



Università degli Studi di Trento

DIPARTIMENTO DI MATEMATICA
Corso di Laurea Magistrale in Matematica

La matematica greca

Studentesse:

Annalisa Ficara

Matricola 000000

Giulia Bondoni

Matricola 168388

Indice

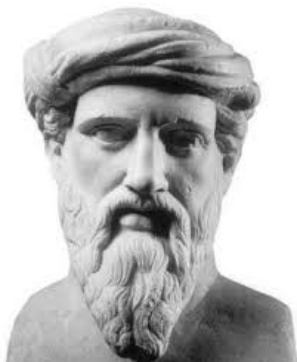
1	Il teorema di Pitagora	2
1.1	La scuola pitagorica	2
1.2	Il teorema e una sua dimostrazione	4
1.3	Terne pitagoriche	5
1.4	Applicazioni del teorema di Pitagora	8
2	I solidi platonici	11
2.1	Introduzione	11
2.2	I poliedri regolari	11
2.3	Il problema di Euclide	18
3	Costruzioni con riga e compasso	20
3.1	Il metodo dei Greci	20
3.2	Richiami sulle estensioni di campi	27
3.3	Approccio algebrico	30
3.4	Problemi non risolubili	33

Capitolo 1

Il teorema di Pitagora

1.1 La scuola pitagorica

La figura storica di Pitagora è avvolta dal mistero, infatti non sono mai stati rinvenuti documenti risalenti all'epoca in cui è vissuto.



Le informazioni che si hanno a disposizione risalgono a secoli successivi ed è piuttosto difficile separare la leggenda dalla realtà. Lo stesso Aristotele, considerato il primo storico della filosofia, si limitava a parlare della scuola pitagorica e non della figura del suo fondatore. L'alone di mistero è ulteriormente infittito dal clima di segretezza che circondava la scuola pitagorica, che si presentava come setta mistica. I suoi adepti dovevano seguire un rigido codice di condotta, le cui restrizioni includevano norme alimentari, comportamentali e relazionali.

I risultati matematici erano considerati proprietà della scuola e non venivano mai citati i singoli autori delle scoperte.

In campo matematico i pitagorici si occupavano di:

- **geometria:** proprietà delle figure geometriche (relazioni tra lunghezze, angoli e aree; in particolare il teorema di Pitagora), costruzione di poligoni regolari;
- **aritmetica:** soluzione geometrica di alcune equazioni algebriche;
- **musica:** scoperta del rapporto numerico alla base dell'altezza dei suoni.

Proprio questo interesse per la musica maturò in un'attenzione particolare verso l'aritmetica, intesa come teoria dei numeri interi, che non ritenevano una teoria astratta bensì concreta. I numeri non erano degli enti intangibili, ma delle grandezze misurabili aventi un'estensione e una forma tanto che essi venivano rappresentati con punti e linee.

I pitagorici tentavano di interpretare ogni fatto naturale attraverso la geometria e l'aritmetica. Questo spirito emergeva chiaramente dal motto della scuola: "Tutto è numero". Tale tema non potrebbe essere più attuale: con l'avvento dei computer, degli strumenti digitali e del mondo virtuale tutto è codificato con sequenze di numeri binari. L'aritmetizzazione del mondo è certamente più evidente ora che ai tempi di Pitagora.

La scoperta dei numeri irrazionali rompe questa simmetria tra matematica e realtà, creando un profondo divario alimentato dalla filosofia platonica secondo la quale la geometria è un'astrazione della materia e non una sua concretizzazione.

Secondo le fonti più attendibili Pitagora sarebbe nato nella prima metà del VI sec. a.C. a Samo, un'isola greca vicino alle coste dell'attuale Turchia. Fece molti viaggi, tra cui a Mileto dove fu allievo di Talete, in Egitto e in Babilonia dove approfondì le sue conoscenze matematiche.

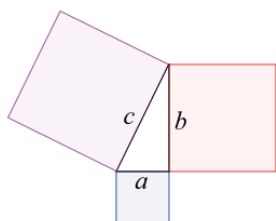


Attorno al 540 a.C. si trasferì in Magna Grecia, a Crotone, ove fondò la sua scuola. Le credenze politiche aristocratiche della scuola si scontrarono presto con la mentalità democratica del popolo. Si narra che durante una rivolta Pitagora rimase ucciso nei pressi di Metaponto nel 497 a.C..

1.2 Il teorema e una sua dimostrazione

Il teorema di Pitagora è forse il più famoso teorema di matematica, familiare anche a chi non ne è pratico. Il suo enunciato, attribuito a Pitagora, era in verità già noto ai Babilonesi ed era conosciuto anche in Cina e in India. La dimostrazione del teorema è invece con ogni probabilità successiva a Pitagora. Esso rappresenta la prima espressione della profonda e nascosta relazione esistente tra aritmetica e geometria.

Teorema 1.2.1 (di Pitagora). *In un triangolo rettangolo, il quadrato costruito sull'ipotenusa è equivalente alla somma dei quadrati costruiti sui cateti.*



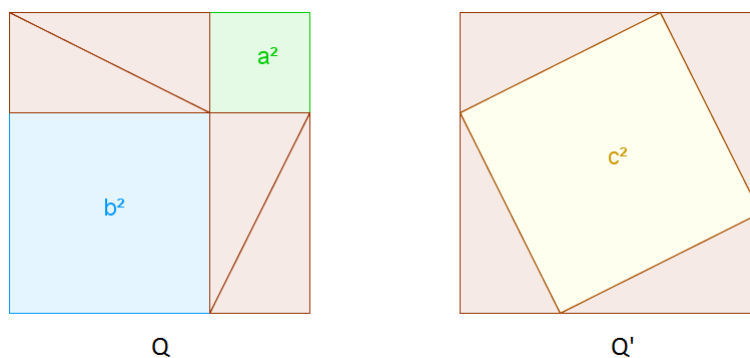
Facendo riferimento alla figura, si può esprimere il teorema con l'equazione:

$$a^2 + b^2 = c^2$$

Le soluzioni di tali equazioni servivano a costruire gli angoli retti. In questo senso il teorema dà un'interpretazione geometrica a un fatto puramente algebrico, in perfetta sintonia con lo spirito della scuola pitagorica.

Le dimostrazioni sono tantissime. Quella classica chiude il primo libro degli *Elementi* di Euclide, ma nel corso dei secoli ne sono state proposte diverse centinaia con molte varianti. Quella che proponiamo è una dimostrazione grafica.

Dimostrazione. Costruiamo i quadrati Q e Q' come in figura.



Entrambi hanno lato $a + b$, quindi sono equivalenti. Sia $A(T)$ l'area del triangolo rettangolo di cateti a, b e ipotenusa c .

$$A(Q) = 4A(T) + a^2 + b^2$$

$$A(Q') = 4A(T) + c^2$$

Essendo $A(Q) = A(Q')$ segue che $a^2 + b^2 = c^2$. □

1.3 Terne pitagoriche

Come già accennato, i Babilonesi conoscevano già il teorema di Pitagora.



La prova fu trovata nella tavoletta Plimpton 322 che raccoglieva un grande numero di coppie intere (a, c) per le quali esiste b soddisfacente: $a^2 + b^2 = c^2$.

Il problema fu poi meglio contestualizzato e risolto dai matematici greci, da Euclide a Diofanto.

Definizione 1.3.1. Una **terna pitagorica** è una terna (a, b, c) , con $a, b, c \in \mathbb{N} \setminus \{0\}$ tale che $a^2 + b^2 = c^2$.

Ad ogni terna pitagorica si può associare un triangolo rettangolo di cateti a, b e ipotenusa c e viceversa.

Definizione 1.3.2. Una terna pitagorica si dice **primitiva** se a, b, c sono coprimi.

Una terna pitagorica è primitiva se e solo se a, b sono coprimi. Infatti se a, b sono coprimi anche a, b, c lo sono. Viceversa, se la terna è primitiva segue che $\nexists p$ primo tale che $p \mid a, p \mid b$ e $p \mid c$. Si supponga che esista p' primo tale che $p' \mid a, p' \mid b \Rightarrow p' \mid a^2 + b^2 = c^2 \Rightarrow p' \mid c$, il che contraddice l'ipotesi. Segue che a, b sono coprimi.

In questa relazione si tratterà solo di terne pitagoriche primitive, in quanto ad ogni terna pitagorica si può associare una primitiva come segue:

sia p un primo che divide a e $b \Rightarrow p \mid a$ e $p \mid b \Rightarrow p \mid a^2 + b^2 = c^2 \Rightarrow p \mid c$.

Si consideri la terna $(a/p, b/p, c/p)$. Essa è una terna pitagorica, infatti:

$$\frac{a^2}{p^2} + \frac{b^2}{p^2} = \left(\frac{a^2 + b^2}{p^2} \right) = \frac{c^2}{p^2}$$

Iterando questo procedimento fino a che $(a, b) = 1$ si ottiene una terna pitagorica primitiva. Dunque ogni terna pitagorica è della forma (da, db, dc) ove (a, b, c) è una terna primitiva.

Alcune terne pitagoriche primitive:

$$\begin{array}{cccc} (3, 4, 5) & (5, 12, 13) & (7, 24, 25) & (8, 15, 17) \\ (9, 40, 41) & (11, 60, 61) & (12, 35, 37) & (13, 84, 85) \\ (16, 63, 65) & (20, 21, 29) & (28, 45, 53) & (33, 56, 65) \\ (36, 77, 85) & (39, 80, 89) & (48, 55, 73) & (65, 72, 97) \end{array}$$

Esistono diversi modi di generare le terne pitagoriche primitive. Alcuni di questi possono generarle tutte, che equivale a determinare tutte le soluzioni intere positive dell'equazione pitagorica. Altri metodi ne generano solo una certa classe.

