

# POTENZE e RADICI in C

più altri argomenti interessanti  
di Leonardo Calconi

Chi ha fretta e non vuole perdersi in letture noiose può limitarsi a dare un'occhiata a questa tabella:

$C\_Exp$	$n$	$p+qi$	$i$
$a$	$a^n$	$a^p e^{(iq \ln a)}$	$e^{i \ln a}$
$z$	$\rho^n e^{in\theta}$	$\rho^p e^{-\theta q} e^{[i(q \ln \rho + \theta p)]}$	$\rho e^{-\theta}$
$i$	$e^{\frac{i n \pi}{2}}$	$e^{\frac{\pi}{2}(pi-q)}$	$e^{-\frac{\pi}{2}}$
$C\_nRoots$	$ReU\_nRoots$	$ImU\_nRoots$	$U\_pRoots$
$z_k = \rho^{\frac{1}{n}} e^{i \left( \frac{\theta + 2k\pi}{n} \right)}$	$z_k = e^{i \left( \frac{2k\pi}{n} \right)}$	$z_k = e^{i \left( \frac{\pi + 4k\pi}{2n} \right)}$	$\varphi(n) = n \prod_{p n} \left( 1 - \frac{1}{p} \right)$

e chi non ha problemi con le rappresentazioni esponenziali può andare direttamente a pagina 7. Non ho perso tempo a diluire la minestra con informazioni e dimostrazioni elementari sui numeri complessi mentre ne ho dedicato un po' di più agli esempi. Ho curato l'impaginazione in modo che ogni argomento sia contenuto in pagine intere e possiate stamparlo dall'inizio alla fine separatamente col titolo in testa.

1. **Premesse** ▶ pagg. 2-4
  - 1.1. Sulla rappresentazione
  - 1.2. Sulla formula di Eulero
  - 1.3. Sulle identità fondamentali
  - 1.4. Sul prodotto
2. **Rotazioni nel piano Argand-Gauss** ▶ pagg. 5-6
  - 2.1. Applicazioni
  - 2.2. Equazione della circonferenza
3. **Sviluppo delle potenze complesse** ▶ pagg. 7-9
  - 3.1. Base reale
    - 3.1.1. Esponente complesso
    - 3.1.2. Esponente immaginario puro
  - 3.2. Base complessa
    - 3.2.1. Esponente intero
    - 3.2.2. Esponente complesso
    - 3.2.3. Esponente immaginario puro
  - 3.3. Base immaginaria
    - 3.3.1. Esponente intero
    - 3.3.2. Esponente complesso
    - 3.3.3. Esponente immaginario puro
  - 3.4. Logaritmo di un numero complesso
4. **Radici complesse** ▶ pagg. 10-14
  - 4.1. Radici ennesime
  - 4.2. Radici ennesime dell'unità
    - 4.2.1. Unità reale
    - 4.2.2. Unità immaginaria
5. **Equazione ciclotomica** ▶ pagg. 15-20
  - 5.1. Teorema fondamentale dell'algebra
  - 5.2. Gruppi ciclici
  - 5.3. Radici primitive dell'unità
  - 5.4. Polinomi ciclotomici
  - 5.5. Equazione ciclotomica

# 1 PREMESSE

## 1.1 Sulla rappresentazione

Per le operazioni di moltiplicazione ed elevazione a potenza complessa si utilizza più efficacemente della rappresentazione **cartesiana**

$$\begin{aligned} \blacktriangleright z &= a + bi \\ \bar{z} &= a - bi \\ z^{-1} &= \frac{a - bi}{a^2 + b^2} \end{aligned}$$

la rappresentazione in **coordinate polari**

$$\begin{aligned} \blacktriangleright z &= \rho(\cos\theta + i\sin\theta) \\ \bar{z} &= \rho(\cos\theta - i\sin\theta) \\ z^{-1} &= \rho^{-1}(\cos\theta - i\sin\theta) \end{aligned}$$

dove per  $z$  si ha

$$\rho = \sqrt{a^2 + b^2}, \quad a = \rho \cos\theta, \quad b = \rho \sin\theta$$

$$\cos\theta = \frac{a}{\sqrt{a^2 + b^2}}, \quad \sin\theta = \frac{b}{\sqrt{a^2 + b^2}}$$

$$\tan\theta = \frac{b}{a}, \quad \theta = \arctan\frac{b}{a}, \quad a \neq 0$$

o, meglio ancora, quella **esponenziale**

$$\begin{aligned} \blacktriangleright z &= \rho e^{i\theta} \\ \bar{z} &= \rho e^{-i\theta} \\ z^{-1} &= \rho^{-1} e^{-i\theta} \end{aligned}$$

che produce espressioni più compatte e dove per la **formula di Eulero** si ha

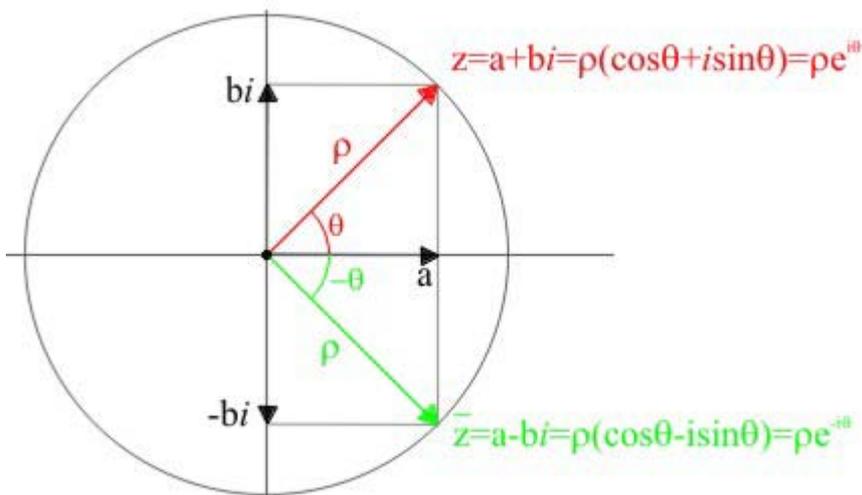
$$\blacktriangleright e^{i\theta} = \cos\theta + i\sin\theta$$

*I numeri complessi possono essere rappresentati anche in termini di matrici emisimmetriche reali*

$$a + bi = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

$$\rho e^{i\theta} = \begin{pmatrix} \rho & 0 \\ 0 & \rho \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

*per via dell'isomorfismo tra  $\mathbb{C}$  e il campo di queste matrici. Ma questa rappresentazione è poco utile per gli scopi di questo lavoro.*



con la funzione  $e^{i\theta}$  che traccia nel piano Argand-Gauss una circonferenza di raggio unitario al variare di  $\theta \in \mathbb{R}$ .

## 1.2 Sulla formula di Eulero

Tale formula discende dallo sviluppo in **serie di Taylor** delle funzioni

$\sin \theta$ ,  $\cos \theta$ ,  $e^\theta$  con  $\theta \in \mathbb{R}$

per le quali si ha

$$\sin \theta = \sum_{k=0}^{\infty} \left( \frac{(-1)^k}{(2k+1)!} \right) \theta^{(2k+1)} = \theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \frac{\theta^7}{7!} + \dots$$

$$\cos \theta = \sum_{k=0}^{\infty} \left( \frac{(-1)^k}{2k!} \right) \theta^{2k} = 1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \frac{\theta^6}{6!} + \dots$$

$$e^\theta = \sum_{k=0}^{\infty} \left( \frac{\theta^k}{k!} \right) = 1 + \theta + \frac{\theta^2}{2!} + \frac{\theta^3}{3!} + \frac{\theta^4}{4!} + \dots$$

Nell'ultima serie, sostituendo  $\theta$  con  $i\theta$  si avrà

$$e^{i\theta} = 1 + i\theta + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + \frac{(i\theta)^5}{5!} + \dots$$

$$= 1 + i\theta - \frac{\theta^2}{2!} - \frac{i\theta^3}{3!} + \frac{\theta^4}{4!} + \frac{i\theta^5}{5!} - \dots$$

$$= \left( 1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \frac{\theta^6}{6!} - \dots \right) + i \left( \theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \frac{\theta^7}{7!} + \dots \right)$$

