

UNIVERSITA' DEGLI STUDI DI TORINO

Facoltà di Scienze Matematiche Fisiche Naturali
Corso di Laurea in Matematica

Tesi di Laurea Triennale

Tre problemi impossibili



Relatore
Prof.ssa **Daniela Romagnoli**
Università di Torino

Laureando
Sebastiano Ferraris

Sessione di marzo 2010
Anno Accademico 2008-2009

“Gli uomini ricercano le cose che ignorano: così in geometria non sulla diagonale, che è nota, si fanno ricerche, ma sulla misura rispetto alle superfici che essa divide; non sul cubo, ma sulla sua reduplicazione. ”
- Platone, Simposio -

Introduzione

Fin da quando frequentavo la scuola elementare sono sempre stato affascinato dal compasso e dalle figure geometriche che con esso si possono disegnare. Il divertimento nella costruzione dei poligoni regolari e una strana passione per il numero sette però mi portarono presto di fronte a una domanda: come mai per quanto ci provassi non riuscivo a costruire un poligono di sette lati? Continuando gli studi scoprii che non ero il solo ad essermi posto questo tipo di problema e che anzi ne esistevano altri tre affini al mio, risalenti all'antichità. La loro storia merita di essere raccontata.

Era l'anno 429 a.C. quando Pericle, celebre stratega, morì durante un'epidemia di peste assieme ad un quarto del popolo ateniese. Durante tale pandemia, per placare l'ira degli dèi che si credeva ne fossero artefici, una delegazione di ateniesi andò ad interpellare l'oracolo di Apollo a Delo. Egli fu chiaro: se i sacerdoti avevano a cuore il futuro di Atene e dei suoi abitanti, allora l'altare cubico del dio della medicina avrebbe dovuto essere raddoppiato, senza che però ne fosse modificata la forma originale. I sacerdoti si misero immediatamente al lavoro e duplicarono la lunghezza degli spigoli del monumento. Inaspettatamente l'epidemia, anziché estinguersi, raggiunse i vertici della sua gravità. Pareva quindi che gli dèi non volessero più ragionare; fu allora interpellato l'uomo che sarà ricordato come l'unico saggio: Platone. Egli sostenne che Apollo avesse voluto punire i sacerdoti per la loro ignoranza, infatti il volume dell'altare cubico era stato moltiplicato per otto e non raddoppiato. A quel punto i migliori geometri, con i loro mezzi, cioè riga e compasso, si misero alla ricerca di una soluzione. Secondo la leggenda fu questa l'origine del problema della **duplicazione del cubo**, noto anche come "problema di Delo". Nonostante gli sforzi, però, nessuno riuscì mai a risolverlo, cioè a trovare la lunghezza del lato che avrebbe reso il volume del cubo doppio di quello iniziale [4].

Durante la stessa epoca, sempre ad Atene, era stato posto un altro problema: **la trisezione dell'angolo**, nel quale si richiede il taglio di un angolo in tre angoli interni di uguale ampiezza [18]. Archimede fu il primo a trovare una soluzione, che prevedeva però l'uso di una riga graduata. Coloro i quali perseverarono nella ricerca di una soluzione con il solo uso della riga non

graduata e del compasso non giunsero mai ad un risultato.

Ecco il terzo celebre problema affine ai due già proposti: **la quadratura del cerchio**. Esso consiste nella ricerca di un procedimento per costruire un quadrato con la stessa area di un cerchio dato, con il solo aiuto di riga e compasso. Analogamente si può considerare il problema di trovare un segmento di lunghezza pari a quella di una circonferenza data. La ricerca della soluzione esatta è stata un inutile sforzo per i matematici dei secoli successivi, fino ad essere considerata la metafora di un'impresa disperata, al punto che Dante, al cospetto della visione divina rappresentata nelle sue terzine, si paragona al geometra che tenta di quadrare il cerchio, aggrappato alla fede nell'esistenza di una soluzione [3]:

*Qual è 'l geometra che tutto s'affige
per misurar lo cerchio, e non ritrova,
pensando, quel principio ond'elli indige,*

*tal era io a quella vista nova:
veder voleva come si convenne
l'imago al cerchio e come vi s'indova;*

*ma non eran da ciò le proprie penne:
se non che la mia mente fu percossa
da un fulgore in che sua voglia venne.*

Rimasi sorpreso nello scoprire che, per più di 2000 anni di storia, gli sforzi per risolvere i tre problemi esposti, nonché la costruzione di alcuni poligoni, come quello di 7 lati che cercai con ostinazione, furono tutti vani. Non solo infatti questi non sono risolubili con il solo uso di riga e compasso, ma la dimostrazione rigorosa dell'impossibilità arrivò solo intorno alla fine del diciannovesimo secolo; tale dimostrazione è l'argomento della mia tesi.

Indice

1	Costruzioni euclidee	1
1.1	Definizioni	1
1.2	Esempi fondamentali	3
1.2.1	Retta perpendicolare ad una retta data	3
1.2.2	Sistema di assi cartesiani	4
1.2.3	Bisettrice di un quadrante	5
1.2.4	Punto medio	7
1.2.5	Retta parallela ad una retta data, per un punto dato	7
1.2.6	Manipolazione di due segmenti	9
1.2.7	Radice quadrata di un segmento dato	13
2	Numeri euclidei	15
2.1	Costruzioni euclidee nel piano reale	15
2.2	Caratterizzazione di \mathfrak{E}	17
2.3	Conseguenze	21
3	Il problema della ciclotomia	23
3.1	Poligoni regolari e numeri complessi	23
3.2	Radici n -esime dell'unità ed estensioni ciclotomiche	24
3.3	Numeri di Fermat	28
3.4	Alcuni esempi	29
3.4.1	Costruzione del decagono e del pentagono	29
3.4.2	Costruzione dell'eptadecagono	31
4	Tre problemi impossibili	35
4.1	Duplicazione del cubo	35
4.2	Trisezione dell'angolo	35
4.3	Trascendenza di e e di π	36
4.4	Quadratura del cerchio	37
4.5	Rettificazione della circonferenza	37

Capitolo 1

Costruzioni euclidee

Per affrontare i “tre problemi classici”, si deve definire formalmente il gesto intuitivo della costruzione di una figura geometrica con il solo aiuto di una riga non graduata e di un compasso. In questo capitolo verranno proposte due definizioni equivalenti di costruzione euclidea ed alcuni esempi rilevanti.

1.1 Definizioni

Definizione 1.1.1. *Dato un piano e una distanza fissata U , una **costruzione euclidea** è una successione (K_0, K_1, \dots, K_n) , i cui elementi possono essere punti, rette, o circonferenze nel piano dato, in modo che siano verificate le seguenti condizioni:*

1. K_0 è un punto iniziale, in posizione arbitraria nel piano e K_1 , un punto a distanza fissata U da K_0 , in direzione arbitraria.
2. Se K_i per $2 \leq i \leq n$ è una retta, allora essa deve passare per due punti K_r, K_s già appartenenti alla successione, ovvero già costruiti, quindi con $r, s < i$.
3. Se K_i per $2 \leq i \leq n$ è una circonferenza, allora deve avere come centro un punto K_c già appartenente alla successione, e come raggio il segmento dato dalla distanza fra due punti K_r e K_s già appartenenti alla successione, ovvero già costruiti, quindi con $c, r, s < i$.
4. Se K_i per $2 \leq i \leq n$ è un punto, allora può essere definito come un punto a distanza fissata U da un altro punto K_a già appartenente alla successione in direzione arbitraria, oppure può essere definito come intersezione fra due circonferenze K_b, K_c già costruite, fra due rette K_d, K_e già costruite, o fra una retta e una circonferenza K_f, K_g già costruite, quindi con $a, b, c, d, e, f, g < i$.

Osservazione 1.1.1. Per poter identificare la tipologia di ogni elemento della costruzione, senza dovere necessariamente usare il diagramma, si propone la seguente notazione per i diversi K_i della successione:

- Se K_i è uno dei due punti iniziali, allora si ha rispettivamente $K_0 := P_0$ e $K_1 := P_1$.
- Se K_i è una retta per due punti K_r e K_s , allora $K_i := R_i(K_r, K_s)$;
- Se K_i è una circonferenza di centro K_c e di raggio il segmento avente per estremi i punti K_r e K_s , allora $K_i := C_i(K_c; \overline{K_r K_s})$;
- Se K_i è un punto di intersezione fra due circonferenze C_a, C_b , oppure di due rette R_a, R_b , oppure di una retta R_a e una circonferenza C_b , allora si ha rispettivamente $K_i := P_i(C_a, C_b)$, $K_i := P_i(R_a, R_b)$ oppure $K_i := P_i(R_a, C_b)$.

Nel caso in cui esista più di una intersezione fra la circonferenza e la retta o fra due circonferenze, allora nella numerazione il primo dei punti sarà quello più a destra, o se sono allineati verticalmente, quello più alto dei due.

La seconda definizione di costruzione euclidea proposta, si avvale della definizione di operazione fondamentale, in cui viene specificata direttamente la convenzione sulle notazioni appena introdotte:

Definizione 1.1.2. Dato un piano \mathcal{P} , un suo punto fissato P_0 e una distanza fissata U , le seguenti possibilità si definiscono **operazioni fondamentali**:

1. Tracciare un punto P_i nel piano a distanza U da un punto P_j già costruito in direzione arbitraria; tale punto sarà indicato con P_i .
2. Tracciare una retta R_i nel piano per due punti P_r, P_s già costruiti; tale retta sarà indicata con $R_i(P_r, P_s)$.
3. Tracciare una circonferenza C_i nel piano, di centro il punto P_c , già costruito e di raggio che ha per estremi i punti P_r, P_s già costruiti; tale circonferenza sarà indicata con $C_i(P_c; \overline{P_r P_s})$.
4. Tracciare un punto P_i nel piano, definito o come intersezione di due circonferenze C_r e C_s , già costruite, o come intersezione di due rette R_r ed P_s già costruite, o come intersezione di una retta e di una circonferenza R_r e C_s già costruite. Tale punto sarà indicato rispettivamente con $P_i(C_r, C_s)$, $P_i(R_r, R_s)$ e $P_i(C_r, R_s)$. Nel caso in cui ci siano due intersezioni fra le figure trattate, allora il primo per numerazione sarà il più a destra oppure se sono allineati verticalmente, il più alto.

Definizione 1.1.3. Una **costruzione euclidea** è una successione di operazioni fondamentali su un piano \mathcal{P} il cui primo elemento è dato dal punto inizialmente fissato P_0 .

1.2 Esempi fondamentali

Nei seguenti sette esempi proposti si elencano le costruzioni euclidee più importanti. Gli ultimi due in particolare saranno di fondamentale importanza nel prossimo capitolo.

1.2.1 Retta perpendicolare ad una retta data

Per costruire una retta perpendicolare ad un'altra retta costruita per i punti iniziali, P_0 e P_1 , si procede nel seguente modo:

1. Si tracci il punto P_1 a distanza U da P_0 in direzione arbitraria.
2. Si tracci la retta $R_2(P_0, P_1)$, passante quindi per i punti P_0 e P_1 .
3. Si tracci la circonferenza $C_3(P_0; \overline{P_0P_1})$, avente centro in P_0 e raggio di lunghezza $\overline{P_0P_1} = U$.
4. Si evidenzi il punto $P_4(C_3, R_2)$, intersezione fra C_3 e R_2 .
5. Si tracci la circonferenza $C_5(P_1; \overline{P_1P_4})$, avente centro in P_1 e raggio di lunghezza $\overline{P_1P_4} = 2U$.
6. Si tracci la circonferenza $C_6(P_4; \overline{P_1P_4})$, avente centro in P_4 e raggio di lunghezza $\overline{P_1P_4} = 2U$.
7. Si evidenzi il punto $P_7(C_5, C_6)$, come prima tra le due intersezioni fra C_5 e C_6 .
8. Si tracci la retta $R_8(P_0, P_7)$, passante per i punti P_0 e P_7 .