La formula più conosciuta per la generazione di tutte le terne pitagoriche primitive è quella scoperta da Euclide e Diofanto (300-250 a.C.) in maniera indipendente:

$$a = m^2 - n^2 \quad b = 2mn \quad c = m^2 + n^2$$

con m, n coprimi di diversa parità.

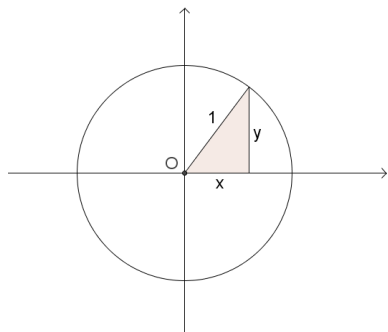
La dimostrazione di Euclide è di tipo aritmetico, mentre Diofanto utilizzò una strategia basata sull'interpretazione geometrica delle terne pitagoriche, come mostriamo di seguito.

Punti razionali sulla circonferenza

Si consideri la terna pitagorica primitiva (a, b, c) . Trovare le soluzioni intere di $a^2 + b^2 = c^2$ equivale a trovare le soluzioni razionali di $x^2 + y^2 = 1$, infatti:

$$a^2 + b^2 = c^2 \quad \Leftrightarrow \quad \frac{a^2}{c^2} + \frac{b^2}{c^2} = 1$$

Chiamando $x := \frac{a}{c}$ e $y := \frac{b}{c}$ si ottiene l'equazione $x^2 + y^2 = 1$.

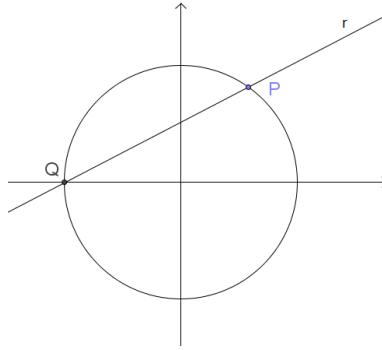


Il punto (x, y) appartiene alla circonferenza unitaria, quindi il triangolo rettangolo di cateti x, y può essere inserito nella circonferenza come in figura.

L'idea di base di questa dimostrazione, e in generale di tutti i problemi diofantini, è quella di partire da una soluzione banale nota. Tracciamo poi la retta tra tale punto e uno generico della circonferenza e cerchiamo le intersezioni razionali tra le due. Se entrambi i punti hanno

coordinate razionali segue che anche la pendenza della retta sarà razionale, in

quanto combinazione lineare delle coordinate dei punti. Si noti che in questo modo troveremo soluzioni anche per $x = 0$ e $y = 0$ che corrispondono a casi degeneri di triangoli rettangoli.



Scegliamo come soluzione banale il punto $Q(-1, 0)$. La retta passante per Q e $P(x, y)$ ha equazione:

$$r : y = t(x + 1)$$

I punti di intersezione tra retta e circonferenza si trovano risolvendo il sistema:

$$\begin{cases} y = t(x + 1) \\ x^2 + y^2 = 1 \end{cases}$$

$$\begin{aligned} x^2 + t^2(x^2 + 2x + 1) &= 1 \\ x^2(1 + t^2) + 2t^2x + t^2 - 1 &= 0 \end{aligned}$$

$$x_{1,2} = \frac{-t^2 \pm \sqrt{t^4 - t^4 + 1}}{t^2 + 1} = \frac{-t^2 \pm 1}{t^2 + 1}$$

da cui si ottengono le soluzioni: $x_1 = -1$ $x_2 = \frac{1 - t^2}{t^2 + 1}$

La prima soluzione corrisponde al punto $Q(-1, 0)$, mentre la seconda al punto

$$P\left(\frac{1 - t^2}{t^2 + 1}, t\left(\frac{1 - t^2}{t^2 + 1} + \frac{t^2 + 1}{t^2 + 1}\right)\right) = P\left(\frac{1 - t^2}{t^2 + 1}, t\left(\frac{2}{t^2 + 1}\right)\right)$$

Come già detto, scegliendo t razionale troviamo una parametrizzazione razionale della circonferenza.

Sia $t = \frac{n}{m}$, con $n, m \in \mathbb{Z}$ non nulli. Le coordinate di P diventano:

$$\begin{cases} x = \frac{1 - \left(\frac{n}{m}\right)^2}{\left(\frac{n}{m}\right)^2 + 1} = \frac{m^2 - n^2}{n^2 + m^2} \\ y = \frac{n}{m} \left(\frac{2}{\left(\frac{n}{m}\right)^2 + 1} \right) = \frac{2nm}{n^2 + m^2} \end{cases}$$

Tornando alla terna pitagorica, ricordiamo che $x := \frac{a}{c}$, $y := \frac{b}{c}$ e che tali frazioni sono sicuramente ai minimi termini, in quanto la terna considerata è primitiva. Si ottiene quindi la formula di Euclide:

$$a = m^2 - n^2 \quad b = 2mn \quad c = m^2 + n^2$$

1.4 Applicazioni del teorema di Pitagora

Scoperta dei numeri irrazionali

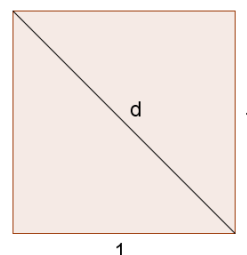
Come già detto, i pitagorici erano alla costante ricerca di una corrispondenza tra matematica e realtà. Ci si può immaginare il loro sgomento quando per la prima volta si ritrovarono di fronte a una quantità non esprimibile attraverso rapporto di numeri interi.

La scoperta dei numeri irrazionali viene attribuita a Ippaso di Metaponto, che vi si imbattè nel tentativo di determinare la lunghezza della diagonale di un quadrato di lato 1 (vedi sotto). Pitagora non poteva tollerare l'esistenza di grandezze incommensurabili tanto che, secondo la leggenda, fece gettare Ippaso in mare.

Applicando il teorema di Pitagora, la diagonale di tale quadrato risulta essere:

$$d = \sqrt{1^2 + 1^2} = \sqrt{2}$$

Teorema 1.4.1. $\sqrt{2}$ non è razionale.



Dimostrazione. Si supponga per assurdo che esistano p, q interi coprimi tali che

$$\frac{p}{q} = \sqrt{2} \quad \Rightarrow \quad p^2 = 2q^2$$

Segue che p^2 è pari, quindi p è pari. Sia $p = 2k$, con $k \in \mathbb{Z} \setminus \{0\}$.

$$(2k)^2 = 2q^2 \quad \Leftrightarrow \quad q^2 = 2k^2$$

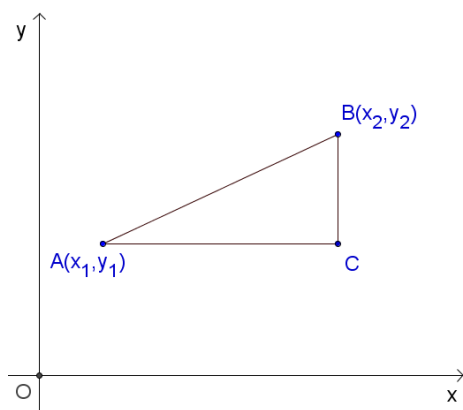
Quindi anche q è pari. Ciò è assurdo, avendo scelto p e q coprimi. □

I numeri irrazionali crearono un forte distacco tra la geometria e l'aritmetica. Fu solo nel XIX secolo che questo apparente conflitto venne riconciliato con il lavoro di Hilbert. In questo nuovo scenario il teorema di Pitagora gioca un ruolo fondamentale, come si mostra nella prossima sezione.

Distanza nel piano cartesiano

A partire dal XVII sec. d.C. si assistè ad una riconciliazione tra geometria e aritmetica, con l'introduzione del sistema di riferimento cartesiano e la nascita della geometria analitica.

Fu Cartesio nel 1637 che nella sua opera "La Géométrie" propose di rappresentare un punto nel piano come una coppia ordinata di numeri, le cui componenti rappresentavano la distanza con due rette perpendicolari fissate su cui era stata definita un'unità di misura (assi cartesiani). Lo scopo di Cartesio era duplice: da un lato liberare la geometria dal ricorso alle figure per arrivare a risultati più generali; dall'altro dare un significato alle operazioni algebriche per mezzo di un'interpretazione geometrica.



Si considerino nel piano cartesiano i punti $A(x_1, y_1)$ e $B(x_2, y_2)$. Il punto C per come è stato costruito avrà coordinate (x_2, y_1) . In un approccio geometrico, usando il teorema di Pitagora si può dedurre che:

$$AB^2 = AC^2 + CB^2$$

Come detto, la seconda coordinata di B e C rappresenta la distanza di tali punti dalla retta x . La distanza relativa tra di essi sarà quindi $y_2 - y_1$. Con

un ragionamento analogo possiamo affermare che la distanza relativa tra A e C è $x_2 - x_1$. Quindi:

$$AB = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad (1.1)$$

Hilbert nel 1899 formalizzò quest'intuizione, prendendo la 1.1 come *definizione* di distanza. Ricostruendo tutta la geometria partendo da questi nuovi fondamenti, i teoremi che prima venivano costruiti sulla figura diventarono teoremi numerici.