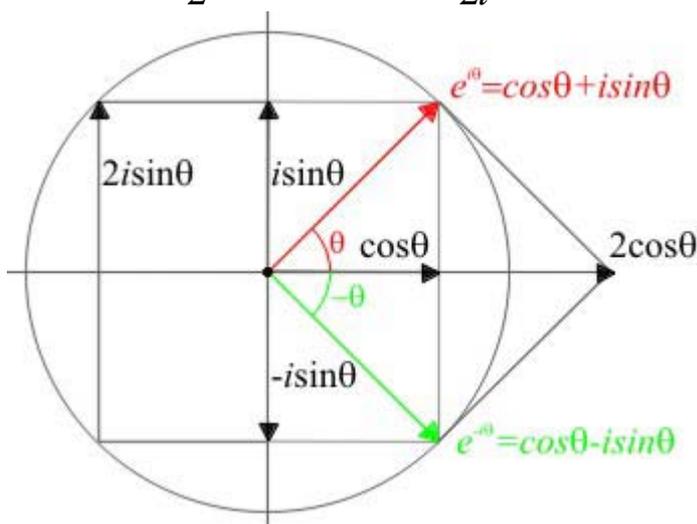
$$= \cos \theta + i \sin \theta$$

ovvero la formula, e poichè è

$$e^{-i\theta} = \cos \theta - i \sin \theta$$

si avrà anche

$$\cos \theta = \frac{e^{i\theta} + e^{-i\theta}}{2}, \quad \sin \theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$$



### 1.3 Sulle identità fondamentali

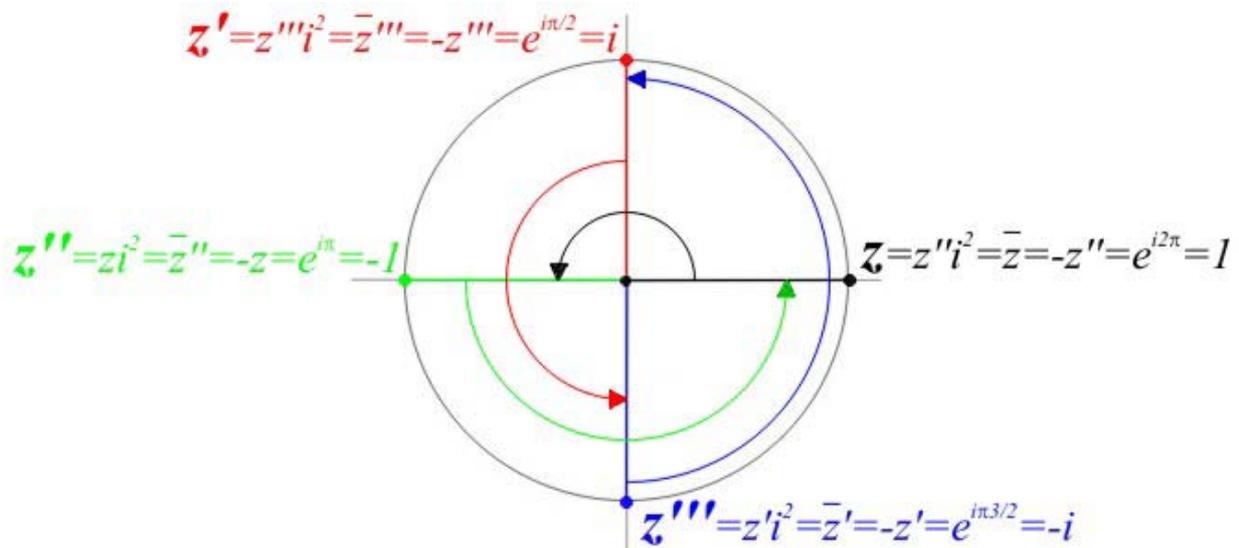
Dalla formula di Eulero discende l'omonima identità:

►  $e^{i\pi} + 1 = 0$

e, più in generale per  $\theta = k\pi/2$ ,  $k \in \mathbb{N}$

$\theta$	$\pi/2$	$\pi$	$\pi 3/2$	$2\pi$
$e^{i\theta}$	$i$	$-1$	$-i$	$1$

Considerando numeri complessi di modulo unitario avremo le seguenti rotazioni ed equivalenze per  $k\pi$ ,  $k \in \mathbb{N}$ :



### 1.4 Sul prodotto

Il prodotto di un numero reale  $n$  per un numero complesso  $z$  è uguale a

►  $nz = n\rho e^{i\theta}$

Il prodotto di due numeri complessi

$z = \rho e^{i\theta}$ ,  $z' = \rho' e^{i\theta'}$

è uguale a

►  $zz' = \rho\rho' e^{i(\theta+\theta')}$

e quindi  $zz'$  ha per modulo il prodotto dei moduli e per argomento la somma degli argomenti.

In particolare si ha

►  $zz = \rho\rho e^{i(\theta+\theta)} = z^2 = \rho^2 e^{i2\theta}$

il che conduce agevolmente al punto 3.2.1.

Non sempre il prodotto di due numeri complessi è un numero complesso. Infatti

$z\bar{z} = (a + bi)(a - bi) = a^2 + b^2 = \rho^2$

$zz^{-1} = a + bi \cdot \frac{a - bi}{a^2 + b^2} = 1$

$zz'^{-1} = \rho\rho'^{-1}$  se  $\theta = \theta'$

e  $zz$  per  $\theta = k\pi/2$ ,  $k \in \mathbb{N}$  è un numero reale o immaginario puro secondo quanto visto in 1.3. ■

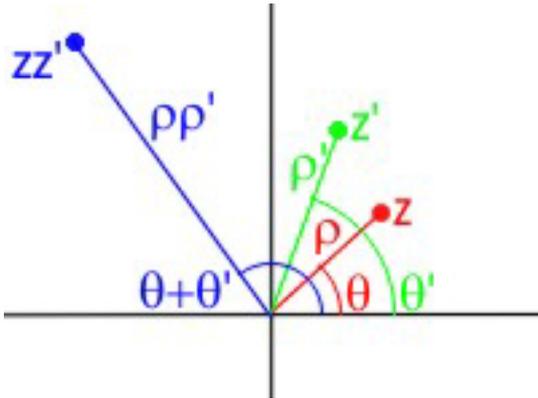
## 2 ROTAZIONI NEL PIANO ARGAND-GAUSS

### 2.1 Applicazioni

E' evidente che l'applicazione

$$\varphi: \mathbb{C} \rightarrow \mathbb{C}$$

dove  $zz' = re^{i(\theta+\theta')}$ ,  $\theta, \theta' \in \mathbb{R}$  con il prodotto  $\rho\rho' = r$  costante, descrive una circonferenza di raggio  $r$  e centro l'origine.



Notate come l'applicazione non sia biettiva in quanto uno stesso numero complesso  $zz'$  è rappresentato da valori diversi di  $(\theta + \theta')$  multipli di  $2\pi$ .

Conviene inoltre notare che, analogamente a quanto accade il campo reale, coppie diverse di numeri complessi danno lo stesso prodotto e quindi descrivono la stessa circonferenza:

► **Esempio**

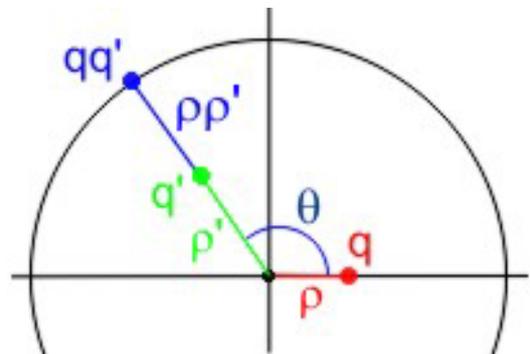
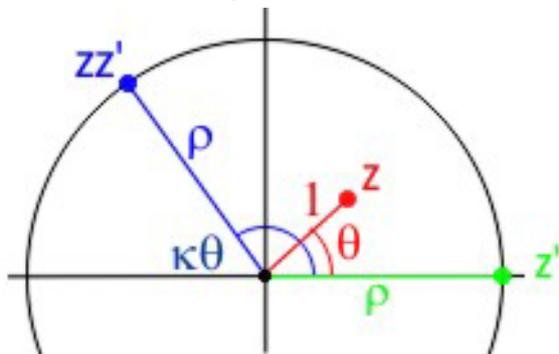
$$z = 9e^{i\pi/6}, z' = 2e^{i3\pi/2}, q = 6e^{i2\pi/3}, q' = 3e^{i\pi}$$

$$zz' = 18e^{i5\pi/3} = qq'$$

In base a queste osservazioni possiamo semplificare la faccenda e far vedere come una circonferenza sia descritta in fin dei conti da un solo numero complesso del quale si faccia variare l'argomento (parlando di rotazioni possiamo sostituire al termine 'argomento' quello di 'fase'). Consideriamo infatti il caso particolare in cui uno dei due numeri complessi sia diverso dall'unità ma con modulo uguale ad uno e l'altro abbia fase iniziale uguale a zero; allora si ha

$$z = e^{i\theta}, z' = \rho, zz' = \rho e^{i(k\theta)} \text{ con } k \in \mathbb{R} \text{ e l'applicazione è per}$$

$$zz' = re^{i(k\theta)} \text{ con } \rho = r \text{ e } k \in \mathbb{R}$$



$$qq' = re^{i(k\theta)} \text{ con } \rho\rho' = r \text{ e } k \in \mathbb{R}$$

Se volete potete considerare  $q$  con modulo qualunque e fase zero, per ottenere lo stesso risultato da una prospettiva diversa.