La retta $R_8(P_0, P_7)$ è perpendicolare ad $R_2(P_0, P_1)$; la costruzione euclidea appena descritta è data dalla successione

$$S_1 = (P_0, P_1, R_2(P_0, P_1), C_3(P_0; \overline{P_0P_1}), \\ P_4(C_3, R_2), C_5(P_1; \overline{P_1P_4}), C_6(P_4; \overline{P_1P_4}), \\ P_7(C_5, C_6), R_8(P_0, P_7))$$

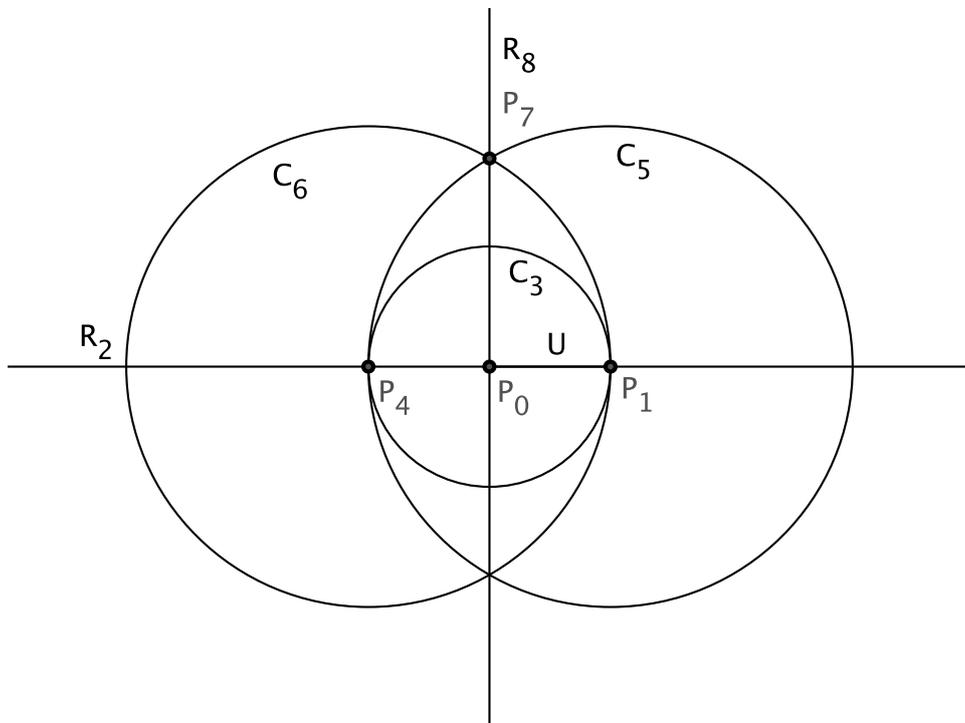


Figura 1.1: Rette perpendicolari

1.2.2 Sistema di assi cartesiani

Per costruire un sistema di assi cartesiani, centrati in P_0 e di unità di misura U data, si procede alla costruzione di due rette perpendicolari descritte dall'esempio precedente; dopodichè ciascuna retta può diventare asse del sistema cartesiano, con una ripartizione in segmenti di lunghezza U attraverso la costruzione di circonferenze successive con centro nell'intersezione fra l'asse stesso e la circonferenza precedente. Si proceda nel seguente modo:

1. Si tracci la costruzione definita dalla successione S_1 dell'esempio precedente.
2. Si rinominino i punti sugli assi, con una notazione più comoda: $P_0 := P_{(0,0)}$ e $P_1 := P_{(1,0)}$.
3. Si costruiscano le circonferenze $C_{(i,0)}(P_{(i,0)}; \bar{U})$ sull'asse orizzontale di centro $P_{(i,0)}$ e di raggio U . Ciascuna di esse formerà due intersezioni, la prima nuova, che sarà chiamata $P_{(i+1,0)}$, e la seconda già costruita precedentemente e chiamata $P_{(i-1,0)}$, per $i = 1 \dots n$
4. Si costruiscano con lo stesso procedimento del punto precedente, i pun-

ti $P_{(0,i)}$ che suddividono l'asse verticale in unità di misura di lunghezza U .

Le due rette perpendicolari $R_2(P_0, P_1)$ e $R_8(P_0, P_7)$ costruite formano gli assi cartesiani cercati. Le successioni di punti $P_{(i,0)}$ e $P_{(0,i)}$, suddividono gli assi nelle unità di misura del sistema. La costruzione euclidea appena descritta è data dalla successione:

$$\begin{aligned}
 S_2 = S_1 \cup & \{C_{(i,0)}(P_{(i,0)}; \bar{U}), P_{(i+1,0)}, | i \in (1, 2 \dots)\} \\
 & \{C_{(0,i)}(P_{(0,i)}; \bar{U}), P_{(i+1,0)} | i \in (1, 2 \dots)\} \cup \\
 & \{C_{(i,0)}(P_{(i,0)}; \bar{U}), P_{(i-1,0)}, | i \in (-1, -2 \dots)\} \cup \\
 & \{C_{(0,i)}(P_{(0,i)}; \bar{U}), P_{(i-1,0)} | i \in (-1, -2 \dots)\}
 \end{aligned}$$

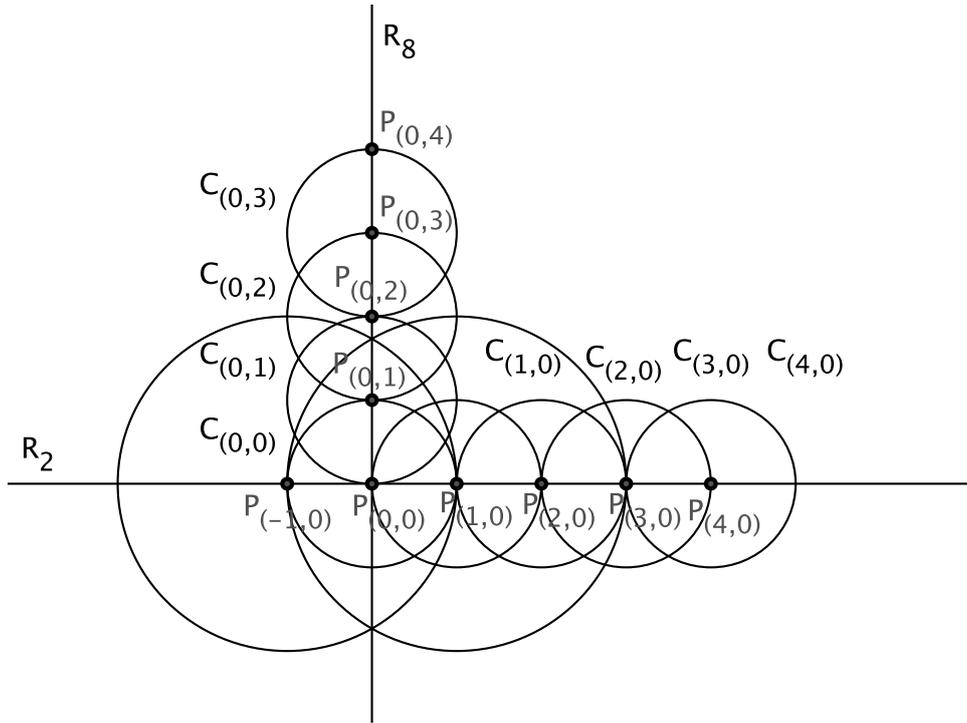


Figura 1.2: Assi cartesiani

1.2.3 Bisettrice di un quadrante

Per costruire la bisettrice dell'angolo formato fra due rette perpendicolari, si può procedere nel seguente modo:

1. Si tracci la successione definita dalla successione S_1 dell'esempio 1.2.1.
2. Si evidenzi il punto $P_9(C_3, R_8)$, come prima intersezione fra C_3 ed R_8 .
3. Si tracci la circonferenza $C_{10}(P_9; \overline{P_1P_4})$.
4. Si evidenzi il punto $P_{11}(C_5, C_{10})$, come prima intersezione fra C_5 e C_{10} .
5. Si tracci infine la retta $R_{12}(P_0, P_{11})$.

La retta $R_{12}(P_0, P_{11})$ è la bisettrice del primo e terzo quadrante cercata. La costruzione euclidea è data da:

$$S_3 = S_1 \cup (P_9(C_3, R_8), C_{10}(P_9; \overline{P_1P_4}), \\ P_{11}(C_5, C_{10}), R_{12}(P_0, P_{11}))$$

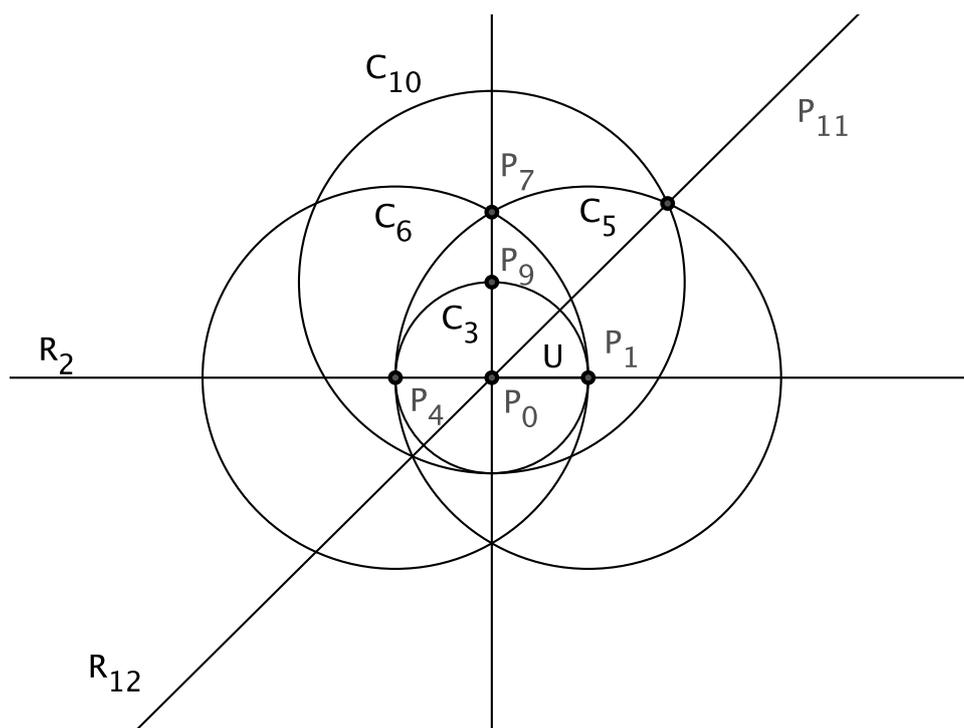


Figura 1.3: Bisettrice

1.2.4 Punto medio

Dato un segmento di estremi P_0 e P_1 , procedendo nel seguente modo è possibile costruire il suo punto medio:

1. Si tracci il punto P_1 a distanza U da P_0 in direzione arbitraria.
2. Si tracci la retta $R_2(P_0, P_1)$.
3. Si tracci la circonferenza $C_3(P_0; \overline{P_0P_1})$.
4. Si tracci la circonferenza $C_4(P_1; \overline{P_1P_0})$.
5. Si evidenzi il primo punto di intersezione $P_5(C_3, C_4)$ fra le due circonferenze appena costruite, secondo l'ordine convenzionale.
6. Si evidenzi il secondo punto di intersezione $P_6(C_3, C_4)$ fra le due circonferenze appena costruite, secondo l'ordine convenzionale.
7. Si tracci la retta $R_7(P_5, P_6)$.
8. Si evidenzi il punto di intersezione $P_8(R_2, R_7)$.

Il punto P_8 è il punto medio del segmento $\overline{P_0P_1}$. La costruzione euclidea è data da:

$$S_4 = (P_0, P_1, R_2(P_0, P_1), C_3(P_0; \overline{P_0P_1}), \\ C_4(P_1; \overline{P_1P_0}), P_5(C_3, C_4), P_6(C_4, C_3), \\ R_7(P_5, P_6), P_8(R_2, R_7))$$

1.2.5 Retta parallela ad una retta data, per un punto dato

Data una retta R_2 passante per P_0 e P_1 , e un punto P_3 esterno alla retta, si richiede la costruzione con riga e compasso della parallela a R_2 passante per P_3 . Per risolvere tale problema, si può applicare due volte la costruzione della perpendicolare ad una retta data, già proposto in 1.2.1, nel seguente modo:

1. Si tracci il punto P_1 a distanza U da P_0 in direzione arbitraria.
2. Si tracci la retta $R_2(P_0, P_1)$, passante quindi per i punti P_0 e P_1 .
3. Si evidenzi con P_3 il punto dato dal problema.
4. Si tracci la circonferenza $C_4(P_3; \overline{P_3P_0})$.
5. Si evidenzi $P_5(R_2, C_4)$, punto di intersezione fra R_2 e C_4 .

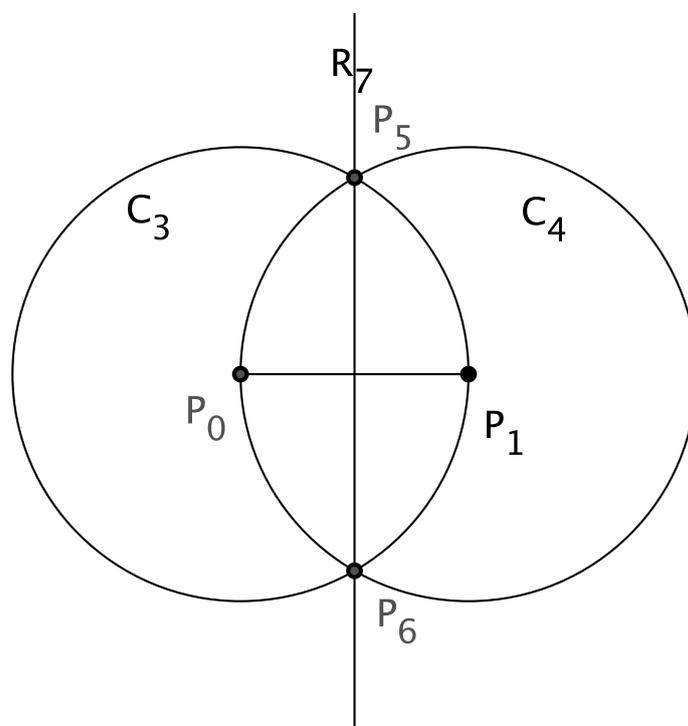


Figura 1.4: Punto medio

6. Si tracci la circonferenza $C_6(P_0; \overline{P_0P_3})$.
7. Si tracci la circonferenza $C_7(P_5; \overline{P_5P_3})$.
8. Si evidenzi $P_8(C_6, C_7)$, punto di intersezione fra C_6 e C_7 .
9. Si tracci la retta $R_9(P_3, P_8)$.
10. Si evidenzi $P_{10}(R_2, R_9)$, punto di intersezione fra R_2 e R_9 .
11. Si tracci $C_{11}(P_3; \overline{P_3P_{10}})$.
12. Si tracci il punto $P_{12}(R_9, C_{11})$.
13. Si tracci la circonferenza $C_{13}(P_{10}; \overline{P_{10}P_{12}})$.
14. Si tracci la circonferenza $C_{14}(P_{12}; \overline{P_{10}P_{12}})$.
15. Si evidenzi $P_{15}(C_{13}, C_{14})$, punto di intersezione fra C_{13} e C_{14} .
16. Si tracci la retta $R_{16}(P_3, P_{15})$.