Capitolo 2

I solidi platonici

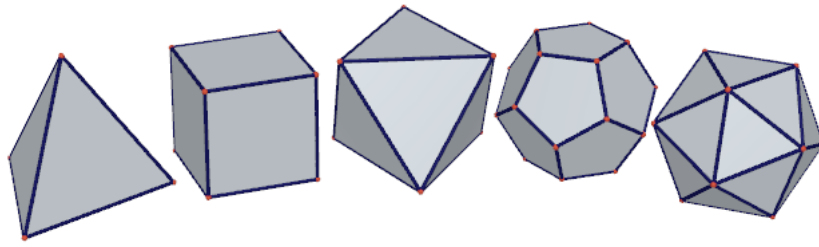
2.1 Introduzione

La geometria greca è praticamente completa per quanto riguarda le proprietà elementari delle figure piane. Euclide nei suoi *Elementi* raccolse i risultati che erano noti fino ad allora come, ad esempio, la geometria elementare dei triangoli e delle circonferenze. Anche altre parti più sofisticate degli *Elementi* erano il frutto del lavoro di matematici antecedenti ad Euclide. Tra queste vi è la geometria solida che essendo, anche oggi, molto più impegnativa di quella piana, venne lasciata in uno stato meno completo dai Greci. La teoria dei poliedri regolari nel libro XII degli *Elementi* è dovuta, almeno in parte, a Teetèto (c.a. 415-369 a.C.) scolaro di Platone a cui è attribuito il completamento di uno dei capitoli più belli della geometria solida con una delle più notevoli scoperte della materia: l'enumerazione dei solidi regolari.

2.2 I poliedri regolari

Un poliedro è regolare se soddisfa le seguenti condizioni:

- le facce sono tutte poligoni regolari,
- le facce sono tutte congruenti tra loro,
- in ogni vertice concorre lo stesso numero di facce.



Mentre i poligoni regolari, con un numero di lati maggiore di tre, sono infiniti si osserva che i poliedri regolari sono solo cinque, infatti si può facilmente dimostrare il seguente

Teorema 2.2.1. *I solidi regolari sono cinque:*

1. *tetraedro*
2. *cubo*
3. *dodecaedro*
4. *ottaedro*
5. *icosaedro*

Dimostrazione. Si considerino i possibili poligoni che possono concorrere in un vertice e per ciascuno di essi si consideri il numero di facce e di angoli possibili.

Per un triangolo equilatero l'angolo al vertice è $\frac{\pi}{3}$, quindi in un vertice di un solido con facce di forma triangolare possono concorrere tre, quattro o cinque triangoli. Nello stesso vertice non potranno invece concorrere sei facce perchè in tal caso si avrebbe un angolo totale pari a 2π e quindi le facce formerebbero un piano.

Procedendo con lo stesso ragionamento si ha che per un poliedro dotato di facce quadrate in un vertice possono concorrere tre facce ma non quattro perchè l'angolo al vertice di un quadrato è $\frac{\pi}{2}$ e in tal caso si avrebbe di nuovo un piano.

Analogamente l'angolo al vertice di un pentagono è $\frac{3\pi}{5}$ e quindi in un vertice di un solido formato da facce pentagonali possono concorrere solamente tre pentagoni ma non quattro.

Per un esagono l'angolo al vertice è pari a $\frac{2\pi}{3}$ quindi per la costruzione di un solido di facce esagonali non si potrebbero nemmeno avere tre facce in un vertice. Allo stesso modo neppure i poligoni con più di sei lati possono essere utilizzati per costruire un poliedro regolare. \square

Per descrivere meglio tali poliedri e in particolare determinare il numero delle facce che ciascuno di essi presenta è possibile utilizzare la formula di Eulero. Siano F , S e V rispettivamente i numeri di facce, spigoli e vertici di un poliedro regolare, la formula di Eulero afferma che

$$F - S + V = 2$$

Tale formula può essere applicata ad ognuno dei casi considerati precedentemente in questo modo:

- Triangolo equilatero

1. Caso in cui in ogni vertice concorrono tre facce: ogni faccia presenta tre vertici ma ognuno di essi sta su tre facce. Un ragionamento analogo può essere fatto anche per gli spigoli del solido e così si ottengono le seguenti formule:

$$V = \frac{3F}{3} \quad \text{e} \quad S = \frac{3F}{2}$$

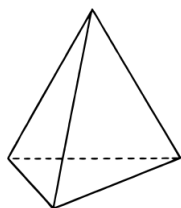
che sostituite nella formula di Eulero danno:

$$F - \frac{3}{2}F + F = 2$$

$$2F - \frac{3}{2}F = 2$$

da cui il numero totale delle facce del solido sarà

$$F = 4$$



2. Caso in cui in ogni vertice concorrono quattro facce:

$$V = \frac{3}{4}F \quad \text{e} \quad S = \frac{3}{2}F$$

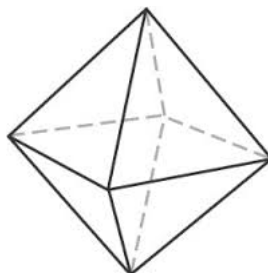
sostituendo queste relazioni nella formula di Eulero si avrà:

$$F - \frac{3}{2}F + \frac{3}{4}F = 2$$

$$\frac{4F - 6F + 3F}{4} = 2$$

da cui il numero totale delle facce del solido

$$F = 8$$



3. Caso in cui in ogni spigolo concorrono cinque facce:

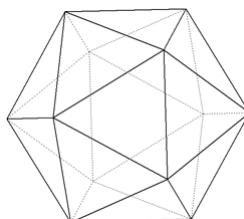
$$V = \frac{3}{5}F \quad \text{e} \quad S = \frac{3}{2}F$$

sostituendo queste relazioni nella formula si ottiene:

$$\begin{aligned} F - \frac{3}{2}F + \frac{3}{5}F &= 2 \\ \frac{10F - 15F + 6F}{10} &= 2 \end{aligned}$$

e quindi il numero totale di facce è:

$$F = 20.$$



- Quadrato

In questo caso in ogni vertice concorrono tre facce e ogni faccia presenta quattro vertici perciò si ha:

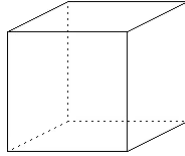
$$V = \frac{4}{3}F \quad \text{e} \quad S = \frac{4}{2}F$$

che sostituite nella formula danno:

$$\begin{aligned} F - 2F + \frac{4}{3}F &= 2 \\ \frac{3F - 6F + 4F}{3} &= 2 \end{aligned}$$

e quindi in questo caso il numero totale della facce è:

$$F = 6$$



- Pentagono

I pentagoni che possono concorrere in un vertice sono tre e ogni faccia presenta cinque vertici perciò si ha:

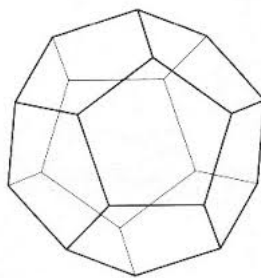
$$V = \frac{5}{3}F \quad \text{e} \quad S = \frac{5}{2}F$$

e sostituendo queste relazioni nella formula si ottiene:

$$F - \frac{5}{2}F + \frac{5}{3}F = 2$$
$$\frac{6F - 15F + 10F}{6} = 2$$

da cui il numero totale delle facce è

$$F = 12$$

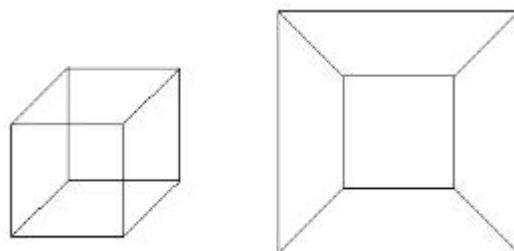


	NOME	FACCE	SPIGOLI	VERTICI	SPIGOLI PER VERTICE	SPIGOLI PER FACCIA	SVILUPPO PIANO
	tetraedro	4	6	4	3	3	
	cubo	6	12	8	3	4	
	ottaedro	8	12	6	4	3	
	dodecaedro	12	30	20	3	5	
	icosaedro	20	30	12	5	3	

La prima dimostrazione rigorosa della formula di Eulero per i poliedri è dovuta ad Augustin-Luis Cauchy.

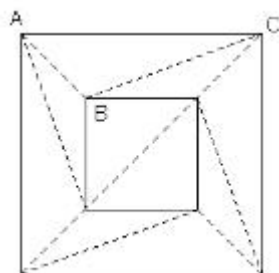
Si consideri un poliedro P semplicemente connesso con F facce, V vertici ed S spigoli. Per dimostrare che questi parametri soddisfano la relazione $F - S + V = 2$, Cauchy suggerì di procedere in questo modo.

Immaginando che il poliedro sia cavo, si asporta una sua faccia e, allungando gli spigoli della faccia eliminata, lo si deforma schiacciandolo sul piano; si ottiene allora un grafo G non orientato raffigurato nel piano i cui nodi sono i vertici di P e i cui lati sono gli spigoli deformati di P . Questa deformazione applicata è un omeomorfismo. Le facce non sono più le stesse dei poligoni, ma aree del piano delimitate da un ciclo di nodi collegati da lati. Per gli elementi del grafo planare ottenuto si possono usare ancora i termini faccia, vertice e spigolo ed i numeri degli oggetti con questi nomi non sono cambiati rispetto a quelli del poliedro P . Si consideri in particolare che la faccia tolta a P corrisponde a tutta l'area esterna a G .