Infine notiamo come il prodotto di un numero complesso per l'unità immaginaria produca le seguenti rotazioni:

$$\rho e^{i\theta} \cdot i = \rho e^{i\theta} e^{i\pi/2} = \rho e^{i(\theta+\pi/2)}$$

$$\rho e^{i\theta} \cdot -i = \rho e^{i(\theta-\pi/2)}$$

Con in tasca queste semplici considerazioni possiamo scoprire l'acqua calda ed affermare che **per qualsiasi operazione con numeri complessi che dia risultati con modulo costante, tali risultati stanno tutti su una circonferenza di raggio il modulo.**

## 2.2 Equazione della circonferenza

Partendo dalla definizione di modulo per la quale si ha

$$\rho = |z| = \sqrt{x^2 + y^2}$$

e che rappresenta la distanza di  $z$  dall'origine degli assi, arriviamo agevolmente alla distanza di due punti nel piano complesso

$$|z' - z''| = |(x' + iy') - (x'' + iy'')| = |(x' - x'') + i(y' - y'')| = \sqrt{(x' - x'')^2 + (y' - y'')^2}$$

ma allora se  $z_o$  rappresenta le coordinate  $(x_o, y_o)$  del centro e  $r$  è il raggio

$$\blacktriangleright |z - z_o| = r$$

è l'equazione della circonferenza nel piano complesso.

Infatti si ha

$$|(x + iy) - (x_o + iy_o)| = r$$

$$(x - x_o)^2 + (y - y_o)^2 = r^2$$

da cui ponendo

$$a = -2x_o, \quad b = -2y_o, \quad c = x_o^2 + y_o^2 - r^2$$

si ottiene la nota equazione cartesiana della circonferenza

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

che si riduce a

$$\blacktriangleright x^2 + y^2 = r^2$$

se la circonferenza ha per centro l'origine.

► Ecco un **esempio** per una circonferenza di centro  $\left(-\frac{\sqrt{2}}{2}, \frac{1}{2}i\right)$  e raggio 1:

$$\left|z + \frac{\sqrt{2}}{2} - \frac{1}{2}i\right| \leq 1 \quad \Rightarrow \quad \left(x + \frac{\sqrt{2}}{2}\right)^2 + \left(y - \frac{1}{2}\right)^2 \leq 1 \quad \Rightarrow \quad 4x^2 + 4y^2 + 4\sqrt{2}x - 4y - 1 \leq 0$$

L'equazione rappresenta il luogo geometrico dei punti del piano complesso:

- compresi entro la circonferenza di equazione data (il cerchio) se vale la disequaglianza
- sulla circonferenza di equazione data (la circonferenza) se vale l'eguaglianza. ■

### 3 SVILUPPO DELLE POTENZE COMPLESSE

Ho escluso la banalità di  $a^p$ , però vorrei rammentarvi che  $\mathbb{R} \subset \mathbb{C}$  e che quindi in questo caso si parlerebbe di numeri complessi con parte immaginaria nulla. In seguito quando il risultato di un'operazione tra numeri complessi darà come risultato un numero complesso con parte immaginaria nulla lo chiamerò 'numero reale', ma solo per comodità.

#### 3.1 Base reale $a$

##### 3.1.1 Se l'esponente è un numero complesso $p + qi$

si ha

$$\blacktriangleright a^{(p+qi)} = a^p a^{qi} = a^p e^{(iq \ln a)}$$

da cui ponendo

$$\theta = q \ln a$$

$$\rho = a^p$$

si ha il numero complesso

$$z = \rho e^{i\theta}$$

risultato dell'elevazione a potenza

$$a^{(p+qi)}$$

##### 3.1.2 Se l'esponente è il numero immaginario $i$

si ha

$$\blacktriangleright a^i = e^{i \ln a} = \cos \ln a + i \sin \ln a$$

#### 3.2 Base complessa $z$

##### 3.2.1 Se l'esponente è un numero intero $n$

si utilizza la **formula di De Moivre** la cui dimostrazione è elementare per induzione:

$$\blacktriangleright z^n = \rho^n (\cos n\theta + i \sin n\theta) = \rho^n e^{in\theta}, \quad n \geq 1$$

► **Esempio**

$$z^5 = (-2 + i2)^5 = 128(1 - i)$$

Trasformiamo  $z$  in forma trigonometrica

$$z = (-2 + i2) = \sqrt{8} \left( -\frac{2}{\sqrt{8}} + i \frac{2}{\sqrt{8}} \right) = 2\sqrt{2} \left( \cos \frac{3\pi}{4} + i \sin \frac{3\pi}{4} \right)$$

$$z^5 = 128\sqrt{2} \left( \cos \frac{15\pi}{4} + i \sin \frac{15\pi}{4} \right) = 128\sqrt{2} \left( \frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2} \right) = 128(1 - i)$$

Ma **non sempre una tale elevazione a potenza è un numero complesso**, e ciò accade ovviamente sempre quando l'argomento è multiplo di  $\pi$ .

► **Esempio**

$$z^4 = (-2 + i2)^4 = -64$$

Si calcola facilmente che l'argomento di  $z$  è  $\frac{3\pi}{4}$  e che quello di  $z^4$  vale  $3\pi$ ; quindi il risultato dell'elevazione a potenza sarà un numero reale, negativo per la disparità del fattore moltiplicativo. Terminiamo il calcolo per controllare:

$$z^4 = 64(\cos 3\pi + i \sin 3\pi) = 64(-1 + 0) = -64$$

### 3.2.2 Se l'esponente è un numero complesso $p + qi$

si ha

$$z^{(p+qi)} = (\rho e^{i\theta})^{(p+qi)} = [e^{\ln \rho} e^{i\theta}]^{(p+qi)}$$

da cui sviluppando il secondo membro

$$\begin{aligned} [e^{\ln \rho} e^{i\theta}]^{(p+qi)} &= (e^{\ln \rho})^p (e^{\ln \rho})^{qi} (e^{i\theta})^p (e^{i\theta})^{qi} \\ &= \rho^p e^{(qi \ln \rho)} e^{ip\theta} e^{-\theta q} \end{aligned}$$

ed ordinando si ottiene

$$\blacktriangleright z^{(p+qi)} = \rho^p e^{-\theta q} e^{i(q \ln \rho + \theta p)}$$

Ponendo ora

$$\rho' = \rho^p e^{-\theta q}$$

$$\theta' = q \ln \rho + \theta p$$

si ha il numero complesso

$$z' = \rho' e^{i\theta'}$$

risultato dell'elevazione a potenza

$$z^{(p+qi)}$$

### 3.2.3 Se l'esponente è il numero immaginario $i$

allora si ha

$$\blacktriangleright z^i = (\rho e^{i\theta})^i = \rho e^{-\theta}$$

ovvero un numero reale.

## 3.3 Base immaginaria $i$

### 3.3.1 Se l'esponente è un numero intero $n$

poichè

$$i = e^{\frac{i\pi}{2}}$$

si ha

$$\blacktriangleright i^n = e^{\frac{in\pi}{2}}$$

Il risultato di  $i^n$  sarà un numero reale o immaginario puro a seconda della parità o disparità dell'esponente.

