Lezione 17 - 10/11/2022

Numeri complessi

Introduciamo ora i **numeri complessi**. Nell'insieme $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ delle coppie ordinate di numeri reali, definiamo le seguenti operazioni:

- $+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ ed equivale proprio alla somma in $\mathbb{R}^2$

$$(a, b) + (c, d) = (a + c, b + d)$$

- $\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$

$$(a, b)(c, d) = (ac - bd, ad + bc)$$

Esempio:

$$(a, 0)(c, 0) = (ac, 0) \leftarrow \text{"copula"}$$
$$(0, 1)(0, 1) = (-1, 0)$$

Proposizione - C è un campo

$\mathbb{C}$ è un campo.

Dimostrazione: è chiaro che $(\mathbb{C}, +)$ è un **gruppo abeliano** il cui elemento neutro è $(0, 0)$. Dobbiamo vedere poi che $(\mathbb{C} \setminus \{0\}, \cdot)$ è un **gruppo abeliano**. Dico che:

1. $(1, 0)$ è l'elemento neutro
2. se $(a, b) \neq (0, 0)$ allora $(a, b)^{-1}$ è

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

Verifiche:

- $(1, 0)$ elemento neutro

$$(a, b)(1, 0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a, b)$$

- Inverso di (a, b)

$$\begin{aligned} (a, b)(a, b)^{-1} &= (a, b) \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) = \\ &= \left(a \cdot \frac{a}{a^2 + b^2} - b \cdot \frac{-b}{a^2 + b^2}, a \cdot \frac{-b}{a^2 + b^2} + b \cdot \frac{a}{a^2 + b^2} \right) = \\ &= \left(\frac{a^2 + b^2}{a^2 + b^2}, 0 \right) = (1, 0) \end{aligned}$$

Forma algebrica

$$(a, b) = (a, 0) + (0, b) = \underbrace{(a, 0)}_{a} + \underbrace{(0, a)}_{i} \underbrace{(b, 0)}_{b}$$

Abbiamo la seguente corrispondenza:

$$(a, b) \leftrightarrow a + ib$$

che prende il nome di **forma algebrica del numero complesso**. Inoltre, i viene chiamata **unità immaginaria**.

Si vede subito che le operazioni introdotte prima corrispondono, quando si usa la **forma algebrica**, a operare con le **usuali regole di calcolo** in $\mathbb{R}$ insieme a:

$$ib = bi \tag{1}$$
$$i^2 = -1 \tag{2}$$

Esempio:

$$(5 + 4i)(7 - 3i) = 35 + 28i - 15i - 4 \cdot 3i^2 = 47 + 13i$$

Nota:

$$\frac{1}{a+ib} \cdot \frac{a-ib}{a-ib} = \underbrace{\frac{a-ib}{a^2+a^2}}_{(*)} = \frac{a}{a^2+b^2} + i \cdot \frac{-b}{a^2+b^2}$$

La scrittura $(*)$ non ha senso **come numero complesso**, mentre quella alla sua destra dopo l'uguale ha senso.

Definizoni - Coniugato e modulo

Sia $z = a + ib$. Il **coniugato** di z è

$$\bar{z} = a - ib$$

mentre il suo **modulo** è

$$|z| = \sqrt{z\bar{z}} = \sqrt{a^2+b^2} \in \mathbb{R}$$

infatti

$$\sqrt{z\bar{z}} = \sqrt{(a+ib)(a-ib)} = \sqrt{a^2-(ib)^2} = \sqrt{a^2+b^2} \in \mathbb{R}$$

