1$ è

$$x^2 + y^2 + ax + by + c = 0$$

e $c_2$ è

$$x^2 + y^2 + dx + ey + f = 0.$$

Imponendo $c_1 = c_2$, otteniamo la retta

$$(a - d)x + (b - e)y + (c - f) = 0,$$

dove $(a - d), (b - e)$ e $(c - f)$ sono tutti punti di $\mathbb{Q}$.
Si ha, dunque, un'altra estensione di grado $[\mathbb{Q}(r) : \mathbb{Q}] = 1$;

- Intersezione di una retta e una circonferenza: supponiamo di avere $a, b, c, d, e$ ed $f \in \mathbb{Q}$.
Consideriamo la retta $l$ di equazione

$$ax + by + c = 0$$

e la circonferenza $c$ di equazione

$$x^2 + y^2 + dx + ey + f = 0.$$

Se imponiamo l'uguaglianza e risolviamo per $x$, otteniamo

$$(b^2 + a^2)x^2 + (2ac + db^2 - aeb)x + (c^2 - ceb + fb^2) = 0.$$

Siano ora $\alpha = (b^2 + a^2)$, $\beta = (2ac + db^2 - aeb)$ e $\gamma = (c^2 - ceb + fb^2)$. La soluzione sarà $x = \dfrac{-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}$, dove $\beta^2 - 4\alpha\gamma$ è costruibile. Dunque, i punti di intersezione tra $l$ e $c$ sono nell'estensione $\mathbb{Q}\left(\sqrt{\beta^2 - 4\alpha\gamma}\right)$, che ha grado $\left[\mathbb{Q}\left(\sqrt{\beta^2 - 4\alpha\gamma}\right) : \mathbb{Q}\right] = 2$.

Dato che ogni passo della costruzione ha grado 1 o 2 e che il numero di mosse deve essere finito, moltiplicando il grado di ogni passo otteniamo un'estensione di grado $2^k$ per un $k \in \mathbb{N}_0$, ossia $[\mathbb{Q}(r) : \mathbb{Q}] = 2^k$ per un $k \in \mathbb{N}_0$. □

**Corollario 3.1.** *Se un poligono a n lati è costruibile, allora* $\exists k \in \mathbb{N}_0$ *tale che* $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right] = 2^k$.

*Dimostrazione.* Partendo da un poligono regolare a $n$ lati, abbiamo che la circonferenza in cui è inscritto è divisa in $n$ angoli uguali di ampiezza $\frac{2\pi}{n}$. Sia $A$ un vertice di coordinate $(\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n}))$, costruibile per ipotesi. Allo stesso modo, anche gli altri vertici sono costruibili, in particolare lo è $A' = (\cos\frac{(n-1)2\pi}{n}), \sin(\frac{(n-1)2\pi}{n})) = (\cos(\frac{2\pi}{n}), \sin(-\frac{2\pi}{n}))$. Tracciamo ora una retta passante per $A$ e $A'$. Il segmento $\overline{AA'}$ avrà lunghezza $2\sin(\frac{2\pi}{n})$. Usando l'identità

$$\cos^2(\theta) + \sin^2(\theta) = 1,$$

otteniamo che $\cos(\frac{2\pi}{n}) = \sqrt{1 - \sin^2(\theta)}$, concludendo che $\cos(\frac{2\pi}{n})$ è costruibile e per Teorema 3.1 $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right] = 2^k$ per un $k \in \mathbb{N}_0$. □

# 4 Teoria di Galois

Dopo aver stabilito quando un poligono a $n$ lati è costruibile grazie alle estensioni di campi, è necessario menzionare alcune nozioni della Teoria di Galois. Infatti, per dimostrare il Criterio di Costruibilità 5.1, utilizzeremo alcune delle seguenti definizioni e teoremi al fine di caratterizzare questi poligoni e avere un criterio che renda possibile affermare immediatamente la loro costruibilità o meno.

**Definizione 4.1.** Sia $K_n$ il campo di riducibilità completa del polinomio $f = x^n - 1$ su $K$. Gli zeri di $f$ sono dette radici $n$-esime dell'unità e formano un sottogruppo ciclico $(G_n, \cdot)$ di $(K_n \setminus \{0\}, \cdot)$ di ordine $n$.

**Definizione 4.2.** Le radici $n$-esime dell'unità che generano il gruppo ciclico $G_n$ si dicono primitive.

**Definizione 4.3.** Fissato $n$, siano $\omega_1, \omega_2, ..., \omega_{\varphi(n)}$ le radici $n$-esime primitive dell'unità. Allora $\Phi_n(x) = (x - \omega_1)(x - \omega_2)...(x - \omega_{\varphi(n)})$ è detto $n$-esimo polinomio ciclotomico su $\mathbb{Q}$. $\Phi_n$ ha grado $\varphi(n)$, dove $\varphi(n)$ è la funzione phi di Eulero.

**Lemma 4.1.** *Se $n \in \mathbb{N}$, $\omega = e^{\frac{2\pi i}{n}}$ radice dell'unità primitiva, allora $\mathbb{Q}(\cos(\frac{2\pi}{n})) \subseteq \mathbb{Q}(\omega)$.*

*Dimostrazione.* Innanzitutto, sappiamo che $\omega = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$.

Sia $\alpha = \cos\left(\frac{2\pi}{n}\right)$ e $\overline{\omega} = \cos\left(\frac{2\pi}{n}\right) - i\sin\left(\frac{2\pi}{n}\right)$. Osserviamo che $\omega$ è una radice di

$$\begin{aligned}(x - \omega)(x - \overline{\omega}) &= x^2 - x(\omega + \overline{\omega}) + (\omega\overline{\omega}) \\ &= x^2 - 2x\cos\left(\tfrac{2\pi}{n}\right) + 1 = x^2 + 2\alpha x + 1.\end{aligned}$$

Osserviamo anche che

$$\omega\overline{\omega} = \left(\cos\left(\tfrac{2\pi}{n}\right)\right)^2 + \left(\sin\left(\tfrac{2\pi}{n}\right)\right)^2 = 1$$

e quindi

$$\alpha = \tfrac{1}{2}(\omega + \overline{\omega}) = \tfrac{1}{2}(\omega + \omega^{-1}) \in \mathbb{Q}.$$

Concludiamo che $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\omega)$. Il polinomio minimo di $\omega$ su $\mathbb{Q}(\alpha)$ è $x^2 - 2\alpha x + 1$ ed è irriducibile poiché lo è in $\mathbb{R}$ e $\mathbb{Q} \subset \mathbb{R}$. □

**Definizione 4.4.** Sia $K \subset F$ un'estensione di campi. Il gruppo di Galois $\mathrm{Gal}(F/K)$ di $F$ su $K$ è l'insieme degli automorfismi di $F$ che associano ogni elemento di $K$ a se stesso, ossia

$\mathrm{Gal}(F/K) = \{\phi : F \to F \mid \phi(x) = x, \forall x \in K\}$.

**Definizione 4.5.** Dato un polinomio $f \in K[x]$, sia $E$ è un campo di riducibilità completa di $f$ su $K$. Allora, $\mathrm{Gal}(f/K) := \mathrm{Gal}(E/K)$ si dice gruppo di Galois di $f$ su $K$.