$\circ$	$i$	$i^2$	$i^3$	$i^4$	$i^5$
$i$	-1	-i	1	i	-1
$i^2$	-i	1	i	-1	-i
$i^3$	1	i	-1	-i	1
$i^4$	i	-1	-i	1	i
$i^5$	-1	-i	1	i	-1

Come calcolare  $i^n$  ?

$$i^n \in G, \quad \circ(i) = 4, \quad i^n = i^r, \quad r = n - 4q$$

Esempio:  $i^{127} = i^3 = -i$

**3.3.2 Se l'esponente è un numero complesso  $z = p + qi$**   
 si ha

$$\blacktriangleright i^{(p+qi)} = \left( e^{\frac{i\pi}{2}} \right)^{p+qi} = e^{-\frac{\pi q}{2}} e^{\frac{i\pi p}{2}} = e^{\frac{\pi}{2}(pi-q)}$$

da cui ponendo

$$\rho = e^{-\frac{\pi q}{2}}$$

$$\theta = \frac{\pi p}{2}$$

si ha il numero complesso

$$z = \rho e^{i\theta}$$

risultato dell'elevazione a potenza

$$i = e^{\frac{i\pi}{2}}$$

**3.3.3 Se l'esponente è il numero immaginario  $i$**   
 si ha

$$\blacktriangleright i^i = \left( e^{\frac{i\pi}{2}} \right)^i$$

da cui il numero reale

$$i^i = e^{-\frac{\pi}{2}}$$

**3.4 Logaritmo di un numero complesso**

Ponendo

$$z = \rho e^{i(\theta+2k\pi)}$$

si ha

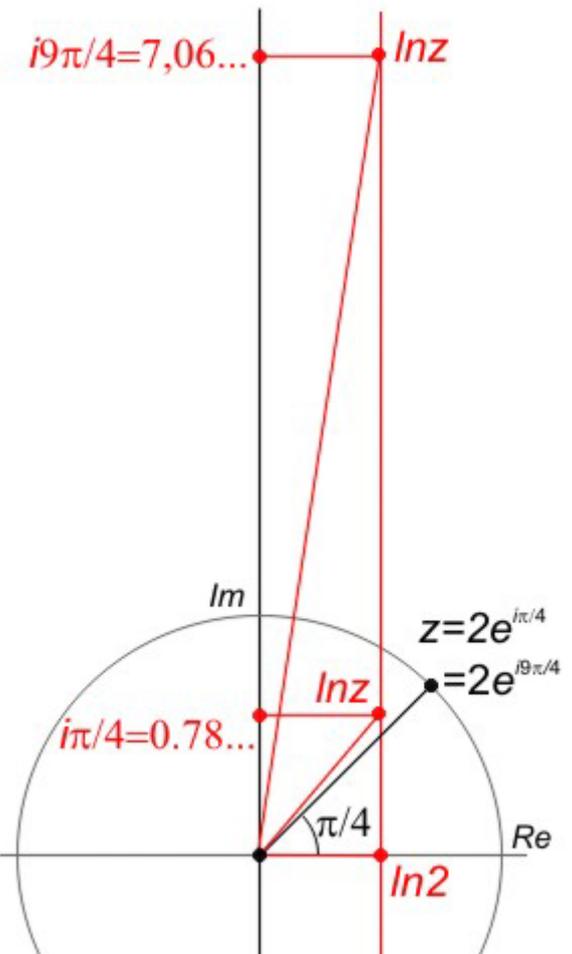
$$\blacktriangleright \ln z = \ln \rho + \ln e^{i(\theta+2k\pi)} = \ln \rho + (\theta + 2k\pi)i$$

Cosa succede nel piano Argand-Gauss al variare di  $k$  ?

Il logaritmo di un numero complesso è una **funzione polidroma di variabile complessa**.

E' infatti evidente che  $\mathcal{Z}$  ha immagini infinite e coincidenti e descrive una circonferenza al variare di  $\theta$ ,

mentre le immagini del logaritmo naturale di  $\mathcal{Z}$  sono sempre infinite ma distinte e giacciono tutte sulla **retta parallela all'asse immaginario  $a = \ln \rho$** . ■



## 4 RADICI COMPLESSE

### 4.1 Radici ennesime di un numero complesso

Possiamo applicare la formula di De Moivre anche a potenze con indice frazionario  $\frac{1}{n}$ ,  $n \in \mathbb{N}$ , ma in tal caso l'operazione è di estrazione di radice e il risultato dell'elevazione a tale potenza non sarà un singolo numero complesso ma  $n$  numeri  $\in \mathbb{C}$ . Infatti se

$$\sigma^n e^{in\vartheta} = w = \rho e^{i\theta} \neq 0$$

è un numero complesso qualsiasi, segue che

$$\sigma = \rho^{1/n}, \quad n\vartheta = \theta + 2k\pi$$

Allora per  $k = 0, 1, 2, 3, \dots, p, \dots, q, \dots, n-1 \rightarrow j = k+1$

► ☺  $\omega_j = \rho^{1/n} e^{i\left(\frac{\theta+2k\pi}{n}\right)}$

saranno le  $n$  radici ennesime, uniche e distinte, di  $w$  in  $\mathbb{C}$ .

La dimostrazione è semplice:

- ✓ tali radici non possono essere **meno** di  $n$  perchè

$$\omega_j^n = \rho e^{i(\theta+2k\pi)} = \sigma^n e^{in\vartheta} = w \text{ e quindi le } \omega_j \text{ sono proprio le radici ennesime di } w;$$

- ✓ non possono essere **più**  $n$  per via del teorema di Ruffini valido anche in  $\mathbb{C}$ ;
- ✓ sono tutte **distinte** perchè se due di esse non lo fossero si avrebbe

$$\omega_p = \rho^{1/n} e^{i\left(\frac{\theta+2p\pi}{n}\right)} = \omega_q = \rho^{1/n} e^{i\left(\frac{\theta+2q\pi}{n}\right)}$$

dove i due argomenti non potrebbero differire che per multipli di  $2\pi$ .

Cioè esisterebbe un  $m$  intero tale che

$$\frac{\theta+2p\pi}{n} - \frac{\theta+2q\pi}{n} = 2m\pi \text{ ovvero } (p-q) = mn$$

il che è impossibile perchè  $(p-q)$  non può essere multiplo di  $n$  essendo  $p, q$  distinti tra loro e compresi tra  $0$  e  $n-1$ .

E' evidente dalla formula ☺ come le radici siano distribuite sulla circonferenza di raggio  $\rho^{1/n}$  e quindi stiano sui vertici di un poligono inscritto di  $n$  lati, il che conferma come esse siano in numero di  $n$  e tutte distinte tra loro.

► **Esempio:** sia il numero complesso

$$z^2 = 1 + \sqrt{3}$$

Per poter utilizzare la formula ☺ occorre prima trovare il valore di  $\theta$ :

$$\rho = \sqrt{a^2 + b^2} = 2, \quad \cos \theta = \frac{a}{\rho} = \frac{1}{2}, \quad \theta = \frac{\pi}{3}$$

Applicando ora la formula ☺ avremo le radici

$$\omega_1 = \rho^{1/2} e^{i\pi/6} = \sqrt{2} \left( \frac{\sqrt{3}}{2} + \frac{i}{2} \right) = \frac{\sqrt{6} + i\sqrt{2}}{2}, \quad \omega_2 = \rho^{1/2} e^{i7\pi/6} = \sqrt{2} \left( -\frac{\sqrt{3}}{2} - \frac{i}{2} \right) = -\frac{\sqrt{6} + i\sqrt{2}}{2}$$

► **Esempio:** sia il numero complesso

$$z^3 = -8i$$

allora avremo

$$\rho = 8, \quad \sin \theta = -1, \quad \theta = \frac{3\pi}{2}$$

$$\omega_1 = 2e^{i3\pi/6} = 2i, \quad \omega_2 = 2e^{i7\pi/6} = -\sqrt{3} - i, \quad \omega_3 = 2e^{i11\pi/6} = \sqrt{3} - i$$

► **Esempio:** siano i numeri complessi

$$z_p^4 = i \quad \text{e} \quad z_q^4 = 1$$

per tutti e due avremo come modulo

$$\rho = 1 \quad \text{mentre gli argomenti saranno rispettivamente} \quad \theta = \frac{\pi}{2}, \quad \theta = 0$$

Per  $z_q^4 = 1$  si calcola facilmente che le radici sono  $1, i, -1, -i$

Per  $z_p^4 = i$  basta calcolare una  $\omega_{pj}$  qualsiasi e moltiplicarla per le radici dell'unità per avere le quattro radici cercate. Scegliendo la prima, quella per  $k = 0$ , abbiamo la conferma che

$$e^{i\left(\frac{\theta}{n}\right)} \cdot e^{i\left(\frac{2k\pi}{n}\right)} = e^{i\left(\frac{\theta+2k\pi}{n}\right)}$$

per cui eseguendo i calcoli si avrà

$$\omega_{p1} = e^{i\frac{\pi}{8}} = \frac{\sqrt{\sqrt{2}+2}}{2} + i \frac{\sqrt{2-\sqrt{2}}}{2} = z_{p1} \cdot 1$$

allora per  $k = 1, 2, 3$  le altre saranno

$$\omega_{p2} = z_{p1} \cdot i = -\frac{\sqrt{2-\sqrt{2}}}{2} + i \frac{\sqrt{\sqrt{2}+2}}{2}$$

$$\omega_{p3} = z_{p1} \cdot -1 = -\frac{\sqrt{\sqrt{2}+2}}{2} - i \frac{\sqrt{2-\sqrt{2}}}{2}$$

$$\omega_{p4} = z_{p1} \cdot -i = \frac{\sqrt{2-\sqrt{2}}}{2} - i \frac{\sqrt{\sqrt{2}+2}}{2}$$