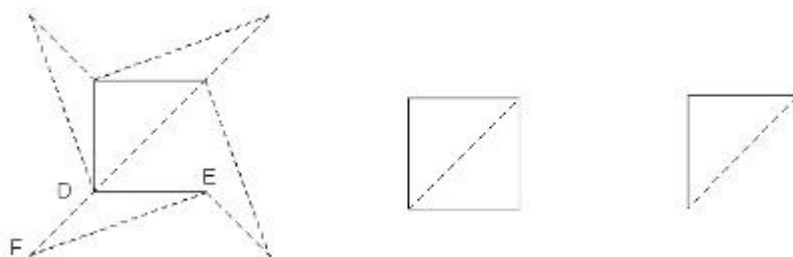
Si procede ora con una serie di modifiche sul grafo G tali da non alterare il valore di $F - S + V$. Ogni modifica consiste nel tracciare per una faccia

avente più di tre lati una diagonale. Quest'operazione aggiunge a G una faccia e uno spigolo ma non modifica il numero di vertici, perciò l'espressione $F - S + V$ resta invariata. Si ripete questa operazione fino ad avere soltanto facce triangolari.



A questo punto si ripetono le seguenti operazioni:

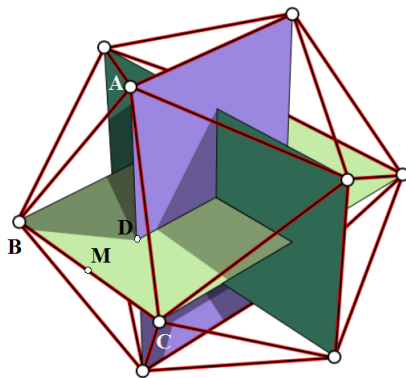
- si eliminano uno per uno tutti i triangoli che hanno due lati sul contorno esterno del grafo G . Ad ogni soppressione, si tolgono un vertice, due spigoli ed una faccia; ciò conserva l'espressione $F - S + V$;
- si eliminano uno per uno tutti i triangoli che hanno un solo lato sul contorno esterno del nostro grafo. Ad ogni soppressione, si tolgono uno spigolo ed una faccia (il numero dei vertici rimane inalterato). Anche questa modifica conserva l'espressione $F - S + V$.



Si possono ripetere le trasformazioni precedenti nell'ordine che si preferisce, fino a rimanere con un solo grafo triangolare. Questo tipo di grafo ha due facce (l'interno e l'esterno del triangolo), tre spigoli e tre vertici. Quindi $F = 2$, $V = 3$ e $S = 3$ e dunque $F - S + V = 2$. Questa espressione è uguale a quella di partenza $F - S + V$ perchè ogni manovra eseguita ne ha conservato il valore. Si conclude quindi che il poliedro di partenza verificava la formula di Eulero.

2.3 Il problema di Euclide

La dimostrazione dell'esistenza del tetraedo, del cubo e dell'ottaedro è facile, tuttavia non è chiaro come 20 triangoli equilateri possano essere assemblati a formare una superficie chiusa. Euclide trovò questo problema abbastanza difficile, tanto da collocarlo verso la fine della sua opera e solo pochi dei suoi lettori riuscirono a padroneggiarne la soluzione. Una bellissima costruzione diretta è dovuta a Luca Pacioli, amico di Leonardo Da Vinci, nella sua opera intitolata *De divina proportione* del 1509. La costruzione di Pacioli utilizza tre copie del *rettangolo aureo* intersecati come in figura:



I dodici vertici dei rettangoli definiscono esattamente 20 triangoli e per dimostrare che essi formano un icosaedro è sufficiente mostrare che sono triangoli equilateri con lato di lunghezza 1. Si può verificare la correttezza della costruzione di Pacioli utilizzando il teorema di Pitagora. Il lato minore di ogni rettangolo aureo è 1, il lato maggiore misura x e soddisfa l'equazione $x^2 - x - 1 = 0$ da cui si ricava che $x = \frac{1+\sqrt{5}}{2}$. Sia M il punto medio del lato BC e sia D il punto in cui si incontrano i due rettangoli i cui vertici definiscono il triangolo ABC . Dal teorema di Pitagora si ha che

$$AM^2 = MD^2 + AD^2,$$

dove $MD = \frac{x-1}{2}$ e $AD = \frac{x}{2}$, perciò sostituendo si ottiene:

$$AM^2 = \left(\frac{x-1}{2}\right)^2 + \left(\frac{x}{2}\right)^2$$

dove, considerando che $(x-1)^2 = x^2 - 2x + 1 = x + 1 - 2x + 1 = 2 - x$, si ottiene:

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

Applicando una seconda volta il teorema di Pitagora si ottiene:

$$AB^2 = AM^2 + BM^2 = \frac{3}{4} + \frac{1}{4} = 1.$$

Quindi AB ha lunghezza 1 così come tutti i lati dei triangoli raffigurati, quindi si tratta di triangoli equilateri e il solido costruito in questo modo è un icosaedro.

Capitolo 3

Costruzioni con riga e compasso

3.1 Il metodo dei Greci

I greci nello studio della geometria erano guidati dall'intuizione sullo spazio fisico. Un aspetto della loro geometria che era particolarmente influenzato da considerazioni di tipo fisico era la teoria delle costruzioni. Essi scoprirono che molti problemi elementari, come ad esempio bisecare un segmento o un angolo, costruire una perpendicolare o disegnare una circonferenza passante per tre punti dati, potevano essere risolti mediante costruzioni con riga e compasso, altrimenti dette *costruzioni euclidee*.

Introducendo un sistema di coordinate non è difficile mostrare che i punti che possono essere costruiti a partire da P_1, \dots, P_n hanno coordinate nel campo generato dalle coordinate P_1, \dots, P_n mediante l'operazione di radice quadrata. Questa operazione compare direttamente dal teorema di Pitagora in questa maniera: dati i punti di coordinate (a, b) e (c, d) , la loro distanza è data da $\sqrt{(c - a)^2 + (d - b)^2}$.

Per i Greci rimanevano tuttavia irrisolti alcuni problemi di costruzione con riga e compasso:

- trisecare gli angoli;
- duplicare il cubo;
- costruire i poligoni regolari;
- rettificare la circonferenza cioè costruire un quadrato di area uguale a quella di una circonferenza data o, equivalentemente, costruire il numero π .

L'impossibilità di risolvere questi problemi non venne provata fino al diciannovesimo secolo. Wantzel nel 1837 si occupò dei primi due problemi, mentre

Lindemann nel 1882 si dedicò alla rettificazione della circonferenza mostrando che il numero π non solo non è definibile da operazioni razionali e radici quadrate ma è anche trascendente, cioè non è la radice di nessuna equazione polinomiale a coefficienti razionali.

Un problema di costruzione con riga e compasso rimane ancora oggi aperto: stabilire quali poligoni regolari siano costruibili con riga e compasso. Gauss nel 1796 scoprì che il poligono con 17 lati è costruibile e mostrò che un poligono regolare con n lati è costruibile se e solo se $n = 2^m p_1 p_2 \dots p_k$ dove ogni p_i è un primo della forma $2^{2^h} + 1$. La dimostrazione di necessità venne completata da Wantzel, tuttavia rimangono sconosciuti quali siano questi primi e anche se essi siano infiniti. Gli unici conosciuti sono quelli per $h = 0, 1, 2, 3, 4$.

Il problema delle costruzioni euclidee può essere formulato in questo modo: sia dato un insieme finito di punti $S_1 = \{P_1, P_2, \dots, P_n\}$ nel piano ω , definiamo il sottoinsieme S_r con $r = 1, 2, \dots$, induttivamente partendo da $S_1 = \{P_1, P_2, \dots, P_n\}$ e procedendo poi con S_{r+1} che è l'unione di S_r con

- (1) insieme dei punti di intersezione delle coppie di linee che connettono punti distinti di S_r ;
- (2) insieme dei punti di intersezione delle linee specificate in (1) con tutte le circonferenze aventi centro in un punto di S_r e raggio uguale al segmento avente l'estremo finale in S_r ;
- (3) insieme dei punti di intersezione delle coppie di circonferenze di (2).

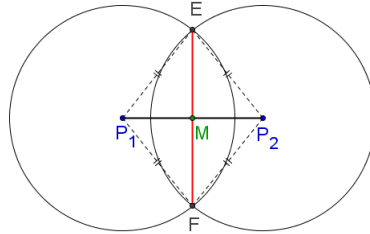
Sia $C(P_1, P_2, \dots, P_n) = \bigcup_{r \in \mathbb{N}} S_r$ l'insieme di tutti i punti costruibili con riga e compasso partendo dall'insieme iniziale $\{P_1, P_2, \dots, P_n\}$. Si può quindi dire che un punto P di ω può essere costruito con riga e compasso a partire dai punti P_1, P_2, \dots, P_n se $P \in C(P_1, P_2, \dots, P_n)$. Altrimenti P non può essere costruito dai P_i .

Esempi

1) Costruzione del punto medio di un segmento

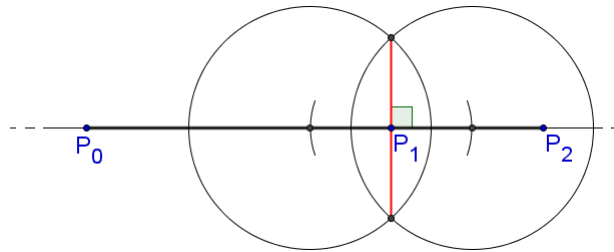
Sia P_1P_2 il segmento dato, si traccino due circonferenze con centri in P_1 e P_2 i cui raggi siano uguali e di lunghezza maggiore della metà del segmento iniziale. Queste due circonferenze si intersecano in due punti equidistanti, per costruzione, dagli estremi del segmento considerato e la cui congiungente interseca P_1P_2 in un punto M che è il punto medio del segmento considerato. Infatti i triangoli P_1EF e EP_2F sono isosceli e congruenti perchè hanno i tre lati ordinatamente congruenti (terzo criterio di congruenza) e in particolare

gli angoli P_1EM e MEP_2 sono congruenti, quindi considerando il triangolo isoscele P_1EP_2 si ha che il segmento EM è bisettrice dell'angolo al vertice e perciò anche mediana e altezza relativa alla base P_1P_2 .