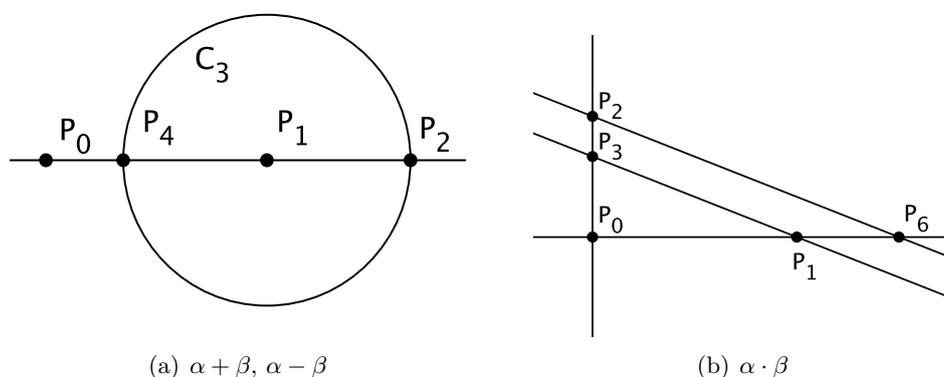


Figura 1.6: Manipolazione di segmenti 1

lunghezza $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ e α/β . Inoltre verrà proposta la costruzione di α^{-1} . Tali possibilità danno al procedimento di costruzione con riga e compasso la struttura di campo.

Somma e differenza dei segmenti dati

Si propone il procedimento per la costruzione di $\alpha + \beta$ e $\alpha - \beta$:

1. Si pongano su una linea retta R i segmenti dati α e β , in questo ordine, con un solo punto di intersezione.
2. Si evidenzino con P_0 e P_1 gli estremi di α ; con P_1 e P_2 gli estremi di β .
3. Si tracci la circonferenza $C_3(P_1; \overline{P_1P_2})$.
4. Si evidenzino con $P_4(C_3, R)$, l'intersezione non ancora tracciata fra la circonferenza e la retta.

A questo punto si ha il segmento P_0P_2 , di lunghezza $\alpha + \beta$, e il segmento P_0P_4 di lunghezza $\alpha - \beta$

Prodotto dei segmenti dati

Si propone il procedimento per la costruzione di $\alpha \cdot \beta$:

1. Dopo aver costruito due rette perpendicolari centrate in P_0 , si pone sull'asse orizzontale il segmento α , con estremi P_0P_1 e sull'asse verticale il segmento β , con estremi P_0P_2 .
2. Si tracci il punto P_3 a distanza U da P_0 , sull'asse verticale.

3. Si tracci la retta $R_4(P_1, P_3)$.
4. Si tracci la retta R_5 parallela ad R_4 e passante per P_2 , usando il procedimento dell'esempio precedente.
5. Si evidenzi il punto P_6 di intersezione fra R_5 e l'asse orizzontale.

Da questa costruzione, applicando il teorema di Talete, si può affermare che

$$\frac{P_0P_6}{\alpha} = \frac{\beta}{U}$$

Dato che U è unità di misura iniziale, si può porre arbitrariamente uguale ad 1, per ottenere

$$\frac{P_0P_6}{\alpha} = \beta$$

Da cui si deduce che il segmento P_0P_6 , è il segmento di lunghezza $\alpha \cdot \beta$ cercato.

Rapporto dei segmenti dati

Si propone il procedimento per la costruzione di α/β :

1. Dopo aver costruito due rette perpendicolari centrate in P_0 , si pone sull'asse orizzontale il segmento α , con estremi P_0P_1 e sull'asse verticale il segmento β , con estremi P_0P_2 .
2. Si tracci il punto P_3 a distanza U da P_0 , sull'asse verticale.
3. Si tracci la retta $R_4(P_1, P_2)$, che congiunge gli estremi di α e β .
4. Si tracci la retta R_5 parallela a R_4 passante per P_3 , usando il procedimento dell'esempio 1.2.5.
5. Si evidenzi il punto P_6 di intersezione fra R_5 e l'asse orizzontale.

Nella costruzione appena descritta vale la seguente proporzione:

$$\frac{P_0P_6}{U} = \frac{\alpha}{\beta}$$

dalla quale, ponendo $U = 1$, si ottiene

$$P_0P_6 = \frac{\alpha}{\beta}$$

Quindi il segmento P_0P_6 , è il segmento di lunghezza α/β cercato.

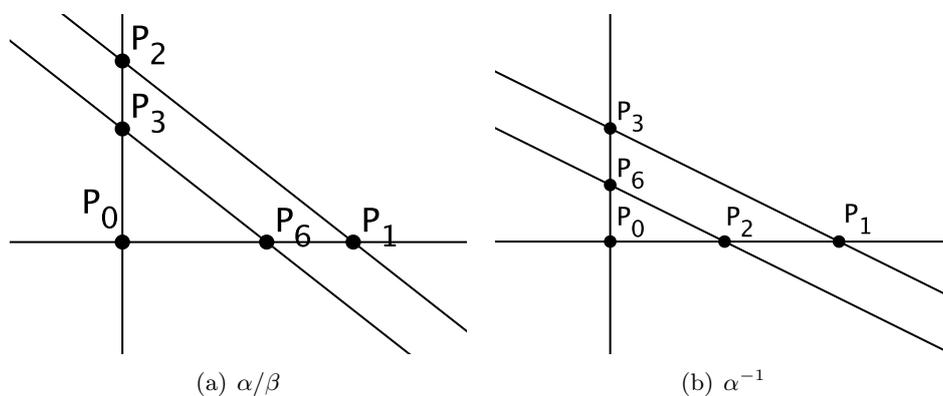


Figura 1.7: Manipolazione di segmenti 2

Inverso del segmento dato

Si propone, per ultimo, il procedimento per la costruzione di α^{-1} .

1. Dopo aver costruito due rette perpendicolari centrate in P_0 , si pone sull'asse orizzontale il segmento α , con estremi P_0P_1 .
2. Si tracci il punto P_2 a distanza U da P_0 , sull'asse orizzontale.
3. Si tracci il punto P_3 a distanza U da P_0 , sull'asse verticale.
4. Si tracci la retta $R_4(P_1, P_3)$, che congiunge gli estremi di α a quelli del segmento unitario verticale.
5. Si tracci la retta R_5 , parallela a R_4 passante per P_2 , usando il procedimento dell'esempio 1.2.5.
6. Si evidenzi il punto P_6 di intersezione fra R_5 e l'asse verticale.

Nella costruzione appena descritta, vale la seguente proporzione:

$$\frac{U}{\alpha} = \frac{P_0P_6}{U}$$

dalla quale, ponendo $U = 1$, si ottiene

$$P_0P_6 = \alpha^{-1}$$

Quindi P_0P_6 è il segmento di lunghezza α^{-1} cercato.

1.2.7 Radice quadrata di un segmento dato

Posto $U = 1$, si vuole costruire un segmento di lunghezza $\sqrt{\alpha}$, dove α è un segmento di lunghezza nota. Si propone la seguente costruzione:

1. Si tracci il punto P_1 a distanza 1 da P_0 in direzione arbitraria.
2. Si costruiscano i due assi cartesiani ortogonali centrati su P_0 con ascisse in direzione P_1 , utilizzando il procedimento visto in 1.2.1 ed ottenendo quindi la costruzione iniziale

$$S_1 = (P_0, P_1, R_2(P_0, P_1), C_3(P_0; \overline{P_0P_1}), \\ P_4(C_3, R_2), C_5(P_1; \overline{P_1P_4}), C_6(P_4; \overline{P_1P_4}), \\ P_7(C_5, C_6), R_8(P_0, P_7))$$

Nella figura proposta compariranno per chiarezza solo gli elementi essenziali P_0, P_1, R_2, P_4, R_8 .

3. Si disegni la circonferenza $C_9(P_0; \alpha)$ di centro P_0 e raggio α .
4. Si evidenzi il punto $P_{10}(C_9, R_2)$, quindi come intersezione fra C_3 e R_2 . E' stato così ottenuto il segmento $\overline{P_4P_{10}}$ di lunghezza $\alpha + 1$.
5. Si trovi il punto medio di $\overline{P_4P_{10}}$, dato da P_{16} , trovato con il seguente procedimento:

$$S'_4 = (C_{11}(P_4, \overline{P_4P_{10}}), C_{12}(P_{10}, \overline{P_{10}P_4}), \\ P_{13}(C_{11}, C_{12}), P_{14}(C_{11}, C_{12}), \\ R_{15}(P_{13}, P_{14}), P_{16}(R_2, R_{15}))$$

analogo a quello usato in 1.2.4. Nella figura, comparirà per chiarezza solo il punto medio risultante del procedimento e la retta R_{15} passante per esso e perpendicolare a P_2 .

6. Si tracci la circonferenza $C_{17}(P_{16}; \overline{P_{16}P_{10}})$, avente quindi come diametro il segmento $\overline{P_4P_{10}}$.
7. Si evidenzi il punto $P_{18}(C_{17}, R_8)$.

Nella costruzione ottenuta, dato che i triangoli $P_4P_0P_{18}$ e $P_0P_{18}P_{10}$ sono simili, sussiste la seguente proporzione:

$$P_4P_0 : P_0P_{18} = P_0P_{18} : P_0P_{10}$$

Cioè

$$1 : P_0P_{18} = P_0P_{18} : \alpha$$

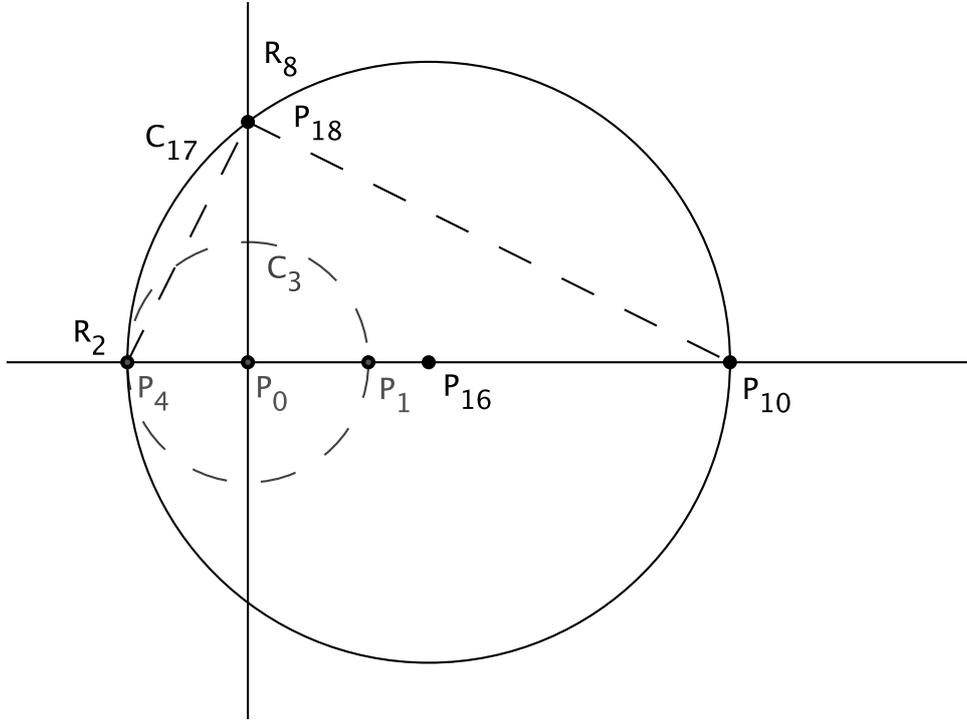


Figura 1.8: Radice quadrata di α

Da cui si ricava che

$$P_0P_{18} = \sqrt{\alpha}$$

Da questa osservazione si deduce un importante risultato: per ogni segmento dato, di lunghezza α , è sempre possibile costruire il segmento di lunghezza $\sqrt{\alpha}$.

La costruzione euclidea del procedimento appena descritto è data da:

$$\begin{aligned}
 S_6 = & (P_0, P_1, R_2(P_0, P_1), C_3(P_0; \overline{P_0P_1}), \\
 & P_4(C_3, R_2), C_5(P_1; \overline{P_1P_4}), C_6(P_4; \overline{P_1P_4}), \\
 & P_7(C_5, C_6), R_8(P_0, P_7), C_9(P_0; \alpha), P_{10}(C_9, R_2) \\
 & C_{11}(P_4, \overline{P_4P_{10}}), C_{12}(P_{10}, \overline{P_{10}P_4}), \\
 & P_{13}(C_{11}, C_{12}), P_{14}(C_{11}, C_{12}), R_{15}(P_{13}, P_{14}), \\
 & P_{16}(R_2, R_{15}), C_{17}(P_{16}; \overline{P_{16}P_{10}}), P_{18}(C_{17}, R_8))
 \end{aligned}$$

Capitolo 2

Numeri euclidei

2.1 Costruzioni euclidee nel piano reale

Ora che si ha una definizione formale delle costruzioni euclidee, intese come successioni di punti, rette e circonferenze fra loro correlate, è necessario esprimere la loro interazione con i punti del piano reale e quindi le proprietà, in termini algebrici, di questa struttura.