Ma avremmo potuto scegliere una radice  $\omega_{pj}$  qualsiasi poichè il risultato è sempre multiplo di  $2\pi$  :

$$e^{i\left(\frac{\theta+2k\pi}{n}\right)} \cdot e^{i\left(\frac{2k\pi}{n}\right)} = e^{i\left(\frac{\theta+4k\pi}{n}\right)}$$

## 4.2 Radici ennesime dell'unità

### 4.2.1 Unità reale

Secondo la formula ☺ se è  $w = 1$  si ha  $\rho = 1, \theta = 0$  e le radici dell'equazione

$$x^n - 1 = 0$$

sono le radici ennesime dell'unità reale e sono date dalla formula ridotta

► ☺  $\omega_j = e^{i\left(\frac{2k\pi}{n}\right)}$

Esse esprimono nel piano complesso le coordinate dei vertici del poligono regolare di  $n$  lati inscritto nella circonferenza unitaria.

► **Esempio:** l'equazione

$$x^3 - 1 = 0, \theta = 0$$

ha come radici

$$\omega_1 = 1, \omega_2 = \frac{-1+i\sqrt{3}}{2}, \omega_3 = \frac{-1-i\sqrt{3}}{2}$$

mentre l'equazione

$$x^3 + 1 = (x+1)(x^2 - x + 1) = 0, \theta = \pi/2$$

ha come radici

$$\omega_1 = \frac{1+i\sqrt{3}}{2}, \omega_2 = -1, \omega_3 = \frac{1-i\sqrt{3}}{2}$$

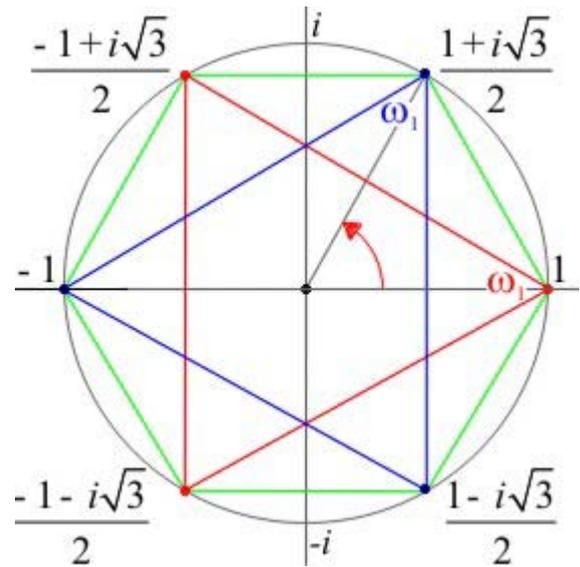
e poichè è

$$(x^3 - 1)(x^3 + 1) = x^6 - 1$$

tutte assieme sono le radici dell'equazione

$$x^6 - 1 = 0$$

e stanno sulla circonferenza unitaria uniformemente distanziate di  $\pi/3$ , sui vertici di due triangoli equilateri ruotati di  $\pi/3$  l'uno rispetto all'altro e su quelli di un esagono regolare.



► **Esempio:** considerando invece radici di indice pari per  $n = 4$  avremo:

$$x^4 - 1 = 0, \theta = 0$$

$$\omega_1 = 1, \omega_2 = i, \omega_3 = -1, \omega_4 = -i$$

$$x^4 + 1 = (x^2 - 1)(x^2 + 1) = 0, \theta = \pi$$

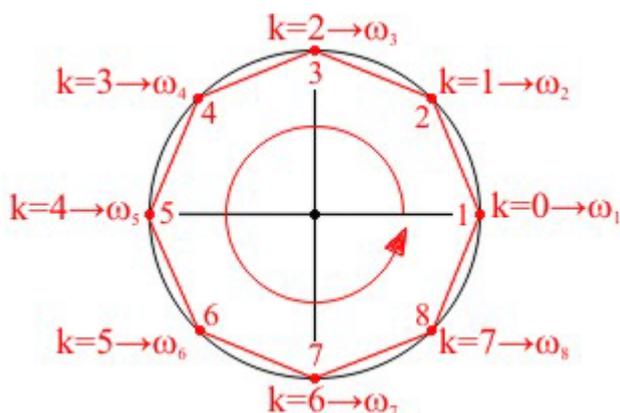
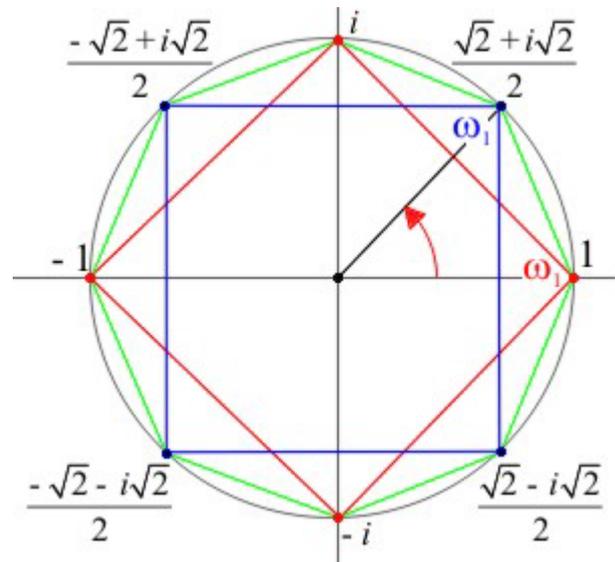
$$\omega_1 = \frac{\sqrt{2}+i\sqrt{2}}{2}, \omega_2 = \frac{-\sqrt{2}+i\sqrt{2}}{2},$$

$$\omega_3 = \frac{-\sqrt{2}-i\sqrt{2}}{2}, \omega_4 = \frac{\sqrt{2}-i\sqrt{2}}{2}$$

$$(x^4 - 1)(x^4 + 1) = x^8 - 1$$

In questo caso le radici stanno sulla circonferenza unitaria uniformemente distanziate di  $\pi/4$ ,

sui vertici di due quadrati ruotati di  $\pi/4$  l'uno rispetto all'altro e su quelli di un ottagono regolare.



*Schema di numerazione delle radici*

$$\omega_j \rightarrow k = 0, 1, 2, \dots, n-1$$

*Per interpretare correttamente le rotazioni bisogna posizionare la prima radice  $\omega_1$ , ovvero quella corrispondente a  $k = 0$ , e ruotare il quadrante in senso antiorario. Per le radici dell'unità reale  $\omega_1$  è sempre uguale ad 1 e quindi la sua posizione è la stessa per  $n$  qualsiasi.*

Ma se  $n < 3$  le radici dell'unità sui vertici di quali 'poligoni' stanno ?

► **Esempio:** con un finale "trivial", ecco le equazioni

$$x^2 \pm 1 = 0, \quad x \pm 1 = 0$$

le cui radici stanno rispettivamente sugli estremi di un segmento e su un punto.

#### 4.2.2 Unità immaginaria

E' abbastanza evidente che per ottenere le radici ennesime dell'unità immaginaria basta ruotare di  $\pi/2$  quelle corrispondenti dell'unità reale, ovvero moltiplicarle per  $i$ . Ma dimostriamolo.