Nota: $z^{-1} = \dfrac{\bar{z}}{|z|^2}$

Proprietà

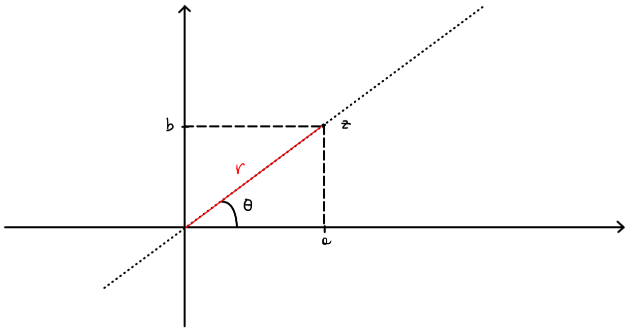
- $\overline{\overline{z}} = z$
- $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
- $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$
- $z = \overline{z} \Leftrightarrow z \in \mathbb{R}$
- $z\overline{z} = a^2 + b^2 \geq 0;\ z\overline{z} = 0 \Leftrightarrow z = 0$

  Il numero reale $z\overline{z}$ prende il nome di **norma del numero complesso** z
- $|z_1 z_2| = |z_1||z_2|$
- $|z_1 + z_2| \leq |z_1| + |z_2|$ (ovvero vale la **disugualianza triangolare**)

Forma trigonometrica

Si ha la corrispondenza

$$\begin{array}{ccc} \mathbb{C} & \longleftrightarrow & \mathbb{R}^2 \\ z = a + ib & & (a, b) \end{array}$$



dove:

$$a = r \cos\theta$$
$$b = r \sin\theta$$
$$z = r \cdot (\cos\theta + i \sin\theta)$$
$$r = |z| = \sqrt{a^2 + b^2}$$

> L'angolo θ prende il nome di **argomento del numero complesso** z.

N.B.: Se $z' = r'(\cos\theta' + i \sin\theta')$

$$zz' = rr'(\cos(\theta + \theta') + i \sin(\theta + \theta'))$$

che ci dice che il **prodotto** di due numeri complessi scritti sotto forma trigonometrica è il numero complesso che ha come argomento la **somma degli argomenti** e come modulo il **prodotto dei moduli** (ricordiamo che r è il modulo).

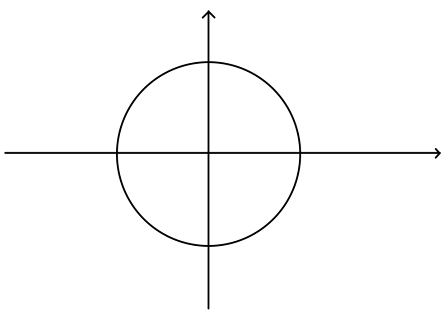
In particolare, la forma trigonometrica di un numero complesso si presta molto bene al **calcolo delle potenze**, perché per ogni intero $n \geq 0$ si ha la seguente formula di **de Moivre**:

$$z^n = r^n(\cos n\theta + i \sin n\theta)$$

Osservazioni varie:

$$S^1 = \{z \in \mathbb{C} : |z| = 1\}$$

rappresenta la circonferenza unitaria:



$$z \in S^1$$
$$z = \cos\theta + i\sin\theta$$

S^1 è un **gruppo** rispetto alla **moltiplicazione**.

Radici n-esime di un numero complesso

Dato $\alpha \in \mathbb{C}$, vogliamo trovare le soluzioni complesse di

$$z^n = \alpha$$

Vedremo che avremo sempre, se $\alpha \neq 0$, n radici n-esime distinte.

Osserviamo che quest'affermazione è falsa in $\mathbb{R}$:

- $\alpha = -1$ con n pari non ha nessuna soluzione
- $\alpha = 1$, $n = 3$ ha una sola soluzione

$$x^3 = 1 \quad x^3 - 1 = 0 \quad (x-1)\underbrace{(x^2+x+1)}_{>0} = 0 \Leftrightarrow x = 1$$

Proposizione

Se $\alpha = r(\cos\theta + i\sin\theta),\ \alpha \neq 0,\ n > 0$ le **radici n-esime** di α sono:

$$z_k = \sqrt[n]{r} \cdot \left(\cos\frac{\theta + 2k\pi}{n} + i\sin\frac{\theta + 2k\pi}{n}\right)$$