**Definizione 4.6.** Sia $F$ un campo.

1. Gli automorfismi $\varphi : F \to F$ di $F$ formano un gruppo $(\operatorname{Aut} F, \circ)$ rispetto alla composizione $\circ$.

2. Sia $G \leq \operatorname{Aut} F$ . Allora l'insieme

$$\operatorname{Fix}_F(G) = \{a \in F \,|\, \varphi(a) = a \text{ per } \varphi \in G\}$$

è un sottocampo di $F$ , detto campo fisso di $G$ in $F$.

**Teorema 4.1.** *Sia $F$ un campo e sia $G \leq \operatorname{Aut} F$ un sottogruppo finito. Allora* $\operatorname{Gal}(F/\operatorname{Fix}_F(G)) = G$.

**Teorema 4.2.** *Per $K \subset F$ estensione di campi, sono equivalenti i seguenti enunciati:*

1. *Esiste un sottogruppo finito $G \leq \operatorname{Aut} F$ tale che $K = \operatorname{Fix}_F(G)$*
2. *$K \subset F$ è un'estensione finita tale che $K = \operatorname{Fix}_F(\operatorname{Gal}(F/K))$*
3. *$K \subset F$ è un'estensione finita tale che $[F : K] = |\operatorname{Gal}(F/K)|$*

*Se $K \subset F$ soddisfa (1),(2) e (3), diciamo che $K \subset F$ è un'estensione di Galois.*

**Lemma 4.2** (Lemma di Dedekind)**.** *Siano $K$, $F$ due campi e siano $\varphi_1, \ldots, \varphi_n : F \to K$ omomorfismi distinti. Allora*

$$L = \{a \in F \mid \varphi_1(a) = \varphi_2(a) = \ldots = \varphi_n(a)\}$$

*è un sottocampo di $F$ con $[F : L] \geq n$.*

**Teorema 4.3** (Teorema fondamentale della teoria di Galois)**.** *Siano $K \subset F$ un'estensione di Galois con $G = \operatorname{Gal}(F/K)$, $\mathcal{L}$ l'insieme dei campi intermedi $K \subset L \subset F$, $\mathcal{H}$ l'insieme dei sottogruppi di $G$. Le applicazioni*

$$\operatorname{Gal} : \mathcal{L} \longrightarrow \mathcal{H},\ L \longmapsto \operatorname{Gal}(F/L)$$
$$\operatorname{Fix} : \mathcal{H} \longrightarrow \mathcal{L},\ H \longmapsto \operatorname{Fix}_F(H)$$

*sono corrispondenze biunivoche mutualmente inverse che invertono l'ordine dato dall'inclusione " $\subseteq$ ".*

*Inoltre, per ogni campo intermedio $K \subset L \subset F$, si ha:*

1. *$L \subset F$ è un'estensione di Galois;*
2. *Se $H = \operatorname{Gal}(F/L)$, allora $[L : K] = [G : H]$;*
3. *Sono equivalenti i seguenti enunciati:*
   a. *$K \subset L$ è un'estensione di Galois;*
   b. *$H \lhd G$;*

*c.* $\varphi(L) \subset L$ *per ogni* $\varphi \in G$.

*Se valgono (a) (b) (c), allora* $\mathrm{Gal}(L/K) \cong G/H$.

*Dimostrazione.* Siano $n := [F : K] = |G|$, $K = \mathrm{Fix}_F(G)$.
Sappiamo per 4.1 che

$$\mathcal{H} \xrightarrow{\mathrm{Fix}} \mathcal{L} \xrightarrow{\mathrm{Gal}} \mathcal{H}, H \longmapsto \mathrm{Fix}_F(H) \longmapsto \mathrm{Gal}(F/\mathrm{Fix}_F(H)) = H$$

coincide con l'identità su $\mathcal{H}$.
Consideriamo ora un campo intermedio $K \subset L \subset F$ e $H := \mathrm{Gal}(F/L)$.

$$K \subset L \subset L' := \mathrm{Fix}_F(H) \subset F.$$

Vogliamo mostrare $L = L'$. Basta verificare $[L' : K] = [L : K]$, ovvero "$\leq$".
Procediamo per step e facciamo una serie di osservazioni che ci serviranno per la nostra dimostrazione:

(*i*) $[L' : K] = \dfrac{[F : K]}{[F : L']} = \dfrac{|G|}{|H|} = [G : H] =: r$

(*ii*) Se $g, \tilde{g} \in G$, allora

$$gH = \tilde{g}H \Leftrightarrow g^{-1}\tilde{g} \in H \Leftrightarrow g^{-1}\tilde{g}(a) = a \text{ per ogni } a \in L \Leftrightarrow \tilde{g}(a) = g(a) \text{ per ogni } a \in L$$

(*iii*) Se $G/H = \{g_1H, \ldots, g_rH\}$ con $g_1 = \mathrm{id}_F$, $g_2, \ldots, g_r \in G$, allora
$\varphi_i := g_i|_L : L \to F$, per $1 \leq i \leq r$ sono $r$ omomorfismi distinti per (*ii*),

(*iv*) $K = \{a \in L \mid \varphi_1(a) = \ldots = \varphi_r(a)\} \subset L$. Ricordiamo che $\varphi_i(a) = a$ per (*ii*) e (*iii*)

"$\subseteq$" : triviale

"$\supseteq$" : Sia $a \in L$ con $\varphi_1(a) = \ldots = \varphi_r(a)$ e sia $g \in G$. Allora $gH = g_iH$ per un $1 \leq i \leq r$ e per (*ii*) abbiamo $g(a) = g_i(a) = \varphi_i(a) = \varphi_1(a) = a$.
Dunque $a \in \mathrm{Fix}_F(G) = K$

(*v*) Concludiamo da 4.2 che $[L : K] \geq r \underset{(i)}{=} [L' : K]$

Perciò $L = L' = \mathrm{Fix}_F(H)$ e abbiamo verificato (1) e (2).
Inoltre

$$\mathcal{L} \xrightarrow{\mathrm{Gal}} \mathcal{H} \xrightarrow{\mathrm{Fix}} \mathcal{L}$$

$$L \longmapsto H = \mathrm{Gal}(F/L) \longmapsto \mathrm{Fix}_F(H) = L$$

è l'identità su $\mathcal{L}$.
Resta da dimostrare (3).

$(b) \Leftrightarrow (c)$: Sia $\varphi \in G$. Abbiamo un campo intermedio $K \subset \varphi(L) \subset F$, estensione di Galois per (1), con

$$\begin{aligned}\operatorname{Gal}(F/\varphi(L)) &= \{\psi \in \operatorname{Aut} F \mid \psi(\varphi(a)) = \varphi(a) \text{ per ogni } a \in L\} \\ &= \{\psi \in \operatorname{Aut} F \mid \varphi^{-1}\psi\varphi(a) = a \text{ per ogni } a \in L\} \\ &= \{\psi \in \operatorname{Aut} F \mid \varphi^{-1}\psi\varphi \in \operatorname{Gal}(F/L) = H\} = \varphi H \varphi^{-1}\end{aligned}$$

Quindi

$$(*) \qquad [F : \varphi(L)] = |\operatorname{Gal}(F/\varphi(L))| = |H| = [F : L].$$

Inoltre,

$$\begin{aligned}H \lhd G &\Leftrightarrow \varphi H \varphi^{-1} = H \text{ per ogni } \varphi \in G \\ &\Leftrightarrow \operatorname{Gal}(F/\varphi(L)) = H = \operatorname{Gal}(F/L) \text{ per ogni } \varphi \in G \\ &\underset{\substack{\text{Gal} \\ \text{è iniettiva}}}{\Leftrightarrow} \quad \varphi(L) = L \Leftrightarrow \varphi(L) \subseteq L\end{aligned}$$

Infatti se $K \subset \varphi(L) \subset L \subset F$, allora $\varphi(L) = L$ per $(*)$ e il Lemma del Grado.