Definizione 2.1.1. *L'insieme delle possibili costruzioni euclidee, aventi P_0 e P_1 come punti iniziali, indicato con $\mathcal{E}(P_0, P_1)$, può essere immerso nel piano $\mathbb{R} \times \mathbb{R}$, definendo la seguente funzione:*

$$\mathcal{I} : \mathcal{E}(P_0, P_1) \longrightarrow \mathbb{R} \times \mathbb{R}$$

1. Se $K_i \in \mathcal{E}(P_0, P_1)$ è uno dei due punti iniziali P_0 o P_1 , allora

$$\mathcal{I} : \mathcal{E}(P_0, P_1) \longrightarrow \mathbb{R} \times \mathbb{R}$$

$$P_0 \longmapsto (0, 0)$$

$$P_1 \longmapsto (1, 0)$$

2. Se $K_i \in \mathcal{E}(P_0, P_1)$ è una retta fra due punti K_m e K_n , allora

$$\mathcal{I} : \mathcal{E}(P_0, P_1) \longrightarrow \mathbb{R} \times \mathbb{R}$$

$$K_i \longmapsto R_i(\mathcal{I}(K_m), \mathcal{I}(K_n))$$

Quindi la retta per i due punti K_m, K_n di $\mathcal{E}(P_0, P_1)$ viene mappata da \mathcal{I} nella retta su $\mathbb{R} \times \mathbb{R}$ passante per le immagini dei medesimi punti K_m, K_n , cioè $\mathcal{I}(K_m), \mathcal{I}(K_n)$.

3. Se $K_i \in \mathcal{E}(P_0, P_1)$ è una circonferenza di centro K_c e di raggio il segmento avente per estremi i punti K_r e K_s , allora

$$\mathcal{I} : \mathcal{E}(P_0, P_1) \longrightarrow \mathbb{R} \times \mathbb{R}$$

$$K_i \longmapsto C_i(\mathcal{I}(K_c); \overline{\mathcal{I}(K_r)\mathcal{I}(K_s)})$$

4. Se $K_i \in \mathcal{E}(P_0, P_1)$ è un punto di intersezione fra due circonferenze C_a, C_b , oppure di due rette R_a, R_b , oppure di una retta R_a e una circonferenza C_b , allora si ha rispettivamente

$$\begin{aligned} \mathcal{I} : \mathcal{E}(P_0, P_1) &\longrightarrow \mathbb{R} \times \mathbb{R} \\ K_i &\longmapsto P_i(\mathcal{I}(C_a), \mathcal{I}(C_b)) \\ K_i &\longmapsto P_i(\mathcal{I}(R_a), \mathcal{I}(R_b)) \\ K_i &\longmapsto P_i(\mathcal{I}(R_a), \mathcal{I}(C_b)) \end{aligned}$$

Si ottiene quindi l'insieme delle costruzioni euclidee con unità di misura iniziale pari a 1 immersa nel piano reale. I suoi elementi saranno chiamati **costruzioni euclidee nel piano reale** e saranno indicati con $\mathcal{E}_{\mathbb{R} \times \mathbb{R}}$.

Osservazione 2.1.1. La definizione precedente garantisce l'esistenza di una biiezione fra i punti, le rette e le circonferenze delle costruzioni euclidee, con quelle disegnate sul piano reale.

$$\mathcal{I} : \mathcal{E}(P_0, P_1) \longrightarrow \mathcal{E}_{\mathbb{R} \times \mathbb{R}} \subset \mathbb{R} \times \mathbb{R}$$

Ad ogni punto delle costruzioni euclidee corrisponde quindi un solo punto delle costruzioni euclidee nel piano reale.

Definizione 2.1.2. Un punto Q di $\mathbb{R} \times \mathbb{R}$ che compare in una costruzione euclidea nel piano, cioè tale che $Q \in \mathcal{E}_{\mathbb{R} \times \mathbb{R}}$ è detto **punto euclideo** o costruibile. L'insieme di tutti i punti euclidei sarà indicato con \mathfrak{E} .

Osservazione 2.1.2. L'insieme di punti $\mathbb{Z} \times \mathbb{Z} := \{(m, n) \mid m \in \mathbb{Z}, n \in \mathbb{Z}\}$ è un sottoinsieme di \mathfrak{E} , infatti, come visto in 1.2.2, a partire dai punti iniziali P_0 e P_1 è possibile costruire un sistema di assi cartesiani ortogonali, i cui punti vanno a ricalcare $\mathbb{Z} \times \mathbb{Z}$ nelle costruzioni euclidee nel piano reale.

Si presentano ancora le definizioni di numero reale euclideo e numero complesso euclideo, strettamente correlate con la definizione di punto euclideo:

Definizione 2.1.3. $\gamma \in \mathbb{R}$ è detto **numero reale euclideo** se esiste una costruzione euclidea nel piano reale nella quale compare un segmento di lunghezza $|\gamma|$.

Definizione 2.1.4. $a + ib \in \mathbb{C}$ è detto **numero complesso euclideo** se il corrispondente punto $(a, b) \in \mathbb{R} \times \mathbb{R}$ appartiene ad una costruzione euclidea nel piano reale.

Osservazione 2.1.3. Si osserva che un punto è euclideo se e solo se lo sono le sue rispettive coordinate nel piano reale. Infatti dato P euclideo nel piano reale, è sempre possibile tracciare le rette parallele agli assi (1.2.5), e passanti per $P(a, b)$. Queste rette tagliano sugli assi due segmenti di lunghezza

$|a|$ e $|b|$, quindi a e b sono numeri reali euclidei. Viceversa se a e b sono due numeri euclidei, allora posso sempre costruire i segmenti di lunghezza $|a|$ e $|b|$. Una volta tracciati, rispettivamente sull'asse x e sull'asse y , si ottengono i numeri complessi euclidei a ed ib . Tracciando le rette parallele agli assi, e passanti per a e ib si ottiene il punto di intersezione $P(a, b)$, che è quindi costruibile. Questo significa che si può parlare in modo equivalente di punti euclidei e numeri reali euclidei sul piano reale.

2.2 Caratterizzazione di \mathfrak{E}

Lo scopo del paragrafo precedente è stato la definizione di \mathfrak{E} ; in questo verranno analizzate le sue proprietà, tratte da [9] e [11], e ne verrà data una caratterizzazione algebrica.

Proprietà 2.2.1. *Dato \mathfrak{E} , insieme dei punti euclidei del piano reale, si ha che*

- i) $\mathbb{Z} \subset \mathfrak{E}$
- ii) $\mathbb{Q} \subset \mathfrak{E}$
- iii) \mathfrak{E} è un campo.

Dimostrazione. i) Segue da 2.1.2.

ii) E' sufficiente provare che ogni numero della forma $1/n$ è costruibile. Segue da 1.2.6.

iii) Per provare che \mathfrak{E} è un campo, si deve dimostrare che vale l'implicazione

$$\forall \alpha, \beta \in \mathfrak{E} \Rightarrow \alpha \pm \beta \in \mathfrak{E} \wedge \alpha\beta \in \mathfrak{E} \wedge \alpha/\beta \in \mathfrak{E} \quad (2.1)$$

Segue da 1.2.6.

□

Osservazione 2.2.1. *Da 1.2.7 si ha la seguente importante proposizione per le costruzioni euclidee: se un numero z è costruibile allora lo è anche la sua radice quadrata.*

$$\forall z \in \mathfrak{E} \Rightarrow \sqrt{z} \in \mathfrak{E}$$

Per l'osservazione 2.2.1, e per la proprietà 2.2.1 si può affermare che:

$$\forall q_0 \in \mathbb{Q} \Rightarrow \sqrt{q_0} \in \mathfrak{E}$$

Quindi

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{q_0}) \subset \mathfrak{E}$$

dove $\mathbb{Q}(\sqrt{q_0})$ è il più piccolo campo che estende \mathbb{Q} contenente $\sqrt{q_0}$. Ripetendo il ragionamento precedente, si ha che

$$\forall q_1 \in \mathbb{Q}(\sqrt{q_0}) \Rightarrow q_1 \in \mathfrak{E} \Rightarrow \sqrt{q_1} \in \mathfrak{E}$$

Quindi si può affermare che:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{q_0}) \subset \mathbb{Q}(\sqrt{q_0}, \sqrt{q_1}) \subset \mathfrak{E}$$

Ripetendo ancora il ragionamento, si ha che

$$\forall q_2 \in \mathbb{Q}(\sqrt{q_0}, \sqrt{q_1}) \Rightarrow q_2 \in \mathfrak{E} \Rightarrow \sqrt{q_2} \in \mathfrak{E}$$

Quindi si può affermare che

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{q_0}) \subset \mathbb{Q}(\sqrt{q_0}, \sqrt{q_1}) \subset \mathbb{Q}(\sqrt{q_0}, \sqrt{q_1}, \sqrt{q_2}) \subset \mathfrak{E}$$

In questo modo si può continuare ad estendere il campo \mathbb{Q} indefinitamente, ottenendo sempre un sottocampo di \mathfrak{E} .

L'idea appena presentata serve a caratterizzare ulteriormente \mathfrak{E} , come una successione di estensioni di campi. Inoltre esso fornisce delle informazioni di fondamentale importanza sul grado di queste estensioni; infatti $[\mathbb{Q}(\sqrt{q_0}), \mathbb{Q}] \leq 2$ e $[\mathbb{Q}(\sqrt{q_0}, \sqrt{q_1}), \mathbb{Q}(\sqrt{q_0})] \leq 2$.

Il prossimo teorema¹, enuncia in modo formale quanto detto fino ad ora.

Teorema 2.2.1. *Un numero complesso α è euclideo se e solo se esiste una successione di campi*

$$\mathbb{Q} = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \dots \subseteq \mathbb{E}_{n+1}$$

che soddisfi le due condizioni seguenti:

1. $\alpha \in \mathbb{E}_{n+1}$
2. $[\mathbb{E}_{j+1}, \mathbb{E}_j] \leq 2 \quad j = 0, 1, \dots, n$

Dimostrazione. \Rightarrow) Per ipotesi $\alpha = a+ib$ è euclideo, quindi esiste una costruzione euclidea in cui compare il punto $P = (a, b)$, indicata con $(K_0, K_1, \dots, K_n = P)$.

1. Si costruisce per induzione una successione di campi $\mathbb{Q} = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \dots \subseteq \mathbb{E}_{n+1}$ che soddisfa la condizione 1. Sia quindi \mathbb{E}_j campo già costruito che verifica la condizione 1, allora il successivo \mathbb{E}_{j+1} lo si costruisce nel seguente modo: si considera il corrispondente elemento K_{j+1} della costruzione euclidea.

¹Presentato in: [9] Proposizione 7.1.10 di pag. 345, [11] Teorema 7.4 di pag. 23, [1] Teorema 4.9 pag. 504. Si segue la dimostrazione di [11].

- Se K_{j+1} è una retta o una circonferenza, si pone $\mathbb{E}_{j+1} = \mathbb{E}_j$
- Se K_{j+1} è un punto di coordinate (c, d) , si pone $\mathbb{E}_{j+1} = \mathbb{E}_j(c, d)$, cioè l'estensione di \mathbb{E}_j con i reali (c, d) .
- Quando si è arrivati al penultimo campo, cioè \mathbb{E}_n , lo si estende con $\mathbb{E}_{n+1} = \mathbb{E}_n(i)$, dove i è l'unità immaginaria. Infatti, dato che $K_n = P = (a, b)$, e per il fatto che $i \in \mathbb{E}_{n+1} = \mathbb{E}_n(i) = \mathbb{E}_{n-1}(a, b)(i)$, si ha che $\alpha \in \mathbb{E}_{n+1}$.

Prima di affrontare la dimostrazione del punto 2 si prova che, se K_j è una retta o una circonferenza allora la sua equazione cartesiana può essere scelta a coefficienti in \mathbb{E}_k

- Se K_j è una retta, allora passa per due punti della successione dati da K_s, K_t con $s, t \leq k$. La formula della retta per due punti, nota dalla geometria analitica, si basa sulle coordinate di K_s e K_t , che sono rispettivamente nei campi $\mathbb{E}_s, \mathbb{E}_t$ e quindi nel campo \mathbb{E}_j .
- Se K_j è una circonferenza, analogamente, il centro e gli estremi del segmento di lunghezza del raggio sono dati da K_s, K_t e K_u , con $s, t, u \leq k$. La formula della circonferenza ha come coefficienti elementi nei rispettivi campi $\mathbb{E}_s, \mathbb{E}_t, \mathbb{E}_u$ e quindi nel campo \mathbb{E}_j .