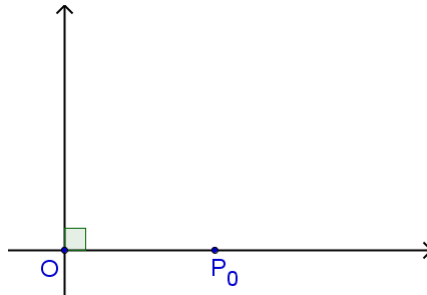
2) Costruzione della perpendicolare a un segmento per un punto

Siano P_0 , P_1 e P_2 tre punti allineati congiunti da una retta. Il primo passo per disegnare la perpendicolare a questa retta passante per P_1 consiste nel tracciare una circonferenza di centro P_1 e raggio tale che essa individui sulla retta data due punti di cui P_1 sarà il punto medio. Si consideri ora il segmento compreso tra questi due punti e si costruisca il suo asse come visto precedentemente: esso sarà proprio la retta perpendicolare alla retta data passante per il punto P_1 .



3) Costruzione di un sistema cartesiano

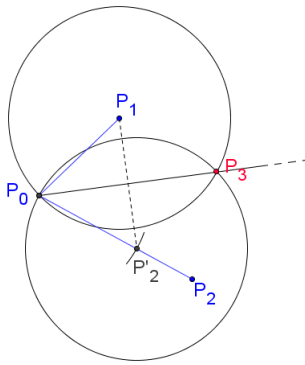
Utilizzando le costruzioni precedenti è possibile costruire un sistema di riferimento cartesiano. Si consideri il punto O e un punto P_0 , si tracci la retta passante per questi due punti e poi la perpendicolare a questa retta passante per O . Si fissi ora l'unità di misura del riferimento cartesiano come la distanza OP_0 e un ordine di percorrenza delle due rette.



4) Bisezione di un angolo

Dato un angolo θ trovare $\frac{\theta}{2}$. Il problema si può tradurre in questa maniera: dati i punti P_0 , P_1 e P_2 nel piano non allineati, trovare il punto P_3 tale che

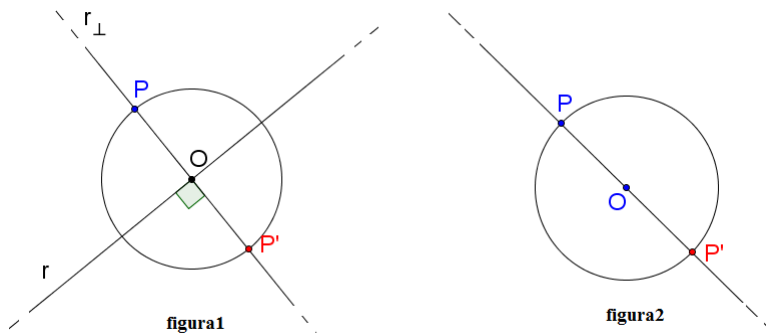
$$\theta = \angle P_1 P_0 P_2 = 2 \angle P_1 P_0 P_3$$



Sia P_0 il vertice dell'angolo considerato. Si tracci la circonferenza di centro P_0 e raggio P_0P_1 che individua un punto P'_2 sull'altro lato dell'angolo θ . Si costruiscano ora due circonferenze uguali di raggio maggiore della metà del segmento $P_1P'_2$ e centrate nei punti P_1 e P'_2 . L'intersezione delle due circonferenze è P_3 . La retta che congiunge i punti P_0 e P_3 oltre ad essere l'asse del segmento $P_1P'_2$ è anche la bisettrice dell'angolo in P_0 .

5) Costruzione del simmetrico di un punto rispetto ad una retta

Siano dati una retta r e un punto P esterno ad essa. Si tracci la perpendicolare r_\perp alla retta data passante per il punto P . Sia O l'intersezione di queste due rette. Si tracci ora la circonferenza di centro O e raggio OP : il punto P' di intersezione della circonferenza con r_\perp è proprio il punto simmetrico cercato (figura 1).

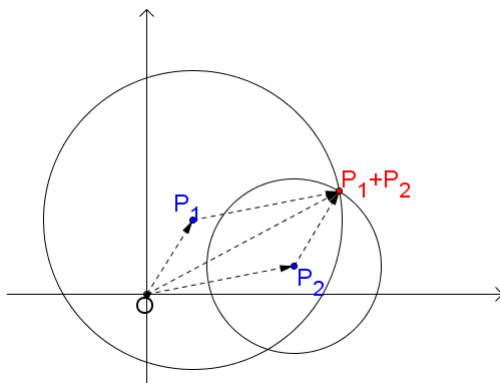


6) Costruzione del simmetrico di un punto dato rispetto a un punto

Si consideri un punto P e un punto O rispetto al quale si vuole costruire il simmetrico di P . Si tracci la retta passante per P ed O e la circonferenza di centro O e raggio OP . Il loro punto di intersezione è il simmetrico cercato (figura 2). In particolare, dato un punto P si può trovare il punto $-P$ facendo il simmetrico rispetto all'origine.

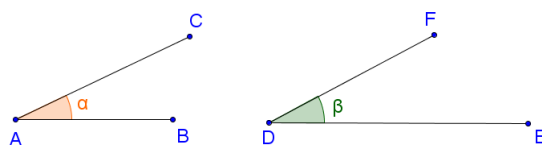
7) Costruzione della somma di due punti dati

Siano dati i punti P_1 e P_2 nel piano cartesiano di origine O . La somma $P_1 + P_2$ si ottiene tracciando due circonferenze, la prima di centro P_1 e raggio OP_2 , la seconda centrata in P_2 con raggio OP_1 . La somma di P_1 e P_2 è il punto di intersezione delle due circonferenze.

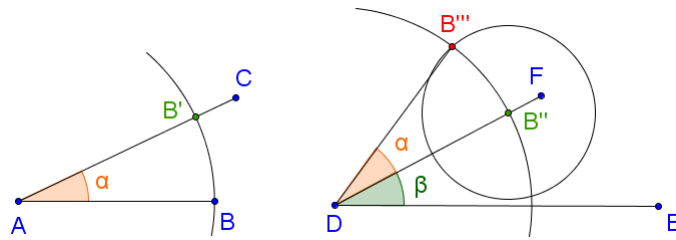


8) Costruzione dell'angolo somma di due angoli dati

Siano $\alpha = BAC$ e $\beta = EDF$ due angoli.

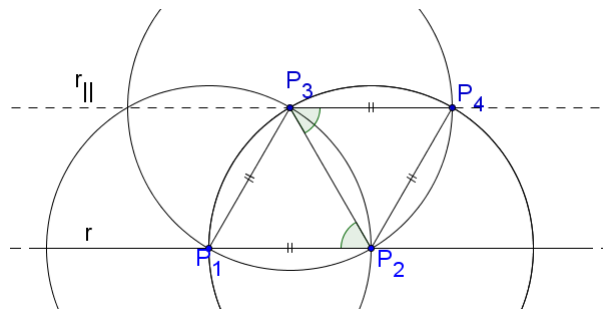


La loro somma si costruisce trasportando un angolo sull'altro, ad esempio α su β , in modo che il vertice e un lato siano in comune mentre gli altri due lati siano posti da parti di piano opposte al lato in comune. Per far questo si tracci la circonferenza di centro A e raggio AB la cui intersezione con il lato AC individua il punto B' . Si tracci la circonferenza di centro D e raggio DE che individua sul lato DF il punto B'' e si consideri poi il punto di intersezione di questa con la circonferenza centrata in B' e di raggio $B'B'$. Il lato DB''' così ottenuto è il lato dell'angolo α non in comune con β e l'apertura totale è la somma dei due angoli di partenza.



9) Costruzione di una retta parallela a una retta data

Sia r una retta, e P_1, P_2 due suoi punti. Si costruisca il triangolo equilatero di base P_1P_2 e vertice P_3 . Si costruisca poi il triangolo equilatero di base P_2P_3 e vertice P_4 . Si tracci la retta r_{\parallel} passante per i punti P_3 e P_4 . I due triangoli equilateri sono per costruzione congruenti, in particolare l'angolo $P_1P_2P_3$ e l'angolo $P_2P_3P_4$ sono congruenti e, dal fatto che essi sono angoli alterni interni tagliati dalla secante P_2P_3 sulle due rette r e r_{\parallel} , si conclude che le due rette sono parallele.

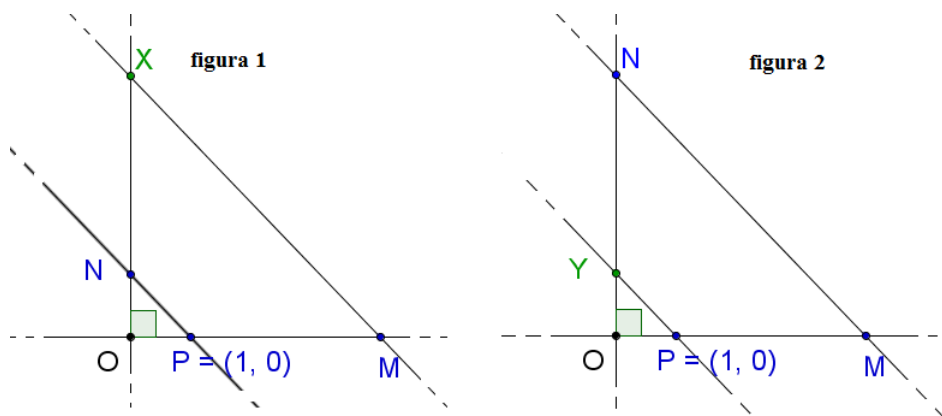


10) Costruzione del prodotto di due punti dati

Su una retta si consideri un punto O e un punto P in modo che $OP = 1$. Si costruisca la perpendicolare a questa retta passante per O e si costruiscano poi due punti N ed M in maniera tale che $OM = m$ e $ON = n$. Si tracci quindi la retta passante per P ed N e poi la parallela a tale retta passante per M . L'intersezione di tale parallela con la retta ON è un punto X che si dimostra essere il prodotto $N \cdot M$ tramite la proporzione

$$X : N = M : 1 \quad \text{da cui si ottiene} \quad X = N \cdot M$$

(figura 1).