$(a) \Rightarrow (c)$: Equivalentemente, dimostriamo che $\neg(c) \Rightarrow \neg(a)$. Sia $r = [L : K] = \operatorname{Gal}(L/K)$ e siano $\psi_1, \ldots, \psi_r$ gli omomorfismi distinti di $\operatorname{Gal}(L/K)$. Essi inducono $r$ omomorfismi distinti $\varphi_i : L \to L \subset F$. Supponiamo "$\neg(c)$", cioè che esista $\varphi \in G$ tale che $\varphi(L) \not\subset L$. Allora $\varphi_1, \ldots, \varphi_r, \varphi|_L$ sono $r+1$ omomorfismi distinti con $K = \{a \in L \mid a = \varphi_1(a) = \ldots = \varphi_r(a) = \varphi|_L\} \subset L$

"$\subseteq$": triviale

"$\supseteq$": Sia $a \in L$ con $\varphi_1(a) = \ldots = \varphi_r(a) = \varphi(a)$. Allora $a \in \operatorname{Fix}_L(\operatorname{Gal}(L/K)) = K$.

Per 4.2 abbiamo $r = [L : K] \geq r + 1$, ossia "$\neg(a)$".

$(c) \Rightarrow (a)$: Ogni $\varphi \in G$ induce un automorfismo $\tilde{\varphi} = \varphi|_L \in \operatorname{Aut} L$ che appartiene a $\operatorname{Gal}(L/K)$. L'applicazione $\nu : G \to \operatorname{Gal}(L/K), \varphi \mapsto \tilde{\varphi}$ è un omomorfismo di gruppi:

$$\nu(\varphi \circ \psi) = (\varphi\psi)|_L = \varphi|_L \circ \psi|_L = \nu(\varphi) \circ \nu(\psi)$$

con nucleo $\{\varphi \in G \mid \varphi|_L = \mathrm{id}_L\} = \operatorname{Gal}(F/L) = H$.
Perciò $[G : H] = |\operatorname{Im} \nu| \leq |\operatorname{Gal}(L/K)|$.
Ma sappiamo che $|\operatorname{Gal}(L/K)|$ divide $[L : K] \underset{(2)}{=} [G : H]$.
Perciò $[G : H] = |\operatorname{Im} \nu| = |\operatorname{Gal}(L/K)| = [L : K]$.
Dunque $K \subset L$ è un'estensione di Galois e $\nu$ è suriettivo, perciò $G/H \cong \operatorname{Gal}(L/K)$.

□

# 5 Criterio di Costruibilità

Carl Friedrich Gauss è stato uno dei più importanti matematici della storia. Sin da piccolo, è sempre stato un grande prodigio nella matematica, tant'è che già dalle elementari le sue straordinarie doti intellettuali furono notate dai suoi professori dell'epoca. A soli diciannove anni, da autodidatta, dimostrò con successo un problema che afflisse le migliori menti matematiche dai tempi dei greci, ossia la costruibilità di un poligono a 17 lati. A ventiquattro, invece, dimostrò il seguente teorema, stabilendo la condizione sufficiente per la costruibilità di un poligono a $n$ lati:

**Teorema 5.1** (Criterio di Costruibilità)**.** *Un poligono a $n$ lati regolare è costruibile se e solo se $n = 2^k p_1 p_2 ... p_t$, dove $k \geq 0$ e ogni $p_i$ è un numero primo della forma $p_i = 2^{m_i} + 1$ per un $m_i \in \mathbb{N}_0$.*

*Dimostrazione.* ($\Rightarrow$) Supponiamo che un poligono a $n$ lati regolare sia costruibile. Ciò implica che, per il Corollario 3.1, $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right] = 2^k$. Per Lemma 4.1, $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) \subseteq \mathbb{Q}(\omega)$, con $\omega = e^{\frac{2\pi i}{n}}$, dove $\mathbb{Q}(\omega)$ è un'estensione di $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$ e $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$ è un'estensione di $\mathbb{Q}$. Dato che $\Phi_n(x)$ è il polinomio minimo di grado $\varphi(n)$ di $\omega$, $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$. Per la teoria dei campi abbiamo che

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right] \cdot \left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right].$$

Per il Teorema fondamentale della teoria di Galois 4.3,

$$\varphi(n) = \left|\mathrm{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right)\right| \cdot \left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right]$$

e quindi

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \frac{\varphi(n)}{|\,\mathrm{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right)|}.$$

Sappiamo anche che $\mathrm{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right) \leq \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$. Ora, sia $H = \mathrm{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right)$ e $G = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ così da avere $H \leq G$. Per la definizione 4.5 di gruppo di Galois, abbiamo che per ogni $\sigma \in H, \sigma(\omega) = \omega^k$ per un qualche $k$, e $\sigma\left(\cos\left(\frac{2\pi}{n}\right)\right) = \cos\left(\frac{2\pi}{n}\right)$. Ma $\omega = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$, quindiö

$$\begin{aligned}\sigma(\omega) &= \sigma\left(\cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)\right)\\ &= \sigma\left(\cos\left(\frac{2\pi}{n}\right)\right) + \sigma(i)\sigma\left(\sin\left(\frac{2\pi}{n}\right)\right).\end{aligned}$$

Si ha anche che $\sigma(\omega) = \omega^k = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$. Dunque, $\cos\left(\frac{2\pi}{n}\right) = \cos\left(\frac{2\pi k}{n}\right)$, che implica che o $k = 1$ o $k = n - 1$ e che $|H| = 2$. Quindi

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \frac{\varphi(n)}{|H|} = \frac{\varphi(n)}{2}.$$

Per supposizione, si ha che $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = 2^k$, e quindi $\varphi(n) = 2^{k-1}$, cioè $\varphi(n)$ deve essere una potenza di 2. Adesso, si supponga che $p_1^{n1}p_2^{n_2}...p_t^{n_t}$ sia la fattorizzazione in numeri primi di $n$ e, dato che la funzione phi di Eulero è moltiplicativa,

$$\begin{aligned} 2^k = \varphi(n) = \varphi(p_1^{n1})\varphi(p_2^{n_2})...\varphi(p_t^{n_t}) \\ = ((p_1-1)(p_1^{n_1-1}))((p_2-1)(p_2^{n_2-1}))...((p_t-1)(p_t^{n_t-1})). \end{aligned}$$

Allora si deve avere che per ogni $i = 1, ..., t$ o $p_i = 2$, oppure $p_i - 1 = 2^{m_i}$, cioè $p_i = 2^{m_i} + 1$ per un $m_i \in \mathbb{N}_0$.