2. Si costruisce per induzione una successione di campi $\mathbb{Q} = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \dots \subseteq \mathbb{E}_{n+1}$ che soddisfa la condizione 2. Si dimostra che $[\mathbb{E}_{j+1}, \mathbb{E}_j] \leq 2$ per $j = 0, 1, \dots, n$. Si distinguono i seguenti tre casi:

- Se K_j è una retta o una circonferenza, si ha dal punto precedente che $\mathbb{E}_j = \mathbb{E}_{j-1}$ da cui segue $[\mathbb{E}_j, \mathbb{E}_{j-1}] = 2$.
- Se K_j è un punto allora può essere intersezione di due rette, di una retta e una circonferenza o di due circonferenze; si distinguono quindi i seguenti sottocasi:
 - i) K_j è intersezione di due rette, K_s, K_t con $s, t \leq j$ allora, per quanto visto prima, si ha che le equazioni cartesiane delle due rette K_s e K_t sono a coefficienti in \mathbb{E}_j . Quindi le coordinate di K_j , ottenute risolvendo il sistema fra le due rette, sono in \mathbb{E}_j . Si ha che $[\mathbb{E}_j, \mathbb{E}_{j-1}] = 1$.
 - ii) K_j è intersezione di una retta K_s e una circonferenza, K_t con $s, t \leq j$, le sue coordinate sono la soluzione del sistema:

$$\begin{cases} K_s : ax + by + c = 0 & a, b, c \in \mathbb{E}_{j-1} \\ K_t : x^2 + y^2 + dx + ey + f = 0 & d, e, f \in \mathbb{E}_{j-1} \end{cases}$$

Per quanto visto prima i coefficienti a, b, c, d, e, f sono tutti in \mathbb{E}_j . Se per esempio $a \neq 0$ (o analogamente $b \neq 0$), per sostituzione si ottiene il sistema :

$$\begin{cases} x = -(b/a)y - (c/a) & a, b, c \in \mathbb{E}_{j-1} \quad a \neq 0 \\ y^2 + ly + m = 0 & l, m \in \mathbb{E}_{j-1} \end{cases}$$

L'equazione $y^2 + ly + m = 0$ può essere risolubile in \mathbb{E}_{j-1} o meno. Si distinguono allora gli ulteriori due sottocasi:

- Se $y^2 + ly + m = 0$ è risolubile in \mathbb{E}_{j-1} (quindi il corrispondente polinomio è riducibile in \mathbb{E}_j), allora si ha che $\mathbb{E}_j = \mathbb{E}_{j-1}$. Cioè $[\mathbb{E}_j, \mathbb{E}_{j-1}] = 1$.
- Se $y^2 + ly + m = 0$ non è risolubile in \mathbb{E}_{j-1} (quindi il corrispondente polinomio, essendo di secondo grado, non è riducibile in \mathbb{E}_{j-1}), allora la soluzione del sistema estenderà il campo \mathbb{E}_{j-1} con il campo \mathbb{E}_j contenente le radici

$$\begin{cases} y_1 = -l - \sqrt{l^2 - 4m} & l, m \in \mathbb{E}_{j-1} \\ y_2 = -l + \sqrt{l^2 - 4m} & l, m \in \mathbb{E}_{j-1} \end{cases}$$

Cioè $\mathbb{E}_j = \mathbb{E}_{j-1}(\sqrt{l^2 - 4m})$. Ma questo implica $[\mathbb{E}_j, \mathbb{E}_{j-1}] = 2$.

- iii) K_j è intersezione di due circonferenze K_s, K_t con $s, t \leq k$. Il ragionamento è analogo al precedente, si ha infatti il sistema:

$$\begin{cases} K_s : x^2 + y^2 + ax + by + c = 0 & a, b, c \in \mathbb{E}_{j-1} \\ K_t : x^2 + y^2 + dx + ey + f = 0 & d, e, f \in \mathbb{E}_{j-1} \end{cases}$$

Che equivale a

$$\begin{cases} K_s : x^2 + y^2 + ax + by + c = 0 & a, b, c \in \mathbb{E}_{j-1} \\ K_t : (a - d)x + (b - e)y + (c - f) = 0 & d, e, f \in \mathbb{E}_{j-1} \end{cases}$$

Riconducibile direttamente al caso precedente.

- L'ultimo passo dell'induzione, cioè quando sono stati costruiti tutti i campi, tranne l'ultimo, e \mathbb{E}_n soddisfa la condizione 2, allora, dato che \mathbb{E}_{n+1} è stato definito come $\mathbb{E}_n(i)$, si ha $[\mathbb{E}_n(i), \mathbb{E}_n] = [\mathbb{E}_{n+1}, \mathbb{E}_n] = 2$.

Quindi la condizione necessaria del teorema è dimostrata. \square

Dimostrazione. \Leftarrow) Per terminare la dimostrazione, si deve ancora verificare che se valgono le condizioni 1 e 2, cioè se

$$\alpha \in \mathbb{E}_{n+1} \supseteq \mathbb{E}_n \supseteq \dots \supseteq \mathbb{E}_1 \supseteq \mathbb{E}_0 = \mathbb{Q}$$

e se

$$[\mathbb{E}_j, \mathbb{E}_{j-1}] \leq 2 \quad j = 1, 2, \dots, n+1$$

allora α è euclideo. Si procede di nuovo per induzione. Sia α_{j-1} elemento di \mathbb{E}_{j-1} , euclideo, e quindi $(j-1)$ -esimo della costruzione euclidea ($K_0, K_1, \dots, K_{j-1} = \beta$). Il punto successivo a α_{j-1} , nella costruzione euclidea, indicato con α_j , appartiene al campo \mathbb{E}_j e, dato che per ipotesi $[\mathbb{E}_j, \mathbb{E}_{j-1}] \leq 2$, α_{j-1} è algebrico su \mathbb{E}_{j-1} di grado 1 o 2^2 . Si hanno quindi i due casi:

- Se il grado di α_{j-1} è 1, allora $\gamma \in \mathbb{E}_j$ e quindi α_{j-1} è euclideo anche su \mathbb{E}_j .
- Se il grado di α_{j-1} è 2, allora verifica una equazione del tipo $x^2 + bx + c = 0$ con $b, c \in \mathbb{E}_{j-1}$. Ma dato $a^2 - 4b$ è sempre possibile costruire un segmento di lunghezze $\sqrt{a^2 - 4b}$, come visto in 1.2.7, quindi $\gamma \in \mathbb{E}_j = \mathbb{E}_{j-1}(\sqrt{a^2 - 4b})$. Questo significa che α_{j-1} è euclideo anche su \mathbb{E}_j .

Tutti i successivi α_k , fino ad arrivare ad α in \mathbb{E}_{n+1} sono euclidei. Quindi la condizione sufficiente del teorema è dimostrata. \square

2.3 Conseguenze

Nel paragrafo precedente è stato caratterizzato \mathfrak{E} come campo che contiene tutti i possibili sottocampi, dati da $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_m)$, in cui si trovano i possibili numeri euclidei. In particolare si ha che un numero reale γ appartiene a \mathfrak{E} solo se appartiene a $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_m)$, per α_i da determinare.

Da queste considerazioni si hanno i seguenti corollari:

Corollario 2.3.1. ³ Se $\alpha \in \mathbb{C}$ è euclideo, allora α è algebrico di grado 2^k per un opportuno naturale k .

Dimostrazione. Tenendo conto della formula $[\mathbb{E}, \mathbb{K}] = [\mathbb{E}, \mathbb{F}][\mathbb{F}, \mathbb{K}]$, si ha, per la successione di campi $\mathbb{Q} = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \dots \subseteq \mathbb{E}_{n+1}$ determinata da α con il procedimento costruttivo enunciato in 2.2.1, $[\mathbb{E}_{n+1}, \mathbb{Q}] = 2^s$ per s opportuno. Quindi si ha che $\alpha \in \mathbb{E}_{n+1}$ è algebrico ed il suo grado divide 2^s cioè equivale a 2^k per qualche k . \square

Osservazione 2.3.1. ⁴ Si ricordi che il grado di una estensione algebrica semplice è uguale al grado del polinomio minimo dell'elemento algebrico mediante il quale si fa l'estensione.

²infatti il grado del polinomio minimo del generico a su \mathbb{K} divide $[\mathbb{F}, \mathbb{K}]$, per \mathbb{F} estensione finita di \mathbb{K}

³Da [11] Corollario 7.5 di pag. 25

⁴Da [11] Esempio 6.9 di pag. 18

Corollario 2.3.2. ⁵ Se un numero reale β è radice di un polinomio irriducibile di grado n che non è una potenza di 2, allora β non è un numero euclideo.

Dimostrazione. Sia β numero reale radice di un polinomio irriducibile $f(x)$ di grado n , allora $f(x)$ è il suo polinomio minimo. Da ciò, segue che $[\mathbb{Q}(\beta), \mathbb{Q}] = n \neq 2^k$, quindi α non può appartenere ad un ampliamento algebrico di grado una potenza di 2, come dovrebbe avvenire se β fosse costruibile. \square

⁵Da [9] Proposizione 7.1.12 di pag. 346

Capitolo 3

Il problema della ciclotomia

In questo capitolo si trova una risposta al problema della ciclotomia, che può essere formulato con la seguente domanda: per quali $n \in \mathbb{N}$ è possibile costruire il poligono regolare di n lati con riga e compasso?

3.1 Poligoni regolari e numeri complessi

Si considera l'insieme delle costruzioni euclidee, immerse nel piano di Gauss tramite

$$\mathcal{I}_c : \mathcal{E}(P_0, P_1) \longrightarrow \mathbb{C}$$

che possiede caratteristiche analoghe a quelle di \mathcal{I} , funzione definita in 2.1.1. Si considerano i poligoni regolari nel piano complesso inscritti nella circonferenza unitaria centrata nell'origine e aventi un vertice nel punto $(1, 0)$. In questo modo tutti i vertici di tali poligoni sono dati da potenze ennesime di numeri complessi e in particolare sono soluzioni di una equazione polinomiale. Per verificare quanto affermato, si considerano da [12] le seguenti:

Proprietà 3.1.1. (*Potenze n -esime di un numero complesso*) Sia $z = (\rho, \theta)$ un numero complesso espresso in coordinate polari e sia $n \in \mathbb{N}$, allora $z^n = (\rho^n, n\theta)$

Proprietà 3.1.2. (*Radici n -esime di un numero complesso*) Sia $z = (\rho, \theta)$ un numero complesso espresso in coordinate polari e sia $n \in \mathbb{N}$, allora l'equazione polinomiale $x^n - z = 0$ ha esattamente n soluzioni distinte le cui espressioni in coordinate polari sono

$$z_k = \left(\sqrt[n]{\rho}, \frac{\theta + 2k\pi}{n} \right) \quad k = 0, 1, \dots, n-1$$

Dalle proprietà appena enunciate, si deduce che, nella circonferenza unitaria le potenze n -esime di $z = (1, 0)$ (soluzioni di $x^n - 1 = 0$), sono date da

$$z_k = \left(1, \frac{2k\pi}{n}\right) \quad k = 0, 1, \dots, n-1$$

che geometricamente rappresentano i vertici di un poligono con n lati inscritto nella circonferenza unitaria, avente un vertice in $(1, 0)$.

Siano ρ e θ coordinate polari del numero complesso z . Esso può essere rappresentato come $z = \rho \cos \theta + i\rho \sin \theta = (\rho, \theta)$, che equivale a $\rho e^{i\theta}$. Per rappresentare il k -esimo vertice di un poligono di n lati, verrà utilizzata la seguente notazione:

$$\delta_n^k := e^{\frac{2k\pi i}{n}} = \cos\left(\frac{2k\pi i}{n}\right) + i \sin\left(\frac{2k\pi i}{n}\right) = \left(1, \frac{2k\pi}{n}\right)$$

che si avvale della formula di Eulero.

Osservazione 3.1.1. *Il problema di costruire un poligono regolare di n lati è equivalente al problema di costruire le soluzioni di $x^n - 1 = 0$. Infatti, come conseguenza della proprietà 3.1.2, l'equazione polinomiale $x^n - 1 = 0$ ha esattamente n soluzioni distinte le cui espressioni in coordinate polari sono:*

$$\delta_n^0 \quad \delta_n^1 \quad \delta_n^2 \quad \dots \quad \delta_n^{n-1}$$

Questa affermazione si dimostra considerando che $\delta_n^j \neq \delta_n^k$, per $j \neq k < n$, e che usando la formula delle potenze n -esime di un numero complesso si ottiene

$$(\delta_n^k)^n = \left(1^n, n \frac{2k\pi i}{n}\right) = (1, 0) = 1$$

3.2 Radici n -esime dell'unità ed estensioni ciclotomiche

In questo paragrafo si vuole stabilire per quali n il numero complesso δ_n^1 è euclideo. Se il secondo vertice δ_n^1 di un poligono di n lati è euclideo, allora il lato del poligono è costruibile e quindi la costruzione di tale poligono è immediata. Dal corollario 2.3.1 si ha che se $\delta_n^1 \in \mathbb{C}$ è euclideo, allora δ_n^1 è algebrico di grado 2^k per un opportuno naturale k . E' quindi necessario studiare il grado dell'estensione in cui si trova δ_n^1 .

Definizione 3.2.1. *Le radici del polinomio $x^n - 1$ sono dette **radici n -esime dell'unità** e si indicano con δ_n^k per $1 \leq k \leq n-1$. Si definisce **ordine** o **periodo**, di una radice n -esima dell'unità δ_n^k il più piccolo intero positivo m tale che $(\delta_n^k)^m = 1$. Inoltre una radice n -esima dell'unità δ_n^k si dice **primitiva**, se il suo ordine è n , cioè $(\delta_n^k)^n = 1$.*

Osservazione 3.2.1. *Ci sono esattamente $\phi(n)$ radici n -esime primitive dell'unità, dove ϕ è la funzione di Eulero. Infatti $(\delta_n^k)^m = 1$ se e solo se $(m, k) = 1$. Se ci fossero divisori comuni fra m e k , allora m non sarebbe più il più piccolo intero positivo a cui elevare δ_n^k per ottenere 1. Si osserva inoltre che δ_n^1 è sempre radice n -esima dell'unità.*

Definizione 3.2.2. *Il campo di spezzamento del polinomio $x^n - 1$ su \mathbb{Q} è detto **estensione ciclotomica**. Si indica con $\mathbb{Q}(\delta_n^k)$ per δ_n^k radice primitiva n -esima dell'unità.*

Osservazione 3.2.2. *Dato che ci sono esattamente $\phi(n)$ radici n -esime primitive dell'unità, l'estensione ciclotomica ha grado $\phi(n)$. Cioè*

$$[\mathbb{Q}(\delta_n^k) : \mathbb{Q}] = \phi(n)$$

Il prossimo teorema comincia a far intravedere per quali fattorizzazioni di n i poligoni regolari di n lati sono costruibili; sarà poi nell'ultimo teorema del paragrafo, la cui condizione necessaria fu dimostrata da Gauss nel 1801 e la condizione sufficiente da Pierre Laurent Wantzel nel 1836¹, che si avrà un criterio effettivo per rispondere al problema della ciclotomia.