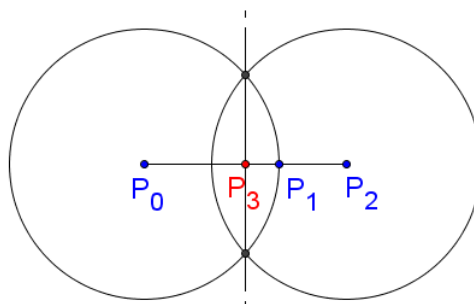
Con una semplice inversione del procedimento si può costruire anche il quoziente di due numeri: si tracci prima la retta che congiunge i punti M ed N e poi la sua parallela passante per P . La nuova intersezione così ottenuta è il punto Y che si dimostra essere il rapporto $\frac{N}{M}$, infatti in questo caso si avrà la proporzione

$$N : Y = M : 1 \quad \text{da cui si ottiene} \quad Y = \frac{N}{M}$$

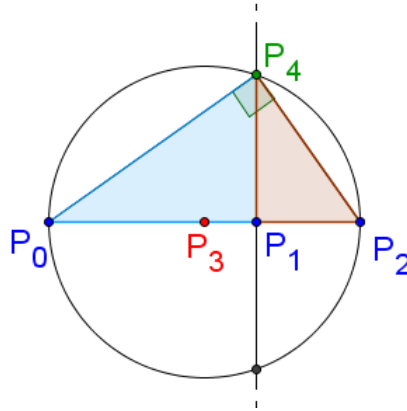
(figura 2).

11) Costruzione della radice di un numero

Dato un numero r trovare \sqrt{r} . Il problema si può tradurre in termini geometrici: dato un segmento lungo r costruirne uno di misura \sqrt{r} . Per risolverlo si procede seguendo questi passaggi. Dati tre punti allineati P_0 , P_1 e P_2 si trovi il punto medio P_3 del segmento P_0P_2 .



Si costruisca poi la circonferenza di centro P_3 e raggio P_0P_3 .



Si costruisca ora la perpendicolare al segmento dato passante per P_1 ottenendo così due triangoli. Il triangolo $P_0P_1P_4$ è simile a $P_1P_2P_4$ quindi si ha la seguente proporzione:

$$P_0P_1 : P_1P_4 = P_1P_4 : 1$$

da cui si ottiene il segmento cercato:

$$P_1P_4 = \sqrt{P_0P_1} = \sqrt{r}$$

3.2 Richiami sulle estensioni di campi

Definizione 3.2.1. Siano E e F due campi tali che $F \subseteq E$. E si dice *estensione* di F e si denota con E/F .

Sia E/F estensione, allora E è uno spazio vettoriale su F . Infatti siano $a, b \in E$ e $\lambda \in F$, si ha banalmente che $a + b \in E$ e $\lambda a \in E$. Si può quindi parlare di dimensione di E su F : essa è chiamata *grado di E su F* e indicata con $|E : F|$.

Teorema 3.2.2 (Formula dei gradi). *Siano K/E e E/F estensioni di campo di grado finito. Allora K/F è un'estensione di campi di grado finito e*

$$|K : F| = |K : E||E : F|$$

Dimostrazione. Sia $\{\alpha_1, \dots, \alpha_m\}$ una base di K su E e $\{\beta_1, \dots, \beta_n\}$ una base di E su F . E' sufficiente mostrare che gli $\alpha_i\beta_j$ per $1 \leq i \leq m$ e $1 \leq j \leq n$ formano una base di K su F . Mostriamo innanzitutto che gli $\alpha_i\beta_j$ generano K su F .

Sia $a \in K$. Poichè gli α_i generano K come E -spazio vettoriale, esisteranno $b_i \in E$ tali che

$$a = \sum_{i=1}^m b_i \alpha_i$$

e poichè i β_j generano l' F -spazio vettoriale E , esisteranno $c_{ij} \in F$ tali che

$$b_i = \sum_{j=1}^n c_{ij} \beta_j$$

Segue che

$$a = \sum_{i=1}^m \sum_{j=1}^n c_{ij} \alpha_i \beta_j$$

e quindi gli elementi $\alpha_i \beta_j$ per $1 \leq i \leq m$ e $1 \leq j \leq n$ generano K come F -spazio vettoriale. Rimane da mostrare che $\alpha_i \beta_j$ sono linearmente indipendenti. Consideriamo una combinazione lineare

$$\sum_{i,j} a_{ij} \alpha_i \beta_j = 0$$

per $a_{ij} \in F$. Essa può essere scritta come

$$\sum_i \left(\sum_j a_{ij} \beta_j \right) \alpha_i = 0$$

La somma tra parentesi è un elemento di E e poichè gli α_i formano una base di K su E , e quindi sono linearmente indipendenti, segue che

$$\sum_i a_{ij} \beta_i = 0 \quad \forall j$$

Ora l'indipendenza lineare dei β_j su F implica $a_{ij} = 0$ per ogni i . Segue che gli $\alpha_i \beta_j$ sono linearmente indipendenti e quindi formano una base per K come F -spazio vettoriale. □

Sia E/F estensione e $a \in E$. Definiamo

$$F[a] := \{f(a) \mid f(x) \in F[x]\}$$

L'unico polinomio monico e irriducibile di $F[x]$ che si annulla in a si dice **polinomio minimo** di a su F .

Proposizione 3.2.3. *Sia $a \in E$ algebrico su F e sia $f(x)$ il suo polinomio minimo. Allora*

$$F[a] \simeq F[x]/(f)$$

$F[a]$ è un campo.

Definiamo $F(a) := \left\{ \frac{f(a)}{g(a)} \mid f, g \in F[x], g(a) \neq 0 \right\}$.

Si può dimostrare che $F(a)$ è il più piccolo campo contenente F e a .

La proposizione 3.2.3 ci suggerisce che $F[a] = F(a)$ se a è algebrico su F .

Proposizione 3.2.4. *Sia F un campo e $f \in F[x]$ un polinomio monico irriducibile. Allora*

$$|F[x]/(f) : F| = \deg(f)$$

Dimostrazione. Sia $d = \deg(f)$. Scriviamo $\gamma = x \bmod f$. Allora $1, \gamma, \dots, \gamma^{d-1}$ sono linearmente indipendenti. Infatti, se fosse

$$a_0 1 + a_1 \gamma + \dots + a_{d-1} \gamma^{d-1} = 0$$

si avrebbe

$$a_0 + a_1 x + \dots + a_{d-1} x^{d-1} = 0 \bmod f$$

Ma poichè f ha grado d segue che $a_0 = a_1 = \dots = a_{d-1} = 0$. Inoltre $1, \gamma, \dots, \gamma^{d-1}$ generano $F[x]/(f)$ perchè per un dato $g \in F[x]$, esiste un polinomio $r \in F[x]$ tale che $\deg(r) < d$ e $g = qf + r$. Segue che $g = r \bmod f$ e quindi $g \bmod f$ è una combinazione lineare di $1, \gamma, \dots, \gamma^{d-1}$. □

Teorema 3.2.5. *Sia E/F un'estensione e $a \in E$, allora*

$$|F[a] : F| = \begin{cases} \infty & \text{se } a \text{ è trascendente} \\ \deg(f) & \text{se } a \text{ è algebrico su } F \text{ e } f \text{ è il suo polinomio minimo} \end{cases}$$

Dimostrazione. Se a è trascendente $F[a] \simeq F[x]$ e quindi ha dimensione infinita su F . Invece se a è algebrico per la proposizione 3.2.3 si ha

$$F[a] \simeq F[x]/(f)$$

Per la proposizione precedente vale che

$$|F[x]/(f) : F| = \deg(f)$$

Sia $d = \deg(f)$, allora $\{1, x, x^2, \dots, x^{d-1}\}$ è una base di $F[x]/(f)$ su F . Allora $\{1, a, a^2, \dots, a^{d-1}\}$ è una base di $F[a]$ su F e $|F[a] : F| = d$. □

3.3 Approccio algebrico

Sia $C(P_1, P_2, \dots, P_n)$ l'insieme definito nella sezione 3.1. Assumiamo che $n \geq 2$, altrimenti $C(P_1) = \{P_1\}$ e l'insieme collaserebbe in un punto. Introduciamo un sistema di coordinate opportuno in modo che $P_1 = (0, 0)$ e $P_2 = (1, 0)$ come nella costruzione 3.

Il piano reale è isomorfo a \mathbb{C} mediante l'isomorfismo:

$$f : \mathbb{R}^2 \rightarrow \mathbb{C} \quad f(x, y) = x + iy$$

L'insieme $\{P_1, \dots, P_n\}$ è mandato nell'insieme complesso $\{z_1, \dots, z_n\}$, con $z_1 = 0$ e $z_2 = 1$. $C(z_1, \dots, z_n)$ sarà l'insieme dei numeri complessi costruibili con riga e compasso a partire da $\{z_1, \dots, z_n\}$.