($\Leftarrow$) Supponiamo che $n = 2^k p_1 p_2 ... p_t$ dove $k \geq 0$ e ogni $p_i$ è un numero primo della forma $p_i = 2^{m_i} + 1$ per un $m_i \in \mathbb{N}_0$.

$$\varphi(n) = [\mathbb{Q}(\omega) : \mathbb{Q}] = |\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})|.$$

Per il Teorema fondamentale della teoria di Galois 4.3, si ha che

$$\begin{aligned} \left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] &= \frac{|\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})|}{\left|\operatorname{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right)\right|}, \\ &= \frac{\varphi(n)}{\left|\operatorname{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right)\right|}. \end{aligned}$$

Da ($\Rightarrow$) sappiamo che

$$\left|\operatorname{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right)\right| = 2$$

e quindi

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \left|\operatorname{Gal}\left(\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right)\right| = \varphi(n)/2.$$

Dopodiché,

$$\begin{aligned} \varphi(n) = \varphi(2^k p_1 p_2 ... p_t) = \varphi(2^k)\varphi(p_1)\varphi(p_2)...\varphi(p_t) \\ = 2^{k-1}(p_1^{1-1}(p_1-1))...(p_t^{1-1}(p_t-1)) \end{aligned}$$

e quindi

$$\varphi(n)/2 = 2^{k-2}(p_1-1)...(p_t-1),$$

dove $p_i = 2^{m_i} + 1$. Ciò implica che $\varphi(n)/2 = 2^{k-2}(2^{m_1})(2^{m_2})...(2^{m_t}) = 2^k$ per un $k \in \mathbb{N}_0$. Dunque,

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = 2^k$$

per un $k \in \mathbb{N}_0$, cioè il poligono a $n$ lati è costruibile. $\square$

In alcuni testi, l'enunciato del teorema può essere trovato in forma leggermente diversa, ossia i numeri primi $p_i$ devono essere primi di Fermat, vale a dire della forma $p_i = 2^{2^m} + 1$. Questo non cambia il risultato del teorema poiché se un numero $p_i$ della forma $p_i = 2^m + 1$ è primo, allora è un primo di Fermat. Infatti, se $t$ è un intero dispari, il polinomio $x^t + 1$ può essere fattorizzato nel prodotto di due polinomi a coefficienti interi:

$$x^t + 1 = (x + 1)(x^{t-1} - x^{t-2} + ... - x + 1).$$

Supponiamo che $2^m + 1$ sia primo e sia $t$ un fattore dispari di $m$. Scrivendo $m = st$, abbiamo dal risultato precedente che

$$2^m + 1 = (2^s)^t + 1 = (2^s + 1) \text{ per un intero.}$$

Poiché $2^m + 1$ è primo, $2^s + 1$ può essere uguale o a 1 o a $2^m + 1$. Essendo il primo caso impossibile, deve necessariamente verificarsi che

$$2^s + 1 = 2^m + 1,$$

da cui segue che $s = m$, quindi $t = 1$.

Tutto ciò dimostra che, se $2m + 1$ è primo, allora $m$ non ha fattori dispari diversi 1. Gli unici valori di $m$ per cui ciò è vero sono le potenze di 2, ovvero $m = 2^k$, e quindi

$$2^m + 1 = 2^{2^k} + 1,$$

che sono esattamente i numeri primi di Fermat.

# 6 I tre problemi classici dell'antichità

Col passare degli anni, gli studi degli antichi greci portarono alla scoperta dei famosi problemi con riga e compasso, tre dei quali sono passati alla storia come "i problemi classici dell'antichità". Questi tre problemi, ossia la trisezione dell'angolo, la quadratura del cerchio e la duplicazione del cubo, non solo non furono risolti al tempo di Euclide, ma è stato dimostrato che la loro risoluzione è impossibile. Queste dimostrazioni sono relativamente recenti e sono frutto di grandi progressi nel campo dell'algebra, dovuti soprattutto al lavoro di Évariste Galois, che consentirono a Wanzel e Lindemann di realizzare queste dimostrazioni.

**Teorema 6.1** (Trisezione di un angolo)**.** *Un angolo $\theta$ non può essere diviso in tre angoli uguali.*

*Dimostrazione.* Sia $\theta = \dfrac{\pi}{3}$. Allora, se potessimo dividerlo in tre parti uguali, in questo caso otterremmo tre angoli di ampiezza $\dfrac{\pi}{9}$ e $\cos\left(\dfrac{\pi}{9}\right)$ sarebbe costruibile. Cerchiamo il polinomio minimo di $a = \cos\left(\dfrac{\pi}{9}\right)$ per mostrare che $a$ non è costruibile, che implicherebbe che non possiamo dividere in tre questo angolo. Utilizzando l'uguaglianza $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$ per $\theta = \dfrac{\pi}{9}$, otteniamo

$$\cos\left(\frac{3\pi}{9}\right) = 4\cos^3\left(\frac{\pi}{9}\right) - 3\cos\left(\frac{\pi}{9}\right).$$

Se poniamo $x = \cos\left(\dfrac{\pi}{9}\right)$, otteniamo

$$\cos\left(\frac{\pi}{3}\right) = 4x^3 - 3x$$

e dato che $\cos\left(\dfrac{\pi}{3}\right) = \dfrac{1}{2}$,

$$4x^3 - 3x - \frac{1}{2} = 0.$$

Dunque, $8x^3 - 6x - 1 = 0$ ha $\cos\left(\dfrac{\pi}{9}\right)$ come radice. Utilizzando il Criterio di sostituzione 1.3 con $x - 1$ al posto di $x$, osserviamo che

$$\begin{aligned} 8(x-1)^3 - 6(x-1) - 1 &= 8(x^3 - 3x^2 + 3x - 1) - 6(x-1) - 1 \\ &= 8x^3 - 24x^2 + 18x - 3 \end{aligned}$$

è un polinomio irriducibile per il Criterio di Eisenstein 1.2 per $p = 3$ e ciò implica che $8x^3 - 6x - 1$ è il polinomio minimo di $a = \cos\left(\frac{\pi}{9}\right)$. Tale polinomio ha però grado 3 e quindi $\left[\mathbb{Q}\left(cos\left(\frac{\pi}{9}\right)\right) : \mathbb{Q}\right] = 3$ e $3 \neq 2^k$ per qualunque k. Concludiamo che $\cos\left(\frac{\pi}{9}\right)$ non è costruibile e non è possibile tripartire questo angolo e, più in generale, dato $\theta$ arbitrario, non è possibile trisezionarlo usando le regole delle costruzioni con riga e compasso. □

**Teorema 6.2** (Quadratura del cerchio)**.** *Data una circonferenza di raggio 1, non è possibile costruire un quadrato con la stessa area.*