Secondo la formula ☺ le radici ennesime delle equazioni

$x^n - i = 0, (\theta = \pi/2)$  e  $x^n + i = 0, (\theta = 3\pi/2)$  sono date rispettivamente da

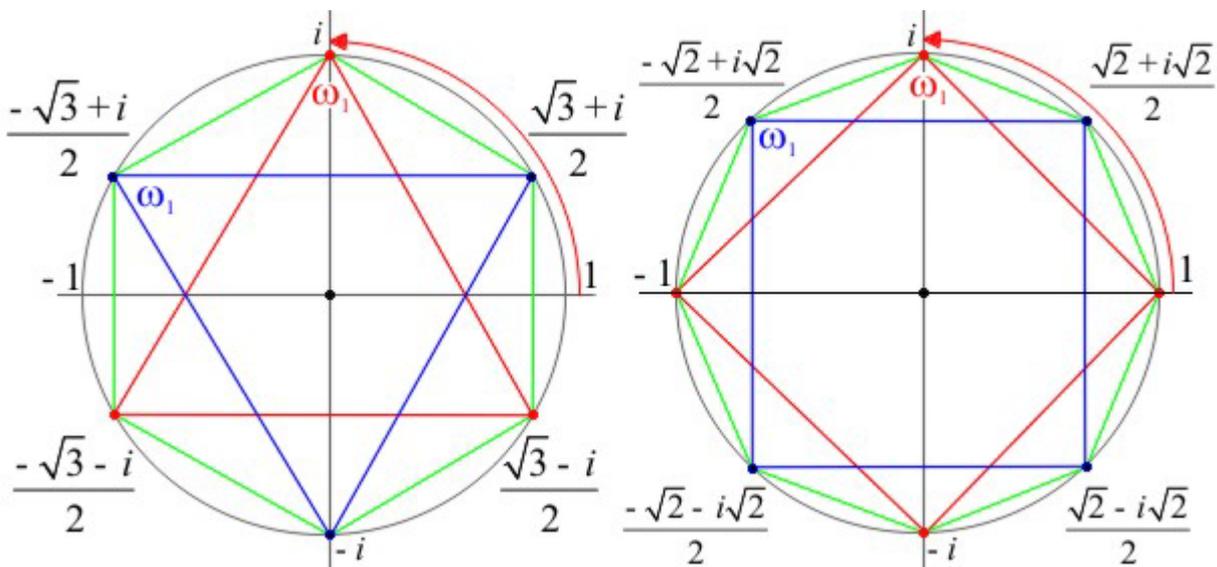
$$\text{► ☺ } \omega_j = e^{i\left(\frac{\pi+4k\pi}{2n}\right)}, e^{i\left(\frac{3\pi+4k\pi}{2n}\right)}$$

► **Esempio.** Le radici cubiche dell'unità immaginaria sono:

$$\omega_1 = e^{\frac{i\pi}{6}} = \frac{\sqrt{3}}{2} + \frac{i}{2}, \quad \omega_2 = e^{\frac{5i\pi}{6}} = -\frac{\sqrt{3}}{2} + \frac{i}{2}, \quad \omega_3 = e^{\frac{9i\pi}{6}} = -i$$

risultati che si ottengono appunto moltiplicando le radici dell'unità reale per  $i$ .

Ripetendo tutti i passaggi del paragrafo precedente otterremo due gruppi di grafici ruotati di  $\pi/2$  rispetto ai precedenti.



► Per quanto sopra dimostrato si può affermare che:

- ✓ le radici complesse sono sempre in numero pari e coniugate due a due;
- ✓ se un'equazione di grado pari possiede radici reali esse devono essere in numero pari e opposte due a due;
- ✓ un'equazione di grado dispari deve avere almeno una radice reale.

✓ è vero che  $\sum_{j=0}^{n-1} \omega_j = 0$

✓ è vero che  $1 + \sum_{m=1}^{n-1} \omega_j^m = 0$  se  $\omega_j \neq 1$  è una radice ennesima dell'unità.

► **Un ultimo esempio.** Mettiamo i risultati di questo paragrafo in uno shaker, agitiamo bene ed esaminiamo il risultato:

$$x^8 + x^4 + 1 = 0$$

Che tipo di cocktail si nasconde in questa equazione e come lo si rappresenta ?

Poichè tutto deve entrare, disegni inclusi, in quel che resta di questa pagina, sarò breve:

$$x_{1,2}^4 = \frac{-1 \pm i\sqrt{3}}{2} \rightarrow x_{1,2}^2 = \frac{\pm 1 \pm i\sqrt{3}}{2}, x_{3,4}^2 = \frac{\mp 1 \pm i\sqrt{3}}{2} \rightarrow$$

$$x_{1,2} = \omega_{1,5} = \frac{\pm\sqrt{3} \pm i}{2}, x_{3,4} = \omega_{3,7} = \frac{\mp 1 \pm i\sqrt{3}}{2}, x_{5,6} = \omega_{6,2} = \frac{\mp 1 \mp i\sqrt{3}}{2}, x_{7,8} = \omega_{4,8} = \frac{\mp\sqrt{3} \pm i}{2}$$

$$\rho_1 = \rho_2 = 1, \theta_{1,2} = \frac{4\pi}{3}, \frac{2\pi}{3}, \omega_{(2,4,6,8)} = e^{i\left(\frac{4+p}{12}\right)\pi}, \omega_{(1,3,5,7)} = e^{i\left(\frac{2+p}{12}\right)\pi}, p = 0, 6, 12, 18$$

Ecco fatto. Abbiamo ottenuto il nostro ottagono, inscritto in una circonferenza unitaria, irregolare ma simmetrico rispetto agli assi, costruito sovrapponendo i due gruppi di grafici delle radici cubiche, privi delle radici reali e immaginarie pure, che giacciono su parte dei vertici di un dodecagono regolare, poligono costruibile con riga e compasso..

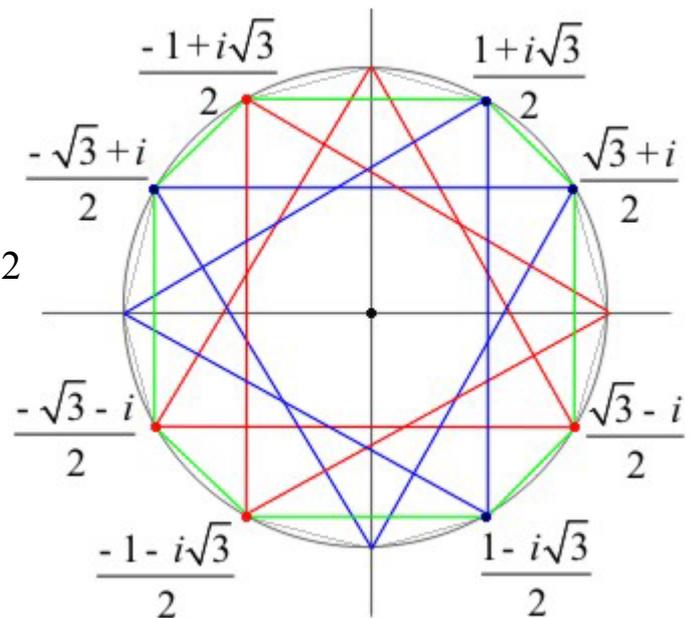
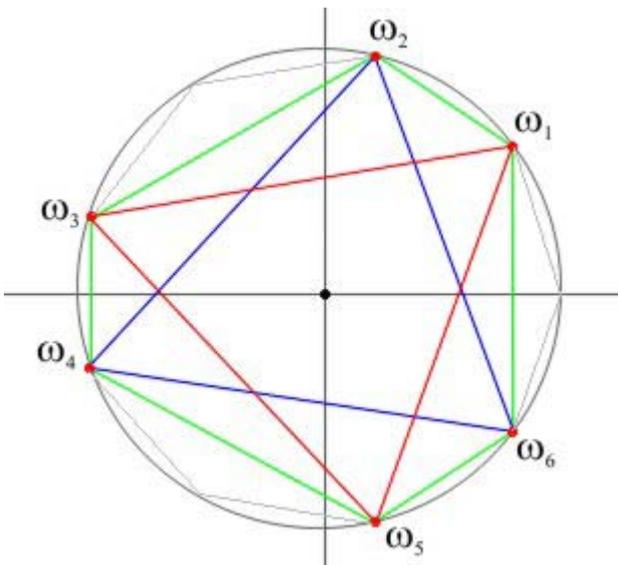
Qualcosa del genere si ottiene anche dal cocktail

$$x^6 + x^3 + 1 = 0$$

per il quale è

$$\rho = 1, \theta_{1,2} = \frac{4\pi}{3}, \frac{2\pi}{3}$$

$$\omega_{(2,4,6)} = e^{i\left(\frac{4+p}{9}\right)\pi}, \omega_{(1,3,5)} = e^{i\left(\frac{2+p}{9}\right)\pi}, p = 0, 6, 12$$



In questo caso per posizionare le sei radici sui vertici di un esagono irregolare, simmetrico rispetto all'asse reale ed inscritto nella circonferenza unitaria, è necessario costruire un poligono regolare di 9 lati; ma l'ennagono non è un poligono costruibile, nè con riga e compasso nè con altri metodi, salvo accettare approssimazioni di varia entità dell'angolo  $2\pi/9$ . ■

## 5 EQUAZIONE CICLOTOMICA

### 5.1 Teorema fondamentale dell'algebra

Ogni polinomio a coefficienti complessi di grado  $n$

$$f_n(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1} + a_nx^n$$

possiede  $n$  radici  $\omega_i$  in  $\mathbb{C}$  non necessariamente distinte.