Teorema 3.2.1. ² *Un poligono regolare di n lati è costruibile se e solo se esiste un intero positivo h tale che $\phi(n) = 2^h$*

Dimostrazione. Il poligono di n lati è costruibile se e solo se δ_n^1 è costruibile; per 2.2.1, esiste $h \in \mathbb{N}$ tale che

$$[\mathbb{Q}(\delta_n^1) : \mathbb{Q}] = 2^h$$

E per 3.2.2 segue che

$$[\mathbb{Q}(\delta_n^1) : \mathbb{Q}] = \phi(n)$$

Cioè $\phi(n) = 2^h$.

Viceversa, se vale $\phi(n) = 2^h$, allora dall'osservazione 3.2.2 segue che

$$[\mathbb{Q}(\delta_n^1) : \mathbb{Q}] = \phi(n) = 2^h$$

Quindi δ_n^1 è un punto euclideo. Pertanto è euclideo anche il lato del poligono di n lati. □

Lemma 3.2.1. ³ *Se p è un numero primo allora $\phi(p^h) = p^h - p^{h-1}$*

¹Da [5] pag. 879

²Da [9], corollario 7.5.2 pag. 375 .

³Da [9], proposizione 2.8.3 pag. 85 .

Dimostrazione. Non sono coprimi con p^h solo i multipli di p , quindi solo gli elementi $i \cdot p$, per $1 \leq i \leq h - 1$. La cardinalità degli elementi non coprimi con p^h è quindi $h - 1$, cioè $\phi(p^h) = p^h - p^{h-1}$. \square

Lemma 3.2.2. ⁴ *Condizione necessaria (ma non sufficiente) affinché un numero della forma $2^h + 1$ sia primo è che l'esponente deve avere la forma $h = 2^k$ per qualche k intero positivo.*

Dimostrazione. Se per assurdo h contiene un fattore dispari, cioè $h = r(2s + 1)$ per r ed s interi positivi, allora

$$\begin{aligned} 2^h + 1 &= 2^{r(2s+1)} + 1 \\ &= (2^r + 1)((2^r)^{2s} - (2^r)^{2s-1} + (2^r)^{2s-2} - \dots + (2^r)^2 - 2^r + 1) \end{aligned}$$

si separa nel prodotto di due fattori. Non vale la condizione sufficiente (Eulero 1732), infatti

$$2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$$

\square

Teorema 3.2.2. ⁵ *Un poligono di n lati è costruibile se e solo se i primi dispari che compaiono nella fattorizzazione hanno tutti esponente 1 e sono primi del tipo $2^{2^n} + 1$. Cioè la fattorizzazione di n è del tipo*

$$n = 2^k p_1 p_2 \dots p_s$$

con $p_1 p_2 \dots p_s$ numeri distinti del tipo $2^{2^n} + 1$.

Dimostrazione. Da 3.2.1 si ha che un poligono regolare di n -lati è costruibile $\Leftrightarrow \exists h \in \mathbb{N} \mid \phi(n) = 2^h$. Sia $n = p_1^{t_1} p_2^{t_2} \dots p_r^{t_r}$ per p_i primo, e t_i intero positivo, allora da 3.2.1

$$\begin{aligned} \phi(n) &= \phi(p_1^{t_1}) \phi(p_2^{t_2}) \dots \phi(p_r^{t_r}) \\ &= (p_1^{t_1} - p_1^{t_1-1})(p_2^{t_2} - p_2^{t_2-1}) \dots (p_r^{t_r} - p_r^{t_r-1}) \end{aligned}$$

Ora per poter affermare che $\phi(n) = 2^h$, si deve stabilire quando il generico fattore $(p^k - p^{k-1})$ è una potenza di 2. Si osserva che ciò accade solo in due casi: per $p = 2$ e per ogni k intero positivo oppure, se $p \neq 2$, per $k = 1$ e $p - 1 = 2^t$. Ovvero

1. $(p^k - p^{k-1}) = (2^k - 2^{k-1}) = 2^{k-1}(2 - 1) = 2^{k-1}$
2. $(p^k - p^{k-1}) = (p^1 - 1) = 2^t$

⁴Da [9], proposizione 2.9.7 pag. 93 .

⁵Da [9], proposizione 7.5.3 pag. 375.

3. Il problema della ciclotomia

Se tutti i fattori $(p^k - p^{k-1})$ sono del tipo 1, allora $\phi(n) = 2^{k-1}$. Se tutti i fattori $(p^k - p^{k-1})$ sono del tipo 2, allora tali fattori sono del tipo $p-1 = 2^t$, cioè $p = 2^t + 1$ per p che deve essere primo. Per 3.2.2 p è primo se e solo se è del tipo $2^{2^m} + 1$. Nel caso generico, in cui i fattori di n possono essere sia del tipo 1 che del tipo 2, si ha che

$$n = 2^k p_1 p_2 \dots p_s$$

con $p_1 p_2 \dots p_s$ numeri distinti del tipo $2^{2^n} + 1$. □

Dal teorema precedente si ottiene la seguente tabella:

Numero di lati	Fattorizzazione	Costruibilità
3	$2 + 1$	sì
4	2^2	sì
5	$2^2 + 1$	sì
6	$2 \cdot 3$	sì
7		no
8	2^3	sì
9	$3 \cdot 3$	no
10	$2 \cdot 5$	sì
11		no
12	$2^2 \cdot 3$	sì
13		no
14	$2 \cdot 7$	no
15	$3 \cdot 5$	sì
16	2^4	sì
17	$2^4 + 1$	sì
18	$2 \cdot 3^2$	no
19		no
20	$2^2 \cdot 5$	sì
21	$3 \cdot 7$	no
22	$2 \cdot 11$	no
23		no
24	$2^3 \cdot 3$	sì
25	5^2	no

Alla luce degli ultimi risultati, i numeri del tipo $2^{2^n} + 1$ assumono un'importanza particolare. Saranno approfonditi nel prossimo paragrafo.

3.3 Numeri di Fermat

I numeri del tipo $F_n = 2^{2^n} + 1$ sono detti numeri di Fermat, e prendono il nome dal matematico francese Pierre De Fermat (1601-1665).

$n = 0$	$F_0 = 3$
$n = 1$	$F_1 = 5$
$n = 2$	$F_2 = 17$
$n = 3$	$F_3 = 257$
$n = 4$	$F_4 = 65537$
\vdots	\vdots

Come già accenato nel capitolo precedente, non tutti i numeri di Fermat sono necessariamente primi.

Si sa che per $n = 6, 7, 8, 9, 11, 12, 18, 23, 36, 38, 73$, i corrispondenti numeri di Fermat non sono primi. Non è attualmente noto se esistano infiniti numeri di Fermat primi⁶.

Vale il seguente teorema, dal quale segue una definizione ricorsiva dei numeri di Fermat.

Teorema 3.3.1. ⁷ Sia F_n l' n -esimo numero di Fermat, allora, $F_n = F_{n-1}^2 - 2F_{n-1} + 2$ per $n \geq 1$.

Dimostrazione. Si verifica per sostituzione:

$$\begin{aligned}
 F_n &= F_{n-1}^2 - 2F_{n-1} + 2 \\
 &= (2^{2^{n-1}} + 1)^2 - 2(2^{2^{n-1}} + 1) + 2 \\
 &= (2^{2^n} + 2 \cdot 2^{2^{n-1}} + 1) - 2 \cdot 2^{2^{n-1}} - 2 + 2 \\
 &= 2^{2^n} + 1 \\
 &= F_n
 \end{aligned}$$

□

Definizione 3.3.1. (Ricorsiva) I numeri che verificano la ricorsione

$$\begin{aligned}
 F_n &= 3 \\
 F_n &= F_{n-1}^2 - 2F_{n-1} + 2
 \end{aligned}$$

sono detti **Numeri di Fermat**.

⁶Da [11] Osservazione 7.10 di pag. 28.

⁷Da [6] Teorema 2.16 di pag. 139.

Per scoprire quali fra i numeri di Fermat sono primi si riporta l'enunciato dell'interessante teorema di Pepin. Si omette la dimostrazione, che esula dallo scopo di questa tesi.

Teorema 3.3.2. ⁸ $F_n = 2^{2^n} + 1$ è un numero primo se e solo se

$$3^{\frac{F_n-1}{2}} \equiv 1 \pmod{F_n}$$

3.4 Alcuni esempi

Si conclude il capitolo con gli esempi⁹ della costruzione del decagono, del pentagono e dell'eptadecagono, indicati rispettivamente con Θ_{10} , Θ_5 e Θ_{17} .

3.4.1 Costruzione del decagono e del pentagono

Si vuole costruire il decagono regolare inscritto nella circonferenza di centro P_0 e raggio P_0P_1 , in modo che P_1 equivalga al primo vertice δ_{10}^0 .

Si procede nel seguente modo:

1. Si tracci la costruzione S_1 di 1.2.1, per ottenere le rette perpendicolari $R_2(P_0, P_1)$ ed $R_8(P_0, P_7)$.
2. Si evidenzi il punto $P_9(C_3, R_8)$ e si costruisca P_{14} , punto medio del segmento P_0P_9 , con la successione

$$C_{10}(P_9; \overline{P_9P_0}), P_{11}(C_3, C_{10}), P_{12}(C_3, C_{10}), \\ R_{13}(P_{11}, P_{12}), P_{14}(R_8, R_{13})$$

3. Si tracci la circonferenza $C_{15}(P_{14}; \overline{P_{14}P_0})$ di centro P_{14} e raggio $P_{14}P_0$.
4. Si costruisca la retta $R_{16}(P_1, P_{14})$, che intercetta sulla circonferenza $C_{15}(P_{14}; \overline{P_{14}P_0})$ il punto $P_{17}(C_{15}, R_{16})$.
5. Si tracci la circonferenza $C_{18}(P_1; \overline{P_1P_{17}})$. Tale circonferenza interseca C_3 nel punto $P_{19}(C_3, C_{18})$. Il punto appena costruito è δ_{10}^1 , secondo vertice del decagono regolare.
6. Ora che si ha il lato del decagono regolare P_0P_{19} , si costruiscono gli altri vertici del poligono con circonferenze successive di raggio pari al lato, con la seguente successione:

$$C_{20}(P_{19}; \overline{P_{19}P_1}), P_{21}(C_3, C_{20}) = \delta_{10}^2, C_{22}(P_{21}; \overline{P_{21}P_{19}}), P_{23}(C_3, C_{22}) = \delta_{10}^3, \\ C_{24}(P_{23}; \overline{P_{23}P_{21}}), P_{25}(C_3, C_{24}) = \delta_{10}^4, C_{26}(P_{25}; \overline{P_{25}P_{23}}), P_{27}(C_3, C_{26}) = \delta_{10}^5, \\ C_{28}(P_{27}; \overline{P_{27}P_{25}}), P_{29}(C_3, C_{28}) = \delta_{10}^6, C_{30}(P_{29}; \overline{P_{29}P_{27}}), P_{31}(C_3, C_{30}) = \delta_{10}^7, \\ C_{32}(P_{31}; \overline{P_{31}P_{29}}), P_{33}(C_3, C_{32}) = \delta_{10}^8, C_{34}(P_{33}; \overline{P_{33}P_{31}}), P_{35}(C_3, C_{34}) = \delta_{10}^9$$