*Dimostrazione.* Assumiamo per assurdo che sia possibile costruire un quadrato con la stessa area di una circonferenza di raggio 1. L'area di tale circonferenza è $\pi * 1^2 = \pi$ e se fosse possibile costruire un quadrato con area $\pi$, allora anche la lunghezza dei suoi lati sarebbe costruibile. Sia $s$ la lunghezza del lato del quadrato. Dato che $s^2 = \pi$, allora $s = \sqrt{\pi}$ e dato che $s$ è costruibile, lo è anche $\sqrt{\pi}$. Ma se $\sqrt{\pi}$ è costruibile, allora lo è anche $\pi$, visto che $\pi = \sqrt{\pi}\sqrt{\pi}$ . Ma sappiamo che $\pi$ è trascendente in $\mathbb{Q}$ per il Teorema di Lindemann 1.4, dunque $\mathbb{Q}(\pi)/\mathbb{Q}$ non è algebrica e non esiste alcun polinomio con coefficienti razionali con radice $\pi$. Quindi, $[\mathbb{Q}(\pi) : \mathbb{Q}]$ è infinito. Ma se $\pi$ fosse costruibile, allora avremmo dovuto ottenere $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2^k$ per un $k \in \mathbb{N}_0$ e ciò porta a una contraddizione dell'ipotesi iniziale. Concludiamo che la quadratura del cerchio non è possibile. □

**Teorema 6.3** (Duplicazione del cubo)**.** *Dato un cubo di lato 1, non è possibile costruire un cubo con il doppio del volume.*

*Dimostrazione.* Supponiamo sia possibile. Il volume di un cubo di lato 1 è $1^3 = 1$, dunque vogliamo costruire un cubo di volume 2. Se fosse costruibile, anche la lunghezza del suo lato, $s$, dovrebbe essere costruibile. Dato che $s^3 = 2$, allora $s = \sqrt[3]{2}$. Il polinomio minimo di $s$ è $x^3 - 2$, irriducibile per il Criterio di Eisenstein 1.2 per p=2. Ma visto che $x^3 - 2$ ha grado 3, $\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3$ e $3 \neq 2^k$ per qualunque $k$. Concludiamo che $s$ non è costruibile e che quindi non è possibile costruire un cubo con il doppio del volume di un cubo di lato 1. □

# 7 Origami

La parola "origami" deriva dai termini giapponesi *oru* (piegare) e *kami* (carta) e indica l'arte di creare mediante la piegatura di fogli di carta. Questa tecnica consente di compiere nuove azioni rispetto alla sola costruzione con riga e compasso. Nelle costruzioni con il metodo origami, infatti, valgono ancora le precedenti regole di costruzione a cui si aggiunge la seguente:

**Definizione 7.1.** Dati due punti $a_1 \neq a_2$ non giacenti sulle rette $l_1 \neq l_2$, è possibile tracciare una nuova retta $l$, chiamata retta origami, che riflette il punto $a_1$ nel nuovo punto $b_1$ sulla retta $l_1$ e il punto $a_2$ nel nuovo punto $b_2$ sulla retta $l_2$.

Le operazioni consentite dalla costruzione con origami sono dunque le seguenti:

- R: Dati due punti, è possibile tracciare una retta passante per essi
- C: Dati due punti, è possibile disegnare una circonferenza centrata in uno e passante per l'altro
- RR: L'intersezione di due rette dà origine a un nuovo punto
- CC: L'intersezione di due circonferenze dà origine a un nuovo punto
- RC: L'intersezione di una retta con una circonferenza dà origine a un nuovo punto
- O: Una retta-origami può essere tracciata secondo la definizione 7.1

Grazie a questa nuova tecnica, siamo in grado di costruire poligoni a $n$ lati regolari che prima non erano possibili con solo riga e compasso. Capiamo perché individuando quali sono esattamente i numeri costruibili con il metodo origami:

Innanzitutto, le rette origami possono essere viste come tangenti simultanee di parabole: iniziamo con un punto $P$ chiamato fuoco, e una linea $l$, la direttrice. Per definizione, una parabola è l'insieme dei punti che sono equidistanti dal fuoco $P$ e la direttrice $l$. Per esempio, possiamo prendere qualsiasi punto $A$ sulla parabola e la distanza dal punto $P$ al punto $A$ è uguale alla distanza tra il punto $A$ e la linea $l$, se tracciamo una retta perpendicolare da $A$. Ora, consideriamo la retta tangente alla parabola nel punto $A$. Questa retta può essere vista come una retta origami che riflette il punto $P$ al punto $D$ sulla retta $l$, come in Figura 12.

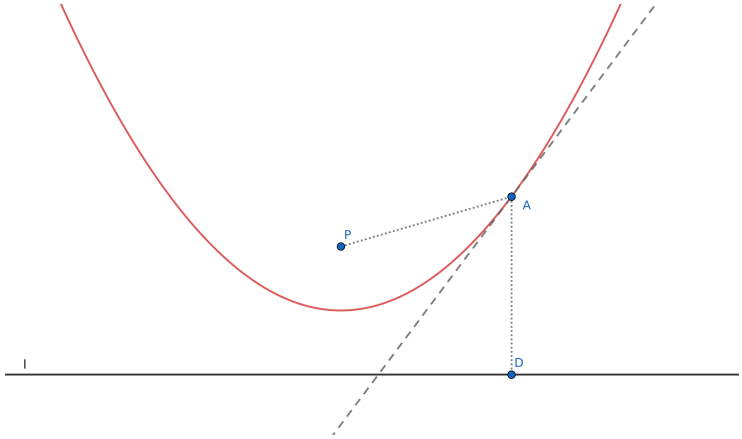


Figura 12: Parabola 1

Osserviamo ora le equazioni di due parabole

$$\left(y - \tfrac{1}{2}a\right)^2 = 2bx \text{ e } y = \tfrac{1}{2}x^2.$$

Iniziando da $\left(y - \frac{1}{2}a\right)^2 = 2bx$, possiamo usare la derivata per trovare la pendenza della tangente, ossia

$$m = \frac{b}{y - \frac{1}{2}a}.$$

Ora, possiamo definire un punto $(x_1, y_1)$ sulla parabola in termini di $m$, ottenendo $(x_1, y_1) = \left(\frac{b}{2m^2}, \frac{b}{m} + \frac{a}{2}\right)$. Facendo lo stesso con $y = \frac{1}{2}x^2$, la derivata è

$$m = x$$

e $(x_2, y_2) = (m, \frac{m^2}{2})$. Utilizzando ora la formula del coefficiente angolare

$$m = \frac{y_2 - y_1}{x_2 - x_1},$$

abbiamo

$$m = \frac{\frac{m^2}{2} - \left(\frac{b}{m} + \frac{a}{2}\right)}{m - \frac{b}{2m^2}} = \frac{m^4 - 2bm - am^2}{2m^3 - b}.$$

Otteniamo dunque che $m$ è soluzione dell'equazione cubica

$$m^3 + am + b = 0.$$

Questo mostra come la costruzione origami ci permette di risolvere equazioni cubiche del tipo $m^3+am+b = 0$ dove $a$ e $b$ sono costruibili utilizzando le tangenti simultanee di due parabole.

Dunque, dato che $m$ è soluzione di un polinomio irriducibile di grado 3, abbiamo anche un'estensione di grado 3. Ora, visto che i passi per le costruzioni possono essere estensioni di grado $1, 2$ e 3, moltiplicando il grado di ogni step si ha un'estensione di grado $2^k3^j$ per qualche $k, j \in \mathbb{N}_0$, cioè $[\mathbb{Q}(x) : \mathbb{Q}] = 2^k3^j$ per $k, j \in \mathbb{N}_0$.