Teorema 3.3.1 (di caratterizzazione). *$C(z_1, \dots, z_n)$ è il più piccolo sottocampo di \mathbb{C} contenente $\{z_1, \dots, z_n\}$ e chiuso rispetto alle operazioni di radice quadrata e coniugio.*

Dimostrazione. Vogliamo dimostrare che:

1. $C(z_1, \dots, z_n)$ è un sottocampo di \mathbb{C} chiuso per radice quadrata e coniugio;
2. $C(z_1, \dots, z_n)$ è il più piccolo sottocampo con tale caratteristica.

Passo 1: per definizione $C(z_1, \dots, z_n)$ contiene $\{z_1, \dots, z_n\}$. Esso è un sottocampo?

- siano $z_1, z_2 \in C(z_1, \dots, z_n)$

$z_1 + z_2$ è costruibile con la regola del parallelogramma, come nella costruzione 7;

$-z_1$ è costruibile, come nella costruzione 6;

Segue che $C(z_1, \dots, z_n)$ è un sottogruppo additivo di \mathbb{C} .

- per mostrare che l'insieme è chiuso per il prodotto è utile introdurre la forma polare: $z = \rho e^{i\theta}$, ove $\rho = \sqrt{x^2 + y^2}$ e θ è l'angolo formato tra il vettore Oz e l'asse delle ascisse.

Siano $z_1 = \rho_1 e^{i\theta_1}$, $z_2 = \rho_2 e^{i\theta_2}$. Segue che $z_1 z_2 = \rho_1 \rho_2 e^{i(\theta_1 + \theta_2)}$.

Nelle costruzioni, 10, 8 è stato mostrato rispettivamente come costruire $P_1 P_2$ partendo da P_1 e P_2 e come sommare due angoli $(\theta_1 + \theta_2)$. Sappiamo quindi costruire con riga e compasso sia $\rho_1 \rho_2$ che $\theta_1 + \theta_2$, e quindi il numero complesso $z_1 z_2$ appartiene a $C(z_1, \dots, z_n)$.

Quindi $C(z_1, \dots, z_n)$ è un sottocampo di \mathbb{C} . Inoltre:

- è chiuso rispetto all'operazione di radice;
Sia $z \in C(z_1, \dots, z_n)$, con $z = \rho e^{i\theta} \Rightarrow \sqrt{z} = \sqrt{\rho} e^{i\frac{\theta}{2}}$.
Nelle costruzioni 4, 11 è mostrato come sia possibile con riga e compasso bisecare l'angolo θ e trovare la radice quadrata di una data lunghezza.
- è chiuso rispetto all'operazione di coniugio;
Sia $z = x + iy$, $\bar{z} = x - iy$ è ottenibile facendo una simmetria rispetto all'asse delle ascisse come mostrato nella costruzione 5.

Passo 2: sia C' un sottocampo di \mathbb{C} contenente $\{z_1, \dots, z_n\}$ e chiuso rispetto alle operazioni radice quadrata e coniugio $\Rightarrow C' \supset C(z_1, \dots, z_n)$.

E' sufficiente mostrare che appartengono a C' :

- l'intersezione di due rette passanti per punti di C' appartiene a C' ;
siano $z_1, z_2 \in C'$, con $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2$. Segue che $x_1, y_1, x_2, y_2 \in C'$, infatti:

$$\begin{cases} z_1 + \bar{z}_1 = 2x_1 & \Rightarrow x_1 \in C' \\ z_1 - \bar{z}_1 = 2iy_1 & \Rightarrow y_1 \in C' \\ z_2 + \bar{z}_2 = 2x_2 & \Rightarrow x_2 \in C' \\ z_2 - \bar{z}_2 = 2iy_2 & \Rightarrow y_2 \in C' \end{cases}$$

Segue che l'equazione di una retta passante per due qualsiasi punti di C' della forma $ax + by + c = 0$, con $a, b, c \in C'$ in quanto combinazione lineare di x_1, y_1, x_2, y_2 . Prendiamo un'altra retta passante per altri due punti di C' ; essa avrà equazione $a'x + b'y + c' = 0$ con $a', b', c' \in C'$. L'intersezione tra le due rette si ottiene risolvendo il sistema:

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0 \end{cases}$$

La soluzione di tale sistema sarà una combinazione lineare di a, b, c, a', b', c' , quindi apparterrà a C' .

- l'intersezione tra una retta e una circonferenza avente centro in un punto di C' e raggio un segmento ottenuto congiungendo due punti di C' appartiene a C'

Siano z_1, z_2 come al prima. La circonferenza con centro in z_1 e raggio $\left| \sqrt{x_1^2 + y_1^2} - \sqrt{x_2^2 + y_2^2} \right|$ avrà equazione:

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

con d, e, f combinazioni di x_1, y_1, x_2, y_2 e quindi appartenenti a C' . L'intersezione con la retta si ottiene risolvendo il sistema:

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 + dx + ey + f = 0 \end{cases}$$

e sarà combinazione di a, b, c, d, e, f , quindi sta in C' .

- l'intersezione tra due circonferenze, ottenute come sopra, appartiene a C' . Essa infatti si trova risolvendo il sistema:

$$\begin{cases} x^2 + y^2 + dx + ey + f = 0 \\ x^2 + y^2 + d'x + e'y + f' = 0 \end{cases}$$

e sarà una combinazione di d, e, f, d', e', f' , quindi appartiene a C' .

Si può concludere che qualsiasi sottocampo di \mathbb{C} chiuso rispetto alle operazioni radice quadrata e coniugio contiene $C(z_1, \dots, z_n)$. Esso è quindi il più piccolo sottocampo con tale caratteristica e il teorema è provato. \square

Da questo teorema si può dedurre la seguente caratterizzazione di $C(z_1, \dots, z_n)$.

Criterio 3.3.2. *Siano $z_1, z_2, \dots, z_n \in \mathbb{C}$ e sia $F = \mathbb{Q}(z_1, \dots, z_n, \bar{z}_1, \dots, \bar{z}_n)$. $z \in \mathbb{C}$ è costruibile con riga e compasso a partire da $z_1, z_2, \dots, z_n \in \mathbb{C}$ se e solo se z appartiene a un sottocampo di \mathbb{C} della forma*

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

$F(u_1, \dots, u_r)$ costruito come sopra si dice **torre di radici quadrate su F** .

Dimostrazione. Sia C' l'insieme delle torri di radici quadrate costruite a partire da F .

Sicuramente $C' \subseteq C(z_1, \dots, z_n)$, dato che quest'ultimo contiene F ed è chiuso per coniugio e radice quadrata.

Siano $z, z' \in C'$, quindi apparterranno a torri di radici quadrate:

$$z \in F(u_1, \dots, u_r) \quad z' \in F(u'_1, \dots, u'_s)$$

Segue che:

$$\begin{aligned} z + z' &\in F(u_1, \dots, u_r, u'_1, \dots, u'_s) \\ zz' &\in F(u_1, \dots, u_r, u'_1, \dots, u'_s) \\ z^{-1} &\in F(u_1, \dots, u_r, u'_1, \dots, u'_s) \quad \text{se } z \neq 0 \end{aligned}$$

Quindi C' è un sottocampo di \mathbb{C} . Esso è chiuso per operazione di radice quadrata per come è stato costruito. Inoltre $\bar{F} = F$, quindi $\overline{F(u_1, \dots, u_n)} = F(\bar{u}_1, \dots, \bar{u}_n)$ che sta in C' . Segue che $C(z_1, \dots, z_n) \subseteq C'$

$$\Rightarrow C(z_1, \dots, z_n) = C'$$

□

Corollario 3.3.3. *Ogni numero complesso costruibile con riga e compasso a partire da z_1, \dots, z_n è algebrico di grado una potenza di 2 sul sottocampo $F = Q(z_1, \dots, z_n)(\bar{z}_1, \dots, \bar{z}_n)$.*

Dimostrazione. Si consideri il campo $K(u)$ con $u^2 \in K$, allora $|K(u) : K| = 2$ per il teorema 3.2.5. Se utilizziamo la formula dei gradi del teorema 3.2.2 possiamo dedurre che una qualsiasi torre di radici quadrate ha grado una potenza di 2 su F , infatti:

$$\begin{aligned} |F(u_1, \dots, u_n) : F| &= \underbrace{|F(u_1, \dots, u_n) : F(u_1, \dots, u_{n-1})|}_2 \cdot |F(u_1, \dots, u_{n-1}) : F| = \\ &= 2 \cdot \underbrace{|F(u_1, \dots, u_{n-1}) : F(u_1, \dots, u_{n-2})|}_2 \cdot |F(u_1, \dots, u_{n-2}) : F| = \\ &= \dots = \\ &= 2^{n-1} \cdot |F(u_1) : F| \\ &= 2^n \end{aligned}$$

□

3.4 Problemi non risolubili

Trisezione di angoli

Non tutti gli angoli possono essere trisecati usando riga e compasso, in particolare si osserva che l'angolo di 60° non può essere trisecato. La costruzione dell'angolo di 20° a partire da uno di 60° richiede la costruibilità di un punto $P = (\cos 20^\circ, \sin 20^\circ)$ a partire dai punti $P_1 = (0, 0)$,