Infatti, poichè  $f_n(x)$  possiede almeno una soluzione  $\omega_1$ , per il teorema di Ruffini (valido in  $\mathbb{C}$ ) possiamo dividerlo per  $x - \omega_1$  ottenendo

$$f_n(x) = (x - \omega_1)f_{n-1}(x)$$

Ma poichè anche  $f_{n-1}(x)$  possiede almeno una soluzione  $\omega_2$  avremo

$$f_n(x) = (x - \omega_1)(x - \omega_2)f_{n-2}(x)$$

e quindi iterando il procedimento sino ad un polinomio di primo grado si ottiene

$$\blacktriangleright f_n(x) = a_n(x - \omega_1)(x - \omega_2)(x - \omega_3) \cdot \dots \cdot (x - \omega_n)$$

con  $\omega_1 \dots \omega_n$  soluzioni dell'equazione

$$f_n(x) = 0$$

► **Esempio:** il polinomio

$$x^3 - 1 = 0$$

ha sicuramente una soluzione reale  $x_1 = 1$  e quindi si scompone in

$$(x - 1)(x^2 + x + 1) = 0$$

Il polinomio ridotto di secondo grado non ha soluzioni reali essendo

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

ma complesse

$$x_+, x_- = \frac{-1 \pm i\sqrt{3}}{2}$$

Il teorema fondamentale dell'algebra beneficia di interessanti dimostrazioni una delle quali è molto semplice e richiede solo la conoscenza del **teorema di Liouville** per il quale se una funzione intera  $f: \mathbb{C} \rightarrow \mathbb{C}$  è limitata allora è costante.

Si dimostra che  $f_n(x)$  ha radici in  $\mathbb{C}$  dimostrando il contrario, e cioè che un polinomio privo di radici in  $\mathbb{C}$  è costante.

Sia la funzione complessa

$$g(z) = \frac{1}{f(z)}$$

con  $f(z)$  polinomio complesso senza radici in  $\mathbb{C}$ .

Essendo  $f(z) \neq 0$ ,  $g(z)$  è definita in  $\mathbb{C}$  ed olomorfa, ovvero intera.

Per applicare il teorema di Liouville basta dimostrare che è anche limitata.

Ed infatti lo è, poichè essendo

$$\lim_{z \rightarrow \infty} f(z) = \infty$$

risulta

$$\lim_{z \rightarrow \infty} g(z) = 0$$

$g(z)$  è quindi limitata ed essendo intera è costante.

Ma essendo  $g(z)$  costante anche  $f(z)$  è costante.

Si è quindi dimostrato che i polinomi senza radici sono quelli costanti.

Teniamo da parte questo risultato e torniamo alle radici ennesime dell'unità.

## 5.2 Gruppi ciclici

Le radici  $n$ esime dell'unità formano **gruppi moltiplicativi abeliani**  $\mathcal{G}$  di ordine  $n$ .

Ad esempio, dette e numerate come visto in precedenza le tre radici cubiche

$$\omega_1 = 1, \quad \omega_2 = -\frac{1}{2} + \frac{i\sqrt{3}}{2}, \quad \omega_3 = -\frac{1}{2} - \frac{1-i\sqrt{3}}{2}$$

le proprietà di  $\mathcal{G}$

- chiusura
- associatività
- esistenza dell'elemento neutro
- esistenza degli inversi
- commutatività

sono verificate nella tabella

$\circ$	$\omega_1$	$\omega_2$	$\omega_3$
$\omega_1$	$\omega_1$	$\omega_2$	$\omega_3$
$\omega_2$	$\omega_2$	$\omega_3$	$\omega_1$
$\omega_3$	$\omega_3$	$\omega_1$	$\omega_2$

$\mathcal{G}$  è inoltre **ciclico** con  $\omega_2$  e  $\omega_3$  generatori, e ciò significa che ciascun elemento di  $\mathcal{G}$

è generato da opportune potenze dell'elemento generico

$$\omega_k = \omega_j^m, \quad m = 0, 1, 2, \dots, n-1$$

e, più in generale, che

$$\omega_k = \omega_g^m$$

con  $\omega_g$  generatore e  $m \in \mathbb{Z}^+$  con  $\mathcal{G}$  che viene generato ciclicamente ogni  $n$  iterazioni, ovvero con  $n$  periodo di ciascuna radice.

Proviamo con la tabella a generare  $\mathcal{G}$  tre volte con le due primitive:

$\omega_2$ generatore		
$\omega_2^0 = \omega_1$	$\omega_2^3 = \omega_1$	$\omega_2^6 = \omega_1$
$\omega_2^1 = \omega_2$	$\omega_2^4 = \omega_2$	$\omega_2^7 = \omega_2$
$\omega_2^2 = \omega_3$	$\omega_2^5 = \omega_3$	$\omega_2^8 = \omega_3$
$\omega_3$ generatore		
$\omega_3^0 = \omega_1$	$\omega_3^3 = \omega_1$	$\omega_3^6 = \omega_1$
$\omega_3^1 = \omega_3$	$\omega_3^4 = \omega_3$	$\omega_3^7 = \omega_3$
$\omega_3^2 = \omega_2$	$\omega_3^5 = \omega_2$	$\omega_3^8 = \omega_2$

D'altro canto anche le radici quarte dell'unità reale

$$\omega_1 = 1, \omega_2 = i, \omega_3 = -1, \omega_4 = -i$$

formano un gruppo  $\mathcal{G}$  che viene generato da  $\omega_2$  e  $\omega_4$  ogni quattro iterazioni:

$\circ$	$\omega_1$	$\omega_2$	$\omega_3$	$\omega_4$
$\omega_1$	$\omega_1$	$\omega_2$	$\omega_3$	$\omega_4$
$\omega_2$	$\omega_2$	$\omega_3$	$\omega_4$	$\omega_1$
$\omega_3$	$\omega_3$	$\omega_4$	$\omega_1$	$\omega_2$
$\omega_4$	$\omega_4$	$\omega_1$	$\omega_2$	$\omega_3$

Vi suggerisce qualcosa questa tabella ?

Tornate indietro al paragrafo 3.3.1...

### 5.3 Radici primitive dell'unità

Si definisce **ordine di un elemento**  $j$  appartenente ad un gruppo  $J$

$$\circ(j), j \in J$$

il più piccolo  $m \in \mathbb{N}$ , se esiste, tale che

$$j^m = e$$

dove  $e$  è l'elemento neutro del gruppo.

Poichè  $\mathcal{G}$  è moltiplicativo il suo elemento neutro è 1; allora si definisce **ordine di una radice  $n$ -esima dell'unità**

$$\circ(\omega_k)$$

il più piccolo  $m \in \mathbb{N}$  tale che

$$\omega_k^m = 1 \text{ e } \omega_k^{m-1} \neq 1, \omega_k^{m-2} \neq 1, \dots, \omega_k \neq 1$$

► Se  $\circ(\omega_k) = n$ ,  $\omega_k$  è radice ennesima **primitiva** dell'unità e  $(k, n) = 1$

La dimostrazione è banale ponendo  $z \neq 1$  e scrivendo:

$$z^n - 1 = (z - 1)(z^{n-1} + z^{n-2} + \dots + z + 1) = 0$$

dove è

$$(z - 1) \neq 0$$

e quindi

$$(z^{n-1} + z^{n-2} + \dots + z + 1) = 0$$

dove

$$z \neq -1$$

Ovviamente se  $n > 1$   $\omega_1$  non è mai primitiva, e se è  $n > 2$  e pari non lo è neanche la sua opposta.

► **Esempio:** per le radici cubiche

$\omega_1$  non è primitiva perchè  $1^m = 1$

$\omega_2, \omega_3$  lo sono perchè  $\left(-\frac{1}{2} \pm \frac{i\sqrt{3}}{2}\right)^3 = 1$  con 3 intero minimo per il quale ciò è verificato.

Per le radici quarte anche l'opposta  $\omega_3$  non è primitiva ( $\omega_3^2 = 1$ ).

Le radici primitive sono dunque un sottogruppo  $\mathcal{P}$  di  $\mathcal{G}$  e poichè  $\mathcal{G}$  è **ciclico** anche  $\mathcal{P}$  è **ciclico**.