Mostriamo ora la risoluzione di due dei tre problemi classici:

**Trisezione di un angolo**

Cominciamo da un "pezzo di carta" quadrato creato dalle rette $j, k, l$ ed $m$ come in Figura 13. Chiamiamo $P_1$ il punto di intersezione tra $m$ e $j$, quindi disegniamo una retta $n$ passante per $P_1$ che crei un angolo $\theta$ arbitrario che in figura è rappresentato da $\measuredangle AP_1D$.

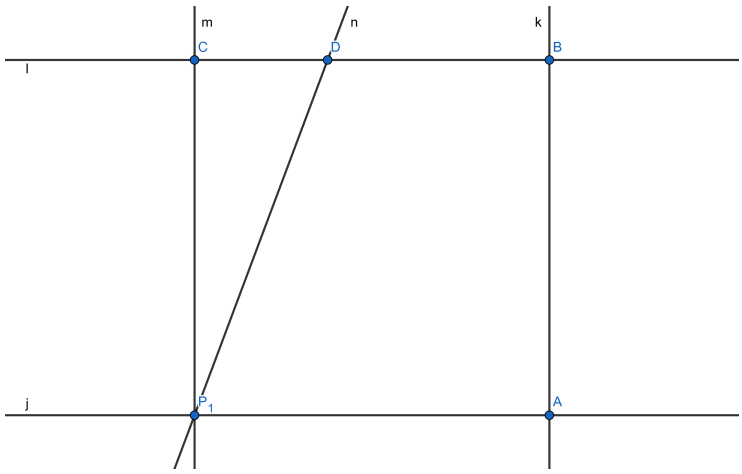


Figura 13: Trisezione 1

Adesso creiamo una retta origami secondo la definizione 7.1 parallela alla retta $j$ riflettendo il punto $P_1$ in un nuovo punto $P_2$ sulla retta $m$ e il punto $A$ in un nuovo punto $F$ sulla retta $k$.

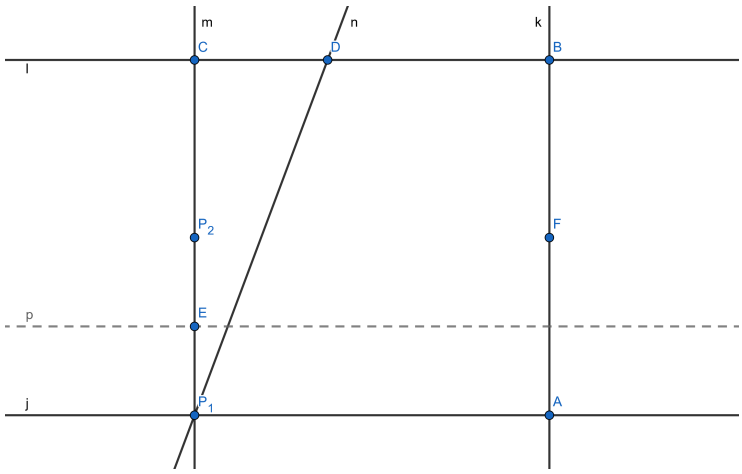


Figura 14: Trisezione 2

Ora, facciamo passare una retta attraverso $P_2$ e $F$.

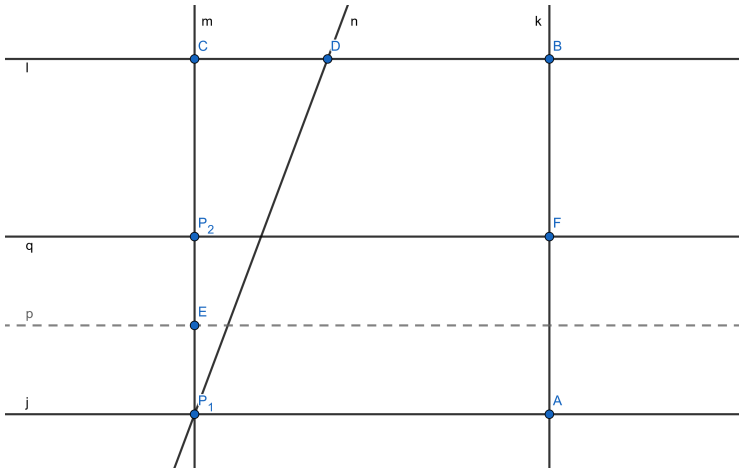


Figura 15: Trisezione 3

Creiamo un'altra retta origami $r$ che rifletta il punto $P_1$ in un nuovo punto $Q_1$ sulla retta $p$ e il punto $P_2$ nel punto $Q_2$ sulla retta $n$.

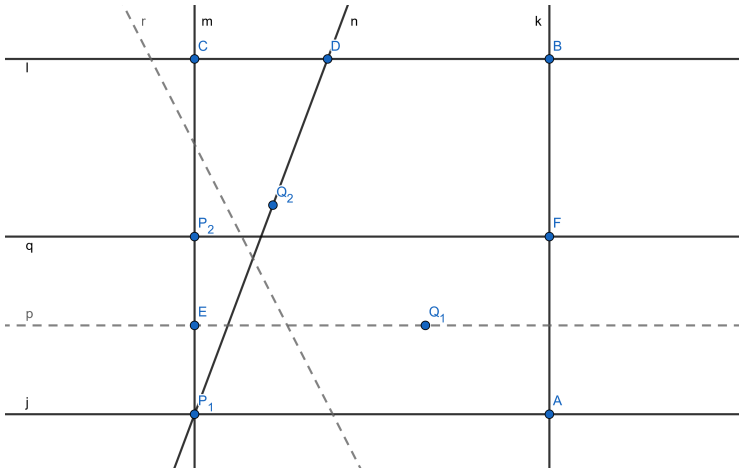


Figura 16: Trisezione 4

Infine, tracciamo la retta $s$ passante per $P_1$ e $Q_1$ e la retta $t$ passante per $P_1$ e il punto di intersezione delle rette origami $G$ e avremo diviso l'angolo iniziale $\theta$ in tre angoli uguali. Per vedere che i tre angoli risultanti siano ampi esattamente $\frac{\theta}{3}$, basta piegare il "foglio" due volte. Abbiamo dunque trisezionato l'angolo di partenza.