$P_2 = (1, 0)$ e $P_3 = (\cos 60^\circ, \sin 60^\circ) = (\frac{1}{2}, \frac{1}{2}\sqrt{3})$. Se questo fosse possibile allora si potrebbe costruire il punto $Q = (\cos 20^\circ, 0)$, cioè il piede della perpendicolare da P a P_1P_2 . Per verificare questo è più facile applicare il criterio e il suo corollario. Nel caso osservato sono stati presi in considerazione i numeri complessi $z_1 = 0$, $z_2 = 1$, $z_3 = \frac{1}{2} + \frac{1}{2}\sqrt{3}i$ e il campo $F = \mathbb{Q}(z_1, z_2, z_3, \overline{z_1}, \overline{z_2}, \overline{z_3}) = \mathbb{Q}(\sqrt{-3})$. Applicando il corollario si vede che il successo nella trisecazione dell'angolo di 60° richiede che il $\cos 20^\circ$ abbia grado una potenza di due su F e quindi su \mathbb{Q} dato che $[\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = 2$. Ora si considera l'identità trigonometrica

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

che dà l'uguaglianza $4a^3 - 3a = \frac{1}{2}$ per $a = \cos 20^\circ$. Quindi il numero richiesto a è una radice dell'equazione

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

e quindi il polinomio minimo di a su \mathbb{Q} è un fattore di questo polinomio. Si dimostra in particolare che esso è irriducibile infatti moltiplicando per 2 si ottiene il polinomio

$$8x^3 - 6x - 1 = 0$$

Per il teorema della radici razionali le sue soluzioni potrebbero essere $\{1, -1, \frac{1}{2}, -\frac{1}{2}, \frac{1}{4}, -\frac{1}{4}, \frac{1}{8}, -\frac{1}{8}\}$ ma si dimostra che nessuna di esse è radice del polinomio considerato, perciò si conclude che il polinomio di partenza è irriducibile. Si ha quindi che il grado del polinomio minimo di a su \mathbb{Q} è tre e non una potenza di due.

Si dimostra ora per assurdo che $a = \cos 20^\circ$ non è costruibile con riga e compasso e quindi che l'angolo di 60° non può essere trisecato.

Se per assurdo lo fosse allora si avrebbe che $a \in \mathbb{Q}(\sqrt{-3})(u_1, \dots, u_r)$, torre di radici quadrate, da cui:

$$\begin{aligned} [\mathbb{Q}(\sqrt{-3})(u_1, \dots, u_r) : \mathbb{Q}(\sqrt{-3})] \cdot [\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] &= \\ &= [\mathbb{Q}(\sqrt{-3})(u_1, \dots, u_r) : \mathbb{Q}(a)] \cdot [\mathbb{Q}(a) : \mathbb{Q}] \end{aligned}$$

dove

$$\begin{aligned} [\mathbb{Q}(\sqrt{-3})(u_1, \dots, u_r) : \mathbb{Q}(\sqrt{-3})] &= 2^\alpha \\ [\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] &= 2 \\ [\mathbb{Q}(\sqrt{-3})(u_1, \dots, u_r) : \mathbb{Q}(a)] &= \gamma \\ [\mathbb{Q}(a) : \mathbb{Q}] &= 3, \end{aligned}$$

e sostituendo questi valori si otterrebbe che $3 \cdot \gamma = 2^\alpha \cdot 2$ da cui si avrebbe una contraddizione.

Duplicazione del cubo

Dato un cubo di lato l si vuole trovare un cubo di lato x tale che $x^3 = 2l^3$ cioè $x = \sqrt[3]{2} l$. Per dimostrare che questo problema non è risolubile con riga e compasso bisogna mostrare che il numero $\sqrt[3]{2}$ non è un numero complesso costruibile. Il problema consiste nel costruire $\sqrt[3]{2}$ a partire da $l = 1$ cioè dall'insieme \mathbb{Q} . I punti da cui si vuole partire per la costruzione sono $z_1 = 0$ e $z_2 = 1$ che implica il fatto che il campo $F = \mathbb{Q}$. Si può dimostrare che il numero $\sqrt[3]{2}$ non sta su una torre di radici quadrate infatti:

- $\sqrt[3]{2} \notin \mathbb{Q}$. Se per assurdo $\sqrt[3]{2}$ appartenesse a \mathbb{Q} si avrebbe che $\sqrt[3]{2} = \frac{m}{n}$ con m ed n coprimi. Elevando entrambi i membri al cubo si otterrebbe:

$$2 = \frac{m^3}{n^3} \quad \text{da cui} \quad m^3 = 2n^3$$

perciò m^3 sarebbe pari e così pure m , quindi si avrebbe

$$m = 2k \quad \text{da cui} \quad m^3 = 8k^3.$$

Sostituendo questo valore nell'espressione precedente si otterrebbe

$$8k^3 = 2n^3 \quad \text{da cui si avrebbe} \quad n^3 = 4k^3$$

perciò anche n^3 , e quindi n , sarebbe pari, da cui la contraddizione.

- $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ perchè $x^3 - 2$ è il polinomio minimo infatti, se per assurdo non lo fosse, si avrebbe che $x^3 - 2 = (x - \alpha) \cdot (x^2 + \beta x + \gamma)$ da cui $\sqrt[3]{2} \in \mathbb{Q}$.
- $\sqrt[3]{2} \notin \mathbb{Q}(u_1, \dots, u_r)$ infatti, se per assurdo lo fosse, questo insieme dovrebbe avere grado 2^α su \mathbb{Q} da cui si avrebbe che

$$\left[\mathbb{Q}(u_1, \dots, u_r) : \mathbb{Q}(\sqrt[3]{2}) \right] \cdot \underbrace{\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q} \right]}_3 = 2^\alpha,$$

cioè una contraddizione.

Si conclude quindi che $\sqrt[3]{2}$ non sta su una torre di radici quadrate.

Costruzione di poligoni regolari con p lati, p primo

Questa costruzione richiede che sia costruibile il numero complesso $z = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p} = e^{\frac{i2\pi}{p}}$ ed equivale a costruire su \mathbb{C} la radice p -esima dell'unità, cioè la soluzione del polinomio

$$z^p - 1 = 0$$

$$z^p - 1 = (z - 1) \cdot \underbrace{(z^{p-1} + z^{p-2} + \dots + 1)}_{\text{per il criterio di Eisenstein è irriducibile su } \mathbb{Q}} = 0$$

perciò il polinomio $z^{p-1} + z^{p-2} + \dots + 1$ è il polinomio minimo e da ciò segue che $[\mathbb{Q}(z^p) : \mathbb{Q}] = p - 1$. Quindi una condizione necessaria e sufficiente per la costruibilità con riga e compasso di un poligono regolare con p lati è che $p - 1 = 2^s$ per un qualche s intero non negativo. Questo implica che il poligono regolare con p lati può essere costruito solo per primi p della forma $2^s + 1$ e questo è il motivo per cui l'esagono regolare non può essere costruito con riga e compasso. Si osserva inoltre che una condizione necessaria affinché $2^s + 1$ sia un primo è che $s = 2^t$ per un qualche intero t non negativo. Supponiamo che s sia divisibile per un numero dispari u e che quindi sia $s = uv$, allora dall'identità

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

per qualsiasi intero dispari positivo si avrebbe

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

Quindi $2^s + 1 = 2^{uv} + 1$ non sarebbe un primo e da questo si ottiene la condizione necessaria per la costruibilità dei poligoni regolari con p lati: p deve essere della forma $2^{2^t} + 1$. I primi di questo tipo sono detti *primi di Fermat* e quelli ad oggi conosciuti sono:

$p = 3$	ottenuto da	$t = 0$
$p = 5$	ottenuto da	$t = 1$
$p = 17$	ottenuto da	$t = 2$
$p = 257$	ottenuto da	$t = 3$
$p = 65537$	ottenuto da	$t = 4$

Basandosi sull'evidenza empirica è stato ipotizzato che il numero dei primi di Fermat è finito ed è possibile che la lista precedente sia l'insieme completo. Infatti per $t = 5$ si avrebbe $p = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417$ che non è un primo.

Rettificazione della circonferenza

La prova del fatto che sia impossibile rettificare la circonferenza con riga e compasso è molto difficile. Il problema consiste infatti nel trovare una costruzione per π o $\sqrt{\pi}$ e in passato diede adito ad innumerevoli ed infruttuosi tentativi. Finalmente nel 1770 con Lambert prevalse l'opinione dell'insolvibilità del problema. Egli stesso trovò che π è irrazionale e una dimostrazione rigorosa è dovuta a Legendre (1794). Ovviamente l'irrazionalità di questo numero non è sufficiente in quanto esistono numeri irrazionali che sono costruibili con riga e compasso (come ad esempio $\sqrt{2}$). La dimostrazione dell'impossibilità venne finalmente ottenuta da Lindemann nel 1882. Egli mostrò che π non è trascendente con una dimostrazione altamente complessa.

Bibliografia

- [1] NATHAN JACOBSON, *Basic Algebra I*, W. H. Freeman and Company, New York, 1985.
- [2] JOHN STILLWELL, *Mathematics and Its History*, Springer, 2010.
- [3] FABIO STUMBO, *Costruzioni con riga e compasso*, Dipartimento di Matematica di Ferrara, <http://web.unife.it/utenti/fabio.stumbo/didattica/varie/costruzioni.pdf>.
- [4] A. OSTERMANN, G. WANNER, *Geometry by Its History*, Springer, 2012.
- [5] W. DE GRAAF, S. CICALÒ, *Teoria di Galois*, Aracne Editrice, 2008.
- [6] http://it.wikipedia.org/wiki/Formula_di_Eulero_per_i_poliedri.
- [7] <http://www2.dm.unito.it/paginepersonali/ferrarese/sito%20mostra/4-poliedri/L%27icosaedro.pdf>.
- [8] ILARIA DEL CORSO, *Estensione di campi*, Dipartimento di Matematica di Pisa, http://www.dm.unipi.it/~delcorso/Ilaria%20DEL%20CORSO_files/aritmetica/campi_small.pdf.