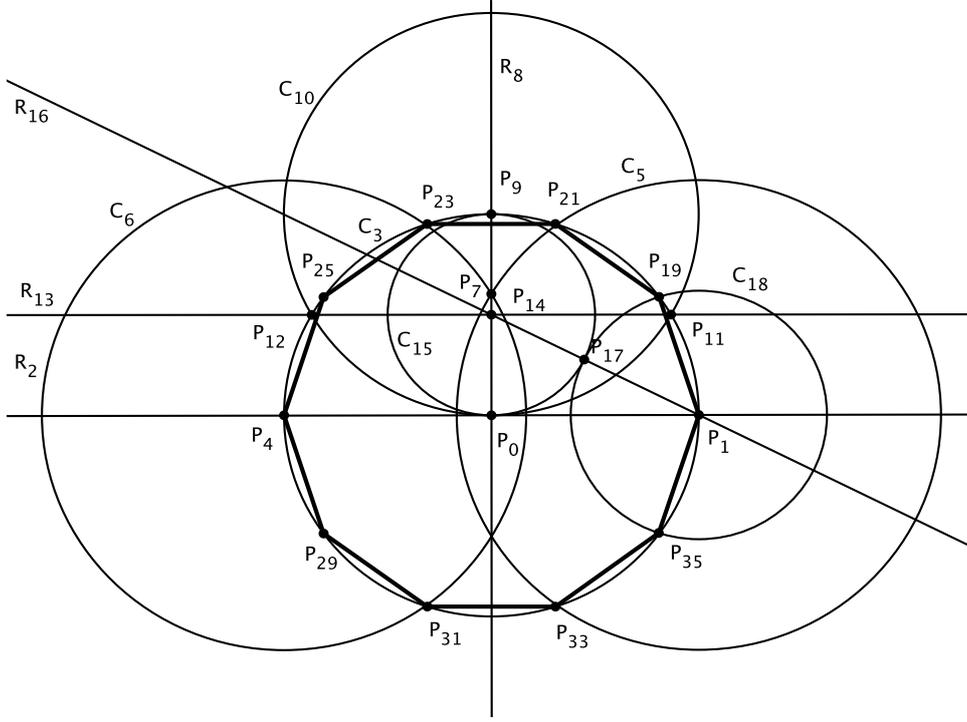


Figura 3.1: Costruzione del decagono

Unendo i passaggi appena elencati, si ottiene la costruzione del decagono:

$$\begin{aligned} \Theta_{10} = & S_1 \cup (P_9(C_3, R_8), C_{10}(P_9; \overline{P_9 P_0}), P_{11}(C_3, C_{10}), \\ & P_{12}(C_3, C_{10}), R_{13}(P_{11}, P_{12}), P_{14}(R_8, R_{13}), C_{15}(P_{14}; \overline{P_{14} P_0}) \\ & R_{16}(P_1, P_{14}), P_{17}(C_{15}, R_{16}), C_{18}(P_1; \overline{P_1 P_{17}}), P_{19}(C_3, C_{18}) \\ & C_{20}(P_{19}; \overline{P_{19} P_1}), P_{21}(C_3, C_{20}), C_{22}(P_{21}; \overline{P_{21} P_{19}}), P_{23}(C_3, C_{22}), \\ & C_{24}(P_{23}; \overline{P_{23} P_{21}}), P_{25}(C_3, C_{24}), C_{26}(P_{25}; \overline{P_{25} P_{23}}), P_{27}(C_3, C_{26}), \\ & C_{28}(P_{27}; \overline{P_{27} P_{25}}), P_{29}(C_3, C_{28}), C_{30}(P_{29}; \overline{P_{29} P_{27}}), P_{31}(C_3, C_{30}), \\ & C_{32}(P_{31}; \overline{P_{31} P_{29}}), P_{33}(C_3, C_{32}), C_{34}(P_{33}; \overline{P_{33} P_{31}}), P_{35}(C_3, C_{34})) \end{aligned}$$

Si ha che $\delta_{10}^0 := P_1$ e $\delta_{10}^{k+1} := P_{19+2k}$ per $k = 0 \dots 8$.

Per costruire il pentagono Θ_5 è sufficiente considerare solo i vertici del tipo δ_{10}^{2k} per $k = 0 \dots 4$ del decagono appena costruito.

⁸Da [14] Teorema 55 di pag. 119.

⁹Da [16], [17] e [21].

3.4.2 Costruzione dell'eptadecagono

Si propone la costruzione dell'eptadecagono regolare inscritto nella circonferenza di centro P_0 e raggio P_0P_1 , in modo che P_1 equivalga al primo vertice δ_{17}^0 :

1. Si tracci la costruzione S_1 di 1.2.1, per ottenere le rette perpendicolari $R_2(P_0, P_1)$ ed $R_8(P_0, P_7)$.
2. Si evidenzi il punto $P_9(C_3, R_8)$. Si costruisca il punto P_{x_1} sul segmento P_0P_9 , tale che $P_0P_{x_1} = \frac{1}{4}P_0P_9$, con il seguente procedimento:

$$P_9(C_3, R_8), C_{10}(P_9; \overline{P_9P_0}), P_{11}(C_3, C_{10}), P_{12}(C_3, C_{10}), R_{13}(P_{11}, P_{12}), \\ P_{14}(R_8, R_{13}), C_{15}(P_{14}; \overline{P_{14}P_0}), C_{16}(P_0; \overline{P_{14}P_0}), P_{17}(C_{15}, C_{16}), \\ P_{18}(C_{15}, C_{16}), R_{19}(P_{17}, P_{18}), P_{20}(R_8, R_{19}) = P_{x_1}$$

3. Si suddivida l'angolo $\angle P_0P_{20}P_1$ in 4 parti uguali, in modo da ottenere il punto P_{x_2} sul segmento P_0P_1 , tale che $\angle P_0P_{20}P_{x_2} = \frac{1}{4}\angle P_0P_{20}P_1$. Si propone il seguente procedimento:

$$R_{21}(P_1, P_{20}), C_{22}(P_{20}; \overline{P_{20}P_{21}}), P_{23}(R_8, C_{22}), C_{24}(P_{23}; \overline{P_{20}P_1}), \\ C_{25}(P_1; \overline{P_{20}P_1}), P_{26}(C_{24}, C_{25}), R_{27}(P_{20}, P_{26}), P_{28}(R_{27}, C_{22}), \\ C_{29}(P_{28}; \overline{P_{28}P_{23}}), C_{30}(P_{23}; \overline{P_{28}P_{23}}), P_{31}(C_{29}, C_{30}), R_{32}(P_{20}P_{31}), \\ P_{33}(R_2, R_{32}) = P_{x_2}$$

4. Si trovi il punto P_{x_3} su R_2 , tale che $\angle P_{33}P_{20}P_{x_3} = \pi/4$. Si procede nel seguente modo:

$$P_{34}(C_{22}, R_{32}), P_{35}(C_{22}, R_{32}), C_{36}(P_{35}; \overline{P_{34}P_{35}}), C_{37}(P_{34}; \overline{P_{34}P_{35}}), \\ P_{38}(C_{36}, C_{37}), R_{39}(P_{38}, P_{20}), P_{40}(R_{39}, C_{22}), C_{41}(P_{40}; \overline{P_{40}P_{35}}), \\ C_{42}(P_{35}; \overline{P_{40}P_{35}}), P_{43}(C_{41}, C_{42}), R_{44}(P_{43}, P_{20}), P_{45}(R_{44}, R_2) = P_{x_3}$$

5. Si costruisca la circonferenza avente per diametro P_1P_{45} , con il seguente procedimento:

$$C_{46}(P_{45}; \overline{P_{45}P_1}), C_{47}(P_1; \overline{P_{45}P_1}), P_{48}(C_{46}, C_{47}), P_{49}(C_{46}, C_{47}), \\ R_{50}(P_{48}, P_{49}), P_{51}(R_{50}, R_2), C_{52}(P_{51}; \overline{P_{51}P_1})$$

6. Si evidenzi il punto $P_{53}(C_{52}, R_8)$ che il cerchio C_{52} appena costruito taglia sul segmento P_0P_9 della retta R_8 .
7. Si costruisca la circonferenza $C_{54}(P_{33}; \overline{P_{33}P_{53}})$ avente per centro P_{33} e per raggio $P_{33}P_{53}$, si evidenzi il punto che essa taglia sul segmento P_0P_1 con $P_{55}(C_{54}, R_2)$.

8. La perpendicolare ad R_2 passante per l'ultimo punto costruito P_{55} interseca la circonferenza C_3 nel terzo vertice δ_{17}^3 dell'eptadecagono. Si procede alla costruzione di tale vertice nel seguente modo:

$$C_{56}(P_{55}; \overline{P_{55}P_{33}}), P_{57}(R_2, C_{56}), C_{58}(P_{33}; \overline{P_{37}P_{33}}), C_{59}(P_{37}; \overline{P_{37}P_{33}}), \\ P_{60}(C_{58}, C_{59}), R_{61}(P_{55}, P_{60}), P_{62}(R_{61}, C_3) = \delta_{17}^3$$

9. Il vertice appena costruito consentirà di ricavare tutti gli altri, con la seguente successione di circonferenze e di punti:

$$C_{63}(P_{62}; \overline{P_{62}P_1}), P_{64}(C_3, C_{63}) = \delta_{17}^6, C_{65}(P_{64}; \overline{P_{64}P_{62}}), P_{66}(C_3, C_{65}) = \delta_{17}^9, \\ C_{67}(P_{66}; \overline{P_{66}P_{64}}), P_{68}(C_3, C_{67}) = \delta_{17}^{12}, C_{69}(P_{68}; \overline{P_{68}P_{66}}), P_{70}(C_3, C_{69}) = \delta_{17}^{15}, \\ C_{71}(P_{70}; \overline{P_{70}P_{68}}), P_{72}(C_3, C_{71}) = \delta_{17}^1, C_{73}(P_{72}; \overline{P_{72}P_{70}}), P_{74}(C_3, C_{73}) = \delta_{17}^4, \\ C_{75}(P_{74}; \overline{P_{74}P_{72}}), P_{76}(C_3, C_{75}) = \delta_{17}^7, C_{77}(P_{76}; \overline{P_{76}P_{74}}), P_{78}(C_3, C_{77}) = \delta_{17}^{10}, \\ C_{79}(P_{78}; \overline{P_{78}P_{76}}), P_{80}(C_3, C_{79}) = \delta_{17}^{13}, C_{81}(P_{80}; \overline{P_{80}P_{78}}), P_{82}(C_3, C_{81}) = \delta_{17}^{16}, \\ C_{83}(P_{82}; \overline{P_{82}P_{80}}), P_{84}(C_3, C_{83}) = \delta_{17}^2, C_{85}(P_{84}; \overline{P_{84}P_{82}}), P_{86}(C_3, C_{85}) = \delta_{17}^5, \\ C_{87}(P_{86}; \overline{P_{86}P_{84}}), P_{88}(C_3, C_{87}) = \delta_{17}^8, C_{89}(P_{88}; \overline{P_{88}P_{86}}), P_{90}(C_3, C_{89}) = \delta_{17}^{11}, \\ C_{91}(P_{90}; \overline{P_{90}P_{88}}), P_{92}(C_3, C_{91}) = \delta_{17}^{14}$$

Unendo i passaggi appena elencati, si ottiene la costruzione dell'eptadecagono:

$$\begin{aligned}
 \Theta_{17} = & S_1 \cup (P_9(C_3, R_8), C_{10}(P_9; \overline{P_9 P_0}), P_{11}(C_3, C_{10}), P_{12}(C_3, C_{10}), \\
 & R_{13}(P_{11}, P_{12}), P_{14}(R_8, R_{13}), C_{15}(P_{14}; \overline{P_{14} P_0}), C_{16}(P_0; \overline{P_0 P_{14}}), \\
 & P_{17}(C_{15}, C_{16}), P_{18}(C_{15}, C_{16}) R_{19}(P_{17}, P_{18}), P_{20}(R_8, R_{19}), R_{21}(P_1, P_{20}), \\
 & C_{22}(P_{20}; \overline{P_{20} P_{21}}), P_{23}(R_8, C_{22}), C_{24}(P_{23}; \overline{P_{20} P_1}), C_{25}(P_1; \overline{P_{20} P_1}), \\
 & P_{26}(C_{24}, C_{25}), R_{27}(P_{20}, P_{26}), P_{28}(R_{27}, C_{22}), C_{29}(P_{28}; \overline{P_{28} P_{23}}), \\
 & C_{30}(P_{23}; \overline{P_{28} P_{23}}), P_{31}(C_{29}, C_{30}), R_{32}(P_{20} P_{31}), P_{33}(R_2, R_{32}), P_{34}(C_{22}, R_{32}), \\
 & P_{35}(C_{22}, R_{32}), C_{36}(P_{35}; \overline{P_{34} P_{35}}), C_{37}(P_{34}; \overline{P_{34} P_{35}}), P_{38}(C_{36}, C_{37}), \\
 & R_{39}(P_{38}, P_{20}), P_{40}(R_{39}, C_{22}), C_{41}(P_{40}; \overline{P_{40} P_{35}}), C_{42}(P_{35}; \overline{P_{40} P_{35}}), \\
 & P_{43}(C_{41}, C_{42}), R_{44}(P_{43}, P_{20}), P_{45}(R_{44}, R_2), C_{46}(P_{45}; \overline{P_{45} P_1}), \\
 & C_{47}(P_1; \overline{P_{45} P_1}), P_{48}(C_{46}, C_{47}), P_{49}(C_{46}, C_{47}), R_{50}(P_{48}, P_{49}), P_{51}(R_{50}, R_2), \\
 & C_{52}(P_{51}; \overline{P_{51} P_1}), P_{53}(C_{52}, R_8), C_{54}(P_{33}; \overline{P_{33} P_{53}}), P_{55}(C_{54}, R_2), \\
 & C_{56}(P_{55}; \overline{P_{55} P_{33}}), P_{57}(R_2, C_{56}), C_{58}(P_{33}; \overline{P_{37} P_{33}}), \\
 & C_{59}(P_{37}; \overline{P_{37} P_{33}}), P_{60}(C_{58}, C_{59}), R_{61}(P_{55}, P_{60}), P_{62}(R_{61}, C_3) \\
 & C_{63}(P_{62}; \overline{P_{62} P_1}), P_{64}(C_3, C_{63}), C_{65}(P_{64}; \overline{P_{64} P_{62}}), P_{66}(C_3, C_{65}), \\
 & C_{67}(P_{66}; \overline{P_{66} P_{64}}), P_{68}(C_3, C_{67}), C_{69}(P_{68}; \overline{P_{68} P_{66}}), P_{70}(C_3, C_{69}), \\
 & C_{71}(P_{70}; \overline{P_{70} P_{68}}), P_{72}(C_3, C_{71}), C_{73}(P_{72}; \overline{P_{72} P_{70}}), P_{74}(C_3, C_{73}), \\
 & C_{75}(P_{74}; \overline{P_{74} P_{72}}), P_{76}(C_3, C_{75}), C_{77}(P_{76}; \overline{P_{76} P_{74}}), P_{78}(C_3, C_{77}), \\
 & C_{79}(P_{78}; \overline{P_{78} P_{76}}), P_{80}(C_3, C_{79}), C_{81}(P_{80}; \overline{P_{80} P_{78}}), P_{82}(C_3, C_{81}), \\
 & C_{83}(P_{82}; \overline{P_{82} P_{80}}), P_{84}(C_3, C_{83}), C_{85}(P_{84}; \overline{P_{84} P_{82}}), P_{86}(C_3, C_{85}), \\
 & C_{87}(P_{86}; \overline{P_{86} P_{84}}), P_{88}(C_3, C_{87}), C_{89}(P_{88}; \overline{P_{88} P_{86}}), P_{90}(C_3, C_{89}), \\
 & C_{91}(P_{90}; \overline{P_{90} P_{88}}), P_{92}(C_3, C_{91}))
 \end{aligned}$$

Si ha che $\delta_{17}^0 := P_1$, $\delta_{17}^3 := P_{62}$ e $\delta_{17}^{4k+1} := P_{64+2k}$ per $k = 0 \dots 15$.