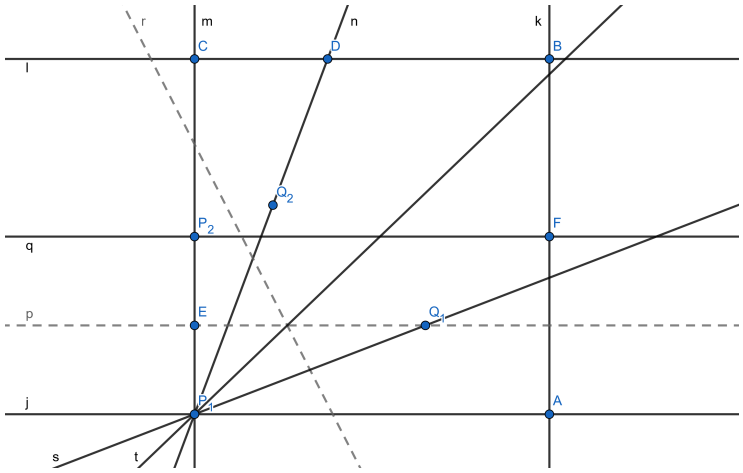


Figura 17: Trisezione 5

**Duplicazione del cubo**

In questo caso, supponiamo di avere un cubo di lato $s_1$ e volume $s_1^3 = V$. L'obiettivo è trovare il lato $s_2$ di un cubo tale che il suo volume sia $s_2^3 = 2V$. Cominciando sempre da un "pezzo di carta" quadrato creato dalle rette $j, k, l$ ed $m$ e tracciamo una retta origami $p$ a metà del "foglio", come in Figura 18, e creiamo il punto $E$.

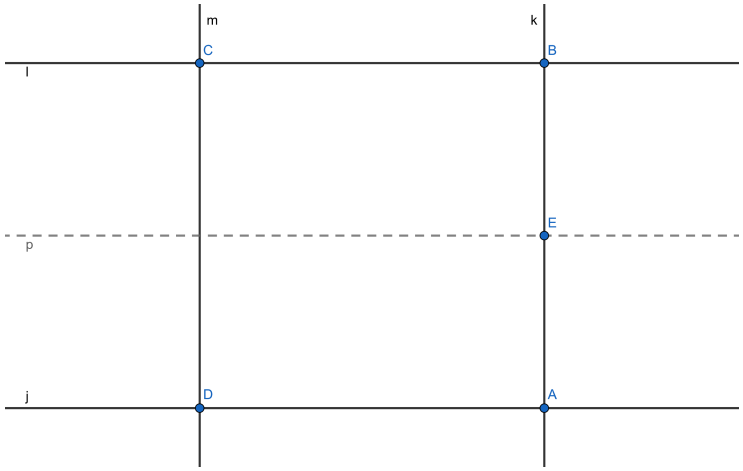


Figura 18: Duplicazione 1

Dopodiché, tracciamo altre due rette origami $q$ ed $r$: la prima che attraversa i punti $A$ e $C$ tracciando una diagonale e la seconda che attraversa $D$ ed $E$. L'intersezione tra queste rette genererà il punto $G$.

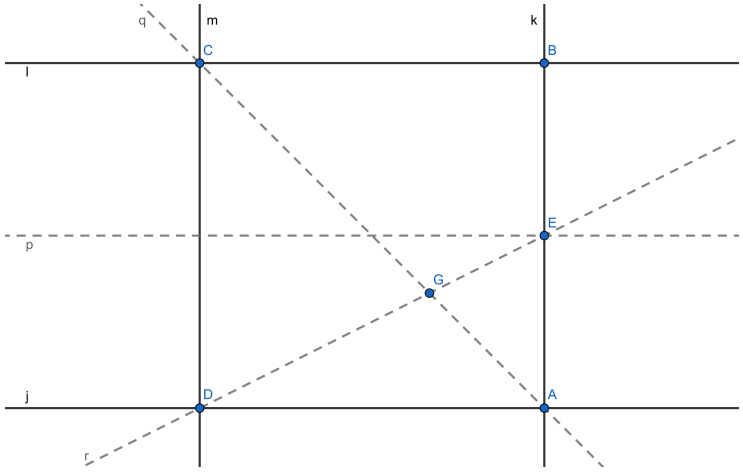


Figura 19: Duplicazione 2

Dividiamo in tre strisce uguali il foglio creando una retta origami $t$ che rifletta la retta $l$ nella retta $s$, passante per $G$, la quale a sua volta riflette la retta $j$ nella retta $t$, come in Figura 20. L'intersezione tra $s$ e $k$ genera il punto $H$.

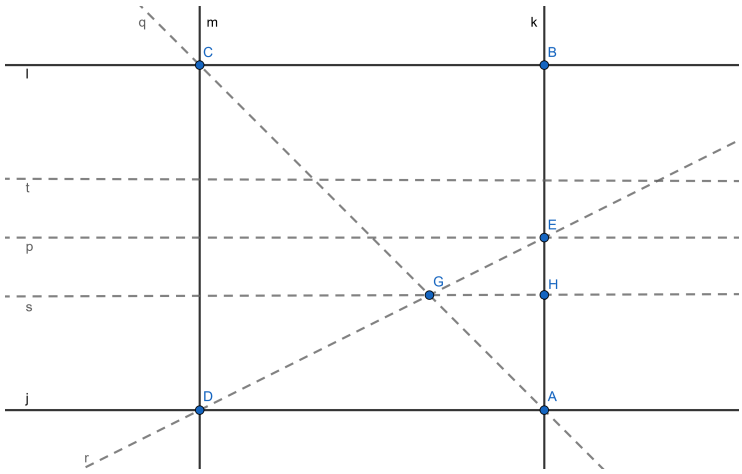


Figura 20: Duplicazione 3

Adesso, pieghiamo il "foglio" in modo che il punto $A$ poggi sul segmento $\overline{CD}$ e il punto $H$ poggi su $t$, come in Figura 21. Il rapporto tra i segmenti $\overline{CA}$ e $\overline{AD}$, moltiplicato per $s_1$, darà come risultato il lato $s_2$ cercato.

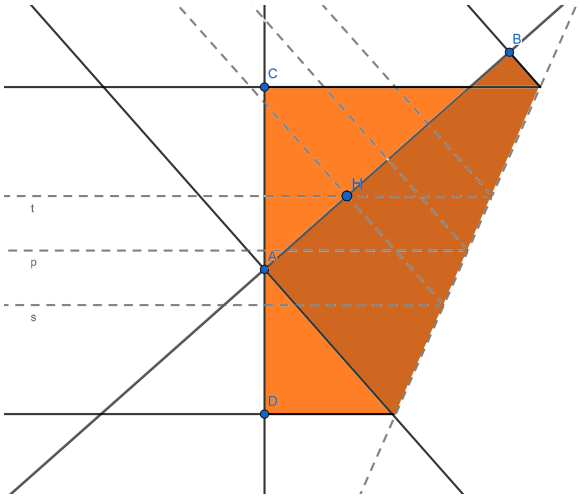


Figura 21: Duplicazione 4

# 8 Criterio di Costruibilità con Origami

**Teorema 8.1** (Criterio di Costruibilità con Origami)**.** *Un poligono a $n$ lati regolare è costruibile con origami se e solo se $n = 2^a 3^b p_1 p_2 ... p_t$, dove $a, b \geq 0$ e ogni $p_i$ è un numero primo della forma $p_i = 2^{m_i} 3^{r_i} + 1$ per $m_i, r_i \in \mathbb{N}$.*

*Dimostrazione.* ($\Rightarrow$) Supponiamo che un poligono a $n$ lati regolare sia costruibile con origami. Ciò implica che $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right] = 2^k 3^j$. Per lemma 4.1, $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) \subseteq \mathbb{Q}(\omega)$, con $\omega = e^{\frac{2\pi i}{n}}$, dove $\mathbb{Q}(\omega)$ è un'estensione di $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$ e $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$ è un'estensione di $\mathbb{Q}$. Dato che $\Phi_n(x)$ è il polinomio minimo di grado $\varphi(n)$ di $\omega$, $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$. Per la teoria dei campi si ha che