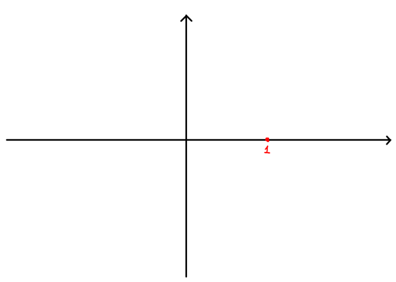
con $k \in \{0, ..., n-1\}$

Vedremo negli esercizi che

$$C_n = \{z \in \mathbb{C} : \overbrace{z^n = 1}^{\text{radici n-esime dell'unità}} \}$$

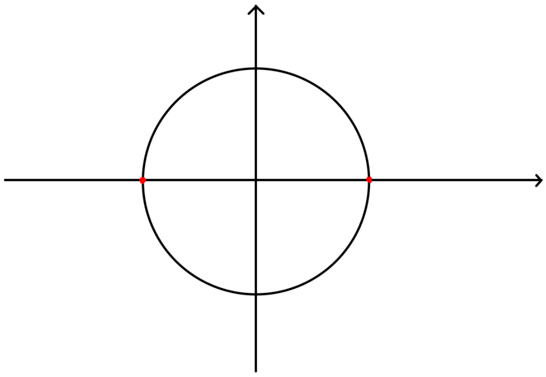
è un **sottogruppo** di $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ **isomorfo** a $\mathbb{Z}_n$.

Se $\alpha = 1$, allora $r = 1$ e $\theta = 0$

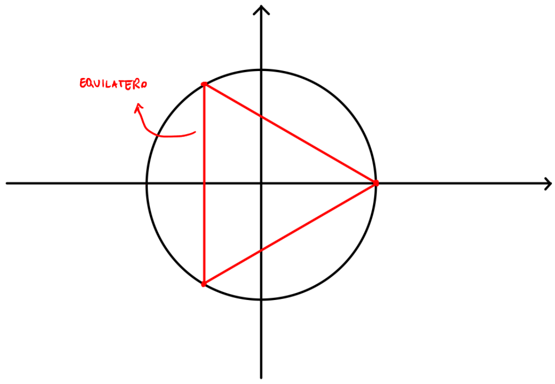


$$z_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

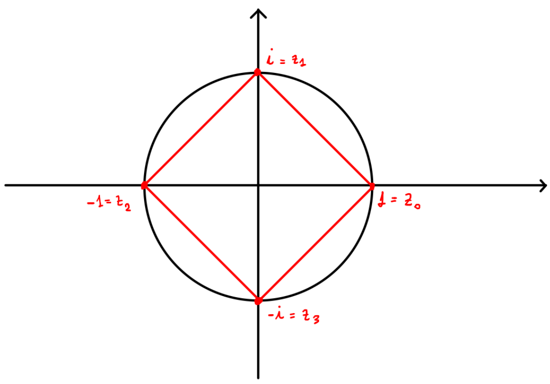
- $n = 2$



- $n = 3$



- $n = 4$



Corollari

Ricoridiamo il **teorema di Lagrange:**

Se G è un **gruppo finito** e $H \leq G$, allora $|H| \mid |G|$. Precisamente

$$|G| = [G : H]|H|$$

Corollario 1

Se $G = p$, p **primo**, allora G è **ciclico**.

Sia $g \in G,\ g \neq e$. Allora $| < g > |$ divide $|G| = p$. Poiché p è **primo**

$$| < g > | = o(g) = p$$

quindi G è ciclico.

Corollario 2

Se G è un **gruppo finito**

$$o(g) \mid |G| \ \forall g \in G$$

Infatti, $o(g) = | < g > |$, che divide $|G|$

Corollario 3

Se $|G| = n$, allora $g^n = e \ \forall g \in G$. Infatti, dato $g \in G$ $|G| = k \cdot o(g)$ quindi

$$g^{|G|} = g^{k \cdot o(g)} = \left(g^{o(g)}\right)^k = e^k = e$$

<u>Esempio</u>: $G = \mathbb{U}_{16}$, $|G| = \phi(2^4) = 8$

$$3^{|G|} = 3^8 = 6561 