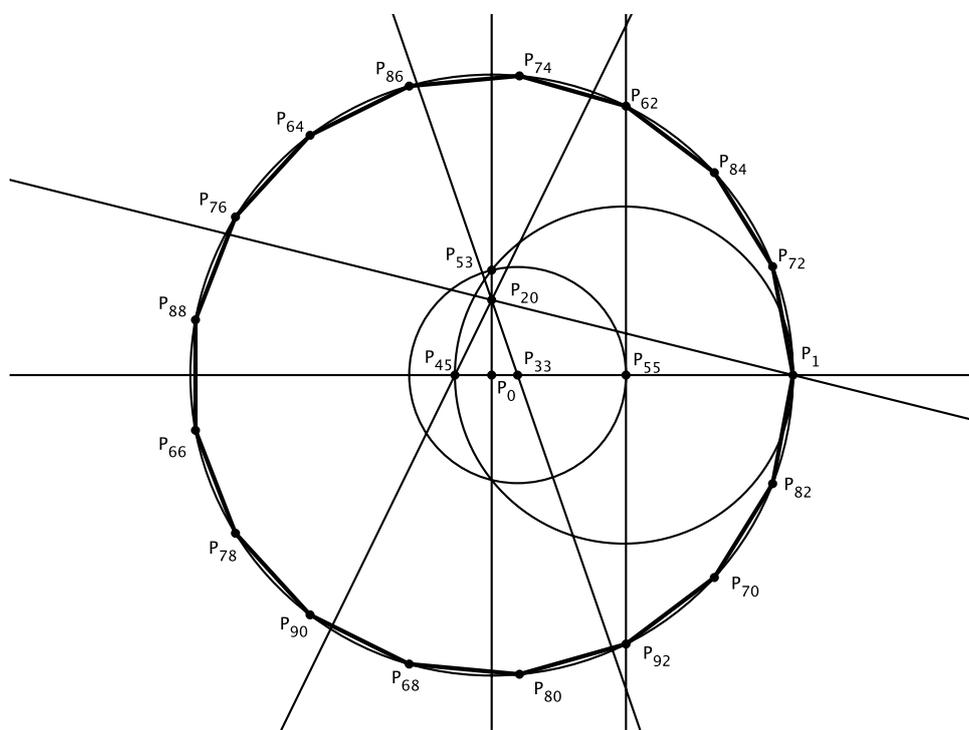


Figura 3.2: Costruzione dell'eptadecagono

Capitolo 4

Tre problemi impossibili

In quest'ultimo capitolo si affronta il tema centrale di questa tesi. Si hanno infatti le basi per dimostrare rigorosamente che, con il solo uso di riga e compasso, non è possibile trovare il lato di un cubo avente volume doppio di un cubo dato, suddividere un angolo dato in tre angoli uguali e costruire un quadrato di area uguale a quella di un cerchio dato.

4.1 Duplicazione del cubo

Dato un cubo di lato l e di volume $l^3 = v$, per costruirne uno di volume doppio di lato l' , si deve tracciare un segmento che soddisfi la seguente equazione

$$l'^3 = 2v$$

Quindi $l' = \sqrt[3]{2v}$. Possiamo sempre porre $l = 1$ utilizzando l'unità di misura l come il segmento di lunghezza P_0P_1 , da cui si ha $v = 1$, e quindi

$$l' = \sqrt[3]{2}$$

Questo implica che l' soddisfa il polinomio $x^3 - 2$ irriducibile su \mathbb{Q} ; per il corollario 2.3.2 l' non è costruibile.

4.2 Trisezione dell'angolo

Non tutti gli angoli dati possono essere sempre trisecati: sia ad esempio¹ $\alpha = 3\theta = \pi/3$, allora costruire l'angolo di $\theta = \pi/9$ equivale a costruire $\cos(\pi/9)$. Dalle note relazioni trigonometriche si ottiene

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

¹Da [9] pag. 347.

Da cui per $3\theta = \pi/3$, si ha che

$$1/2 = 4\cos^3(\pi/9) - 3\cos(\pi/9)$$

Quindi $\cos(\pi/9)$ soddisfa il polinomio

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

irriducibile su \mathbb{Q} , di grado 3. Quindi per il corollario 2.3.1 $\cos(\pi/9)$ non è costruibile.

Alcuni angoli possono essere trisecati; ad esempio quello di $(3/4)\pi$ formato dalle semirette r_1 ed r_2 . Con il procedimento 1.2.1 e 1.2.3 è possibile costruire prima una retta s_1 perpendicolare a r_1 e poi la bisettrice di r_1 ed s_1 , indicata con s_2 . In questo modo l'angolo fra r_1 ed r_2 è trisecato dalle rette s_1 ed s_2 .

4.3 Trascendenza di e e di π

La necessità di determinare se un dato numero sia algebrico, cioè radice di un polinomio a coefficienti interi, o viceversa trascendente, si presentò per la prima volta a metà del 1800 da Joseph Liouville (Saint Omer, 1809 - Parigi, 1882). Egli infatti dimostrò l'esistenza dei numeri trascendenti, affermando che ogni numero della forma

$$\frac{a_1}{10} + \frac{a_1}{10^{2!}} + \frac{a_1}{10^{3!}} + \dots$$

con a_i numeri interi arbitrari, compresi fra 0 e 9, è trascendente.

A questo punto si presenta il secondo protagonista della storia dei numeri trascendenti, Charles Hermite (Dieuze, 1822 - Parigi, 1901), il quale, tentando di dimostrare la trascendenza di π , giunse nel 1873 a dimostrare la trascendenza del numero di Nepero. Dopo questo successo scrisse in una lettera indirizzata al collega tedesco Carl Wilhelm Brochardt (Berino, 1817 - Ruedesdorf 1880) le seguenti parole:²

“Non oso tentare di dimostrare la trascendenza di π . Se altri ci riusciranno, nessuno sarà più felice di me per il loro successo, ma credimi, caro amico, ciò non mancherà di costare loro qualche sforzo.”

L'artefice della felicità di Hermite, fu Carl Louis Ferdinand von Lindemann (Hannover, 1852 - Gottinga, 1939), che nel 1882 scoprì la trascendenza di π . Egli arrivò a dimostrare che se x_1, x_2, \dots, x_n sono numeri algebrici distinti, reali o complessi, e se p_1, p_2, \dots, p_n sono numeri algebrici non tutti nulli, allora la somma

$$p_1 e^{x_1} + p_2 e^{x_2} + \dots + p_n e^{x_n}$$

²Da [5] pag. 1146.

è sempre diversa da zero. Da tale fatto, per $n = 2$, $p_1 = p_2 = 1$ e $x_2 = 0$ si ha

$$e^{x_1} + 1 \neq 0$$

per ogni x_1 algebrico. Ma per la formula di Eulero $e^{i\pi} + 1 = 0$ si ha che $i\pi$ deve essere trascendente, e dato che i è algebrico, si ha che π deve essere trascendente³. Tale dimostrazione di teoria dei numeri, assieme alla teoria dei campi applicata alle costruzioni con riga e compasso, ha risolto definitivamente il problema della quadratura del cerchio che aveva tenuto occupati i matematici di ogni epoca.

4.4 Quadratura del cerchio

Preso un cerchio di raggio r e area $a = \pi r^2$, si vuole costruire un quadrato della stessa area. Possiamo sempre porre $r = 1$ utilizzando l'unità di misura r come il segmento di lunghezza P_0P_1 da cui $a = \pi$. Per risolvere il problema, si deve allora costruire un segmento di lunghezza $\sqrt{\pi}$ ma dato che, come visto in 4.3, π è trascendente, si ha che non appartiene a nessun ampliamento di \mathbb{Q} avente grado una potenza di due. Non è quindi costruibile.

4.5 Rettificazione della circonferenza

In analogia con il problema 4.4 sulla quadratura del cerchio, si può chiedere di risolvere con riga e compasso il seguente problema: data una circonferenza di raggio r e lunghezza $h = 2\pi r$ si richiede la costruzione di un segmento di lunghezza pari ad h . Possiamo sempre porre $r = 1$ utilizzando l'unità di misura r come il segmento di lunghezza P_0P_1 , da cui si ha $h = 2\pi$. Ma anche in questo caso, come nel precedente, il segmento di lunghezza 2π non è costruibile, in virtù della trascendenza di π .

³Per la dimostrazione completa della trascendenza di e e π , vedere ad esempio [15] Teorema 6.4 di pag. 72, oppure [2] pag. 6.

Appendice

I lettori di questa tesi si saranno chiesti come mai così tanti matematici hanno trascorso molto tempo a cercare una soluzione dei tre problemi classici, usando esclusivamente riga e compasso, nonostante avessero a disposizione una soluzione trovata con mezzi più moderni. In queste poche righe, vorrei provare a spiegare che la loro non è stata solo la ricerca della soddisfazione personale, ma è conseguenza di motivazioni filosofiche e inaspettatamente pratiche.

Come è noto, negli Elementi di Euclide, la riga e il compasso sono alla base di un sistema assiomatico, che una volta finito nelle mani dei matematici successivi è stato ammirato per la sua forma, eleganza e per la sua completezza.

In verità le lacune degli Elementi sono molteplici; per esempio nella costruzione del triangolo equilatero si usa una proprietà che non viene mai né dimostrata né espressa chiaramente, cioè che due circonferenze, con centro sui diversi estremi di un segmento e aventi per raggio il segmento stesso, abbiano intersezione non vuota [8].

Basandosi sull'osservazione di questa ed altre lacune, lo studioso Lucio Russo [13], sostiene che gli Elementi non sono altro che una sorta di manuale di istruzioni per utilizzare il più potente calcolatore dell'epoca: la riga e il compasso. L'idea che ogni figura geometrica pensabile sia costruibile e quindi misurabile direttamente con questi due oggetti ci porterebbe a credere che i greci avessero sviluppato un sistema completo, elegante e soprattutto definitivo.

A questo punto l'impossibilità di risolvere i tre problemi classici, arrivata per via algebrica, ha dimostrato la necessità di affrontare nuovi orizzonti. Ha dato quindi un contributo fondamentale a rendere, già nella seconda metà dell'ottocento, non del tutto soddisfacente la visione della geometria fornita dall'opera di Euclide.

Bibliografia

- [1] Michael Artin, *Algebra*, Prentice Hall of India, New Delhi 2007
- [2] Alan Baker, *Transcendental Number theory*, Cambridge univesity press 1990, prima ed. 1975.
- [3] Dante Alighieri, *La Divina Commedia*, Einaudi 1954.
- [4] Carl B. Boyer, *Storia della matematica*, Mondadori 2005, prima ed. 1976.
- [5] Morris Kline *Storia del pensiero matematico, dal settecento ad oggi*, volume secondo, Einaudi editore 1991.
- [6] Thomas Koshy, *Elementary Number Theory with applications*, Accademic Press, Elzevier, 2007.
- [7] Mario Livio, *L'equazione impossibile*, BUR 2007, prima ed. 2006.
- [8] Donald O'Shea, *La congettura di Poincarè*, BUR, Milano 2007.
- [9] Giulia Maria Piacentini Cattaneo, *Algebra, un approccio algoritmico*, Zanichelli 2007, prima ed. 1996.
- [10] Platone, *Dialoghi*.
- [11] Claudio Procesi, *Elementi di teoria di Galois*, Zanichelli 2008, prima ed. 1977.
- [12] Margherita Roggero, *Appunti ed esercizi di Matematica Discreta*, Quaderni didattici dell'Università di Torino, 2005.
- [13] Lucio Russo, *La rivoluzione dimenticata: il pensiero scientifico greco e la scienza moderna*, Feltrinelli Milano 1997.
- [14] Daniel Shanks *Solved and unsolved problems in Number Theory* , AMS 1993, prima ed. 1962
- [15] Ian Stewart, *Galois Theory*, Chapman and Hall 1973, prima ed. 2006.

BIBLIOGRAFIA

- [16] Dal Web: sito della Wolfram Research, pagina sulla costruzione dell'eptadecagono:

<http://mathworld.wolfram.com/Heptadecagon.html>

- [17] Dal Web: sito del prof. Lorenzo Roi, pagina sulla costruzione del decagono e dell'eptadecagono:

<http://www.lorenzoroi.net/geometria/Poligoni.html>

- [18] Da Wikipedia, sulla trisezione dell'angolo:

http://it.wikipedia.org/wiki/Trisezione_dell'angolo

- [19] Da Wikipedia, sul problema di Delo:

http://it.wikipedia.org/wiki/Problema_di_Delo

- [20] Da Wikipedia, sulla quadratura del cerchio:

http://it.wikipedia.org/wiki/Quadratura_del_cerchio

- [21] Da Wikipedia, sulla costruzione dell'eptadecagono:

<http://it.wikipedia.org/wiki/Eptadecagono>