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right] \cdot \left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right].$$

Per il Teorema fondamentale della teoria di Galois 4.3,

$$\varphi(n) = \left|\mathrm{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right)\right| \cdot \left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right]$$

e quindi

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \frac{\varphi(n)}{|\,\mathrm{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right)|}.$$

Sappiamo anche che $\mathrm{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right) \leq \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$. Ora, sia $H = \mathrm{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right)$ e $G = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ così da avere $H \leq G$. Per la definizione 4.5 di gruppo di Galois, abbiamo che per ogni $\sigma \in H, \sigma(\omega) = \omega^k$ per un qualche $k$, e $\sigma\left(\cos\left(\frac{2\pi}{n}\right)\right) = \cos\left(\frac{2\pi}{n}\right)$. Ma $\omega = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$, quindi

$$\begin{aligned}\sigma(\omega) &= \sigma\left(\cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)\right) \\ &= \sigma\left(\cos\left(\frac{2\pi}{n}\right)\right) + \sigma(i)\sigma\left(\sin\left(\frac{2\pi}{n}\right)\right).\end{aligned}$$

Si ha anche che $\sigma(\omega) = \omega^k = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$.

Dunque, $\cos\left(\frac{2\pi}{n}\right) = \cos\left(\frac{2\pi k}{n}\right)$, che implica che o $k = 1$ o $k = n - 1$ e che $|H| = 2$.

Quindi,

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \frac{\varphi(n)}{|H|} = \frac{\varphi(n)}{2}.$$

Per supposizione, si ha che $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = 2^k 3^j$, e quindi $\varphi(n) = 2^l 3^j$, dove $l = k - 1$. Sia $p_1^{n1} p_2^{n_2} ... p_r^{n_r}$ la fattorizzazione in numeri primi di $n$ e, dato che la funzione phi di Eulero è moltiplicativa,

$$\begin{aligned}2^l 3^j = \varphi(n) = \varphi(p_1^{n1})\varphi(p_2^{n_2})...\varphi(p_t^{n_t}) \\ = ((p_1 - 1)(p_1^{n_1 - 1}))((p_2 - 1)(p_2^{n_2 - 1}))...((p_t - 1)(p_t^{n_t - 1})).\end{aligned}$$

Allora si deve avere che per ogni $i = 1, ..., t$ $p_i = 2$ o 3, oppure $p_i - 1 = 2^{m_i}3^{n_i}$, cioè $p_i = 2^{m_i}3^{n_i} + 1$ per un $m_i, n_i \in \mathbb{N}_0$.

($\Leftarrow$) Supponiamo che $n = 2^a 3^b p_1 p_2 ... p_t$ dove $a, b \geq 0$ e ogni $p_i$ è un numero primo della forma $p_i = 2^{m_i}3^{n_i} + 1$ per un $m_i, n_i \in \mathbb{N}_0$. Sappiamo che

$$\varphi(n) = [\mathbb{Q}(\omega) : \mathbb{Q}] = |\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})|.$$

Per il Teorema fondamentale della teoria di Galois 4.3, abbiamo che

$$\begin{aligned}\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] &= \frac{|\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})|}{\left|\operatorname{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right)\right|} \\ &= \frac{\varphi(n)}{\left|\operatorname{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right)\right|}.\end{aligned}$$

Da ($\Rightarrow$) sappiamo che

$$\left|\operatorname{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right)\right| = 2$$

e quindi

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \left|\operatorname{Gal}\left(\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right)\right| = \varphi(n)/2.$$

Dopodiché, sappiamo anche che

$$\begin{aligned}\varphi(n) &= \varphi(2^a 3^b p_1 p_2 ... p_t) \\ &= \varphi(2^a)\varphi(3^b)\varphi(p_1)\varphi(p_2)...\varphi(p_t) \\ &= 2^{a-1}3^{b-1}(p_1^{1-1}(p_1 - 1))...(p_t^{1-1}(p_t - 1))\end{aligned}$$

e quindi

$$\varphi(n)/2 = 2^{a-2}3^{b-1}(p_1 - 1)...(p_t - 1),$$

dove $p_i = 2^{m_i}3^{n_i} + 1$. Ciò implica che

$$\varphi(n)/2 = 2^{a-2}3^{b-1}(2^{m_1}3^{n_1})(2^{m_2}3^{n_2})...(2^{m_t}3^{n_t}) = 2^k 3^j \text{ per un } k, j \in \mathbb{N}_0.$$

In conclusione, abbiamo

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = 2^k 3^j$$

per un $k, j \in \mathbb{N}_0$, cioè il poligono a $n$ lati è costruibile. □

Ora sappiamo esattamente quali poligoni a $n$ lati regolari possiamo costruire con il metodo origami. Possiamo notare che questa tecnica ha allargato le nostre possibilità di costruzione: ad esempio, con la costruzione tradizionale potevamo creare poligoni regolari a

$$3, 4, 5, 6, 8, 10, 12, 15, 16, 17, ...$$

lati, mentre adesso siamo in grado di creare poligoni regolari a

$$3, 4, 5, 6, 7, 8, 9, 10, 12, 15, 16, 17, 18, ...$$

lati grazie il metodo origami.

Per quanto riguarda i problemi classici invece, abbiamo una soluzione grazie alla possibilità di avere estensioni di grado multiplo di tre: infatti, come abbiamo visto nel Capitolo 6, sia per la trisezione dell'angolo che per la duplicazione del cubo era necessaria un'estensione di grado tre, per la precisione $\left[\mathbb{Q}\left(cos\left(\frac{\pi}{9}\right)\right) : \mathbb{Q}\right] = 3$ per il primo e $\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3$ per il secondo.

# Riferimenti bibliografici


[1] Betzabe Bojorquez. Geometric constructions from an algebraic perspective. https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1265&context=etd.

[2] "Davide". I tre problemi greci insolubili – problemi con riga e compasso. https://www.mathone.it/problemi-greci-insolubili/.

[3] Jean-Pierre Escofier. *Galois theory*, volume 204. Springer Science & Business Media, 2000.

[4] Julia Greene. Geometric constructions, origami, and galois theory. 2019.

[5] Israel N Herstein. *Abstract algebra*. John Wiley & Sons, 1996.

[6] David (https://math.stackexchange.com/users/119775/david). Consider numbers of the type $n = 2^m + 1$. prove that such an n is prime only if $n = f_k$ for some $k \in n$, where $f_k$ is a fermat prime. Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/840204 (version: 2014-06-20).

[7] Robert J. Lang. From flapping birds to space telescopes: The modern science of origami. https://static.usenix.org/event/usenix08/tech/slides/lang.pdf.

[8] Professor Alexei Skorobogatov. Rings and fields. https://www.ma.imperial.ac.uk/~anskor/notesM2P4.pdf.

[9] Treccani. Costruzione con riga e compasso. https://www.treccani.it/enciclopedia/costruzione-con-riga-e-compasso_(Enciclopedia-della-Matematica)/.