Il numero di differenti radici primitive si calcola con la **funzione  $\varphi$  di Eulero**, detta anche **toziante**, definita per

$$\varphi(1) = 1$$

$n > 1$ ,  $\varphi(n)$  = numero degli interi **int** minori di  $n$  e primi con  $n$ .

Ad esempio, senza bisogno di calcoli si trova ( $k = 0, 1, 2, 3, \dots, n-1$ )

$$\varphi(3) \Rightarrow 1, 2 = 2 \Rightarrow -\frac{1}{2} + i\sqrt{3}, -\frac{1}{2} - i\sqrt{3}$$

$$\varphi(4) \Rightarrow 1, 3 = 2 \Rightarrow i, -i$$

$$\varphi(6) \Rightarrow 1, 5 = 2 \Rightarrow \frac{1}{2} + i\sqrt{3}, \frac{1}{2} - i\sqrt{3}$$

$$\varphi(8) \Rightarrow 1, 3, 5, 7 = 4 \Rightarrow \frac{\sqrt{2} + i\sqrt{2}}{2}, \frac{-\sqrt{2} + i\sqrt{2}}{2}, \frac{-\sqrt{2} - i\sqrt{2}}{2}, \frac{\sqrt{2} - i\sqrt{2}}{2}$$

e poichè  $\varphi$  è una funzione moltiplicativa si ha che

$$\varphi(n)\varphi(q) = \varphi(nq) \text{ se } n, q \text{ sono coprimi}$$

e quindi, ad esempio,

$$\varphi(12) \Rightarrow 1, 5, 7, 11 = \varphi(3)\varphi(4) = 4$$

$$\varphi(24) \Rightarrow 1, 5, 7, 11, 13, 17, 19, 23 = \varphi(3)\varphi(8) = 8 \text{ (ma non } \varphi(4)\varphi(6) \text{ !)}$$

In generale per calcolare il valore della la funzione  $\varphi$  per  $n$  qualsiasi si adopera la

**produttoria di Eulero**

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \text{ con } p \text{ primi distinti di } n.$$

► **Esempio:** per l'equazione

$$x^{55} - 1 = 0$$

si ha

$$\varphi(55) = \varphi(5 \cdot 11) = 55 \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{11}\right) = 40$$

Quindi le radici 55esime dell'unità reale sono 55 delle quali 40 primitive.

La funzione  $\varphi$  di Eulero dunque rappresenta l'ordine del sottogruppo delle radici primitive.

A questo punto sappiamo **quante** sono le primitive, ma sappiamo anche **quali** sono tra le ennesime ?

Certamente, perchè abbiamo detto che è

$$\omega_k^n (k, n) = 1$$

Allora, ricordando il sistema di numerazione delle radici ennesime dell'unità, risultano primitive quelle che portano come indice **int + 1**.

Per concludere, sono radici 55esime primitive dell'unità:

$$\omega_2, \omega_3, \omega_4, \omega_5, \omega_7, \omega_8, \omega_9, \omega_{10}, \omega_{13}, \omega_{14}, \omega_{15}, \dots, \omega_{55}$$

Proviamo che è vero, escludendo la banalità di  $k = 0 \rightarrow \omega_1^1 = 1$ :

$$\omega_2^{55} = \left(e^{i2\pi/55}\right)^{55} = 1, \omega_6^{55} = \left(e^{i10\pi/55}\right)^{11} = 1$$

dove quelli assegnati sono gli esponenti minimi perchè le due equazioni siano verificate.

Bene, ora possiamo parlare di polinomi ciclotomici.

## 5.4 Polinomi ciclotomici

Consideriamo il polinomio seguente e la sua elementare fattorizzazione

$$x^4 - 1 = (x - 1)(x + 1)(x^2 + 1) = (x - 1)(x^3 + x^2 + x + 1)$$

Sarebbe comodo avere a disposizione un metodo per fattorizzare un polinomio di grado  $n$ ? Naturalmente sì. Vediamo come fare.

Intanto sappiamo che se  $n$  è primo si avrà sempre

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

In generale, se  $\omega_n^k$ ,  $(k, n) = 1$  sono le radici primitive ennesime dell'unità, consideriamo il polinomio monico seguente che chiameremo **polinomio ciclotomico** e che sarà di grado  $\varphi(n)$ :

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (k,n)=1}}^n (x - \omega_n^k)$$

Si dimostra che i polinomi ciclotomici sono irriducibili su  $\mathbb{Q}$  e quindi utilizzabili per la fattorizzazione di  $x^n - 1$  su  $\mathbb{Q}$  stesso.

Infatti, poichè le radici primitive ennesime sono di ordine  $n$ , è chiaro che le radici ennesime dell'unità sono radici primitive  $d$ -esime dell'unità e quindi di ordine  $1 \leq d < n$ ,  $(n, d) = 1$ .

Allora secondo la ♠ potremo scrivere tanti polinomi ciclotomici  $\Phi_d(x)$  e concludere che

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Naturalmente calcolare tramite la ♠ tutti i polinomi ciclotomici  $\Phi_d(x)$  necessari alla fattorizzazione sarebbe un procedimento oneroso e pertanto a tale scopo utilizzeremo la formula seguente

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)}$$

che ci permette di calcolare qualsiasi polinomio ciclotomico in funzione dei precedenti.

► **Esempio.** Proponiamoci di fattorizzare

$$x^{18} - 1$$

Partendo dai primi polinomi ciclotomici, di calcolo elementare ed immediato

$$\Phi_1(x) = x - 1, \quad \Phi_2(x) = x + 1, \quad \Phi_3(x) = x^2 + x + 1, \quad \Phi_4(x) = x^2 + 1$$

con ♠ calcoliamo in cascata:

$$\Phi_6 = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = \frac{x^6 - 1}{(x - 1)(x + 1)(x^2 + x + 1)} = x^2 - x + 1$$

$$\Phi_9 = \frac{x^9 - 1}{\Phi_1(x)\Phi_3(x)} = \frac{x^9 - 1}{(x - 1)(x^2 + x + 1)} = \frac{(x^3 - 1)(x^6 + x^3 + 1)}{x^3 - 1} = x^6 + x^3 + 1$$

$$\begin{aligned}\Phi_{18} &= \frac{(x^9 - 1)(x^9 + 1)}{(x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)(x^6 + x^3 + 1)} = \\ &= \frac{(x^6 - 1)(x^6 - x^3 + 1)(x^6 + x^3 + 1)}{(x^6 - 1)(x^6 + x^3 + 1)} = x^6 - x^3 + 1\end{aligned}$$

e quindi con ♥ fattorizziamo tranquillamente per  $n = 18$ ,  $d = 1, 2, 3, 6, 9, 18$

$$x^{18} - 1 = \Phi_1 \Phi_2 \Phi_3 \Phi_6 \Phi_9 \Phi_{18}$$

$$x^{18} - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)(x^6 + x^3 + 1)(x^6 - x^3 + 1)$$

Si, lo so. Con **Derive**® basta immettere  $x^{18}-1$ , premere *Enter* e quindi *Fattorizza*...

### 5.5 Equazione ciclotomica

Siamo alla fine, possiamo tirare le somme.

Consideriamo il polinomio di grado  $n$

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

che, come visto in ♣ è così fattorizzato quando  $n$  è primo.

Dell'equazione

$$\blacktriangleright \frac{x^n - 1}{(x - 1)} = (x^{n-1} + x^{n-2} + \dots + x + 1) = 0$$

oltre a dire che:

- ✓ è irriducibile se  $n$  è primo
- ✓ è soddisfatta dalle radici primitive dell'unità se è irriducibile
- ✓ se è riducibile è soddisfatta anche dalla radice reale  $-1$

diremo che è **ciclotomica** o di divisione della circonferenza e le sue radici, dette anche **Numeri di De Moivre**, sono le  $n$  radici dell'unità ovvero le coordinate nel piano Argand-Gauss dei vertici del poligono regolare di  $n$  lati inscritto nella circonferenza unitaria che dividono in  $n$  parti. ■

Leonardo Calconi  
leo@4dmatrix.it  
19/01/2007

*Se siete arrivati fin qui vi sarete accorti di una grave assenza: le radici quinte.*

*Non si tratta di una dimenticanza ma di una scelta precisa per mettere la parola fine a questa tesina che si è dilatata fin troppo strada facendo.*

*L'argomento infatti è talmente denso di fascino che merita un lavoro a parte:*

*radici quinte → pentagono → pentagramma → sezione aurea → Fibonacci → ...*

Una versione aggiornata e corretta potrebbe essere disponibile all'indirizzo:

[www.4dmatrix.it/math](http://www.4dmatrix.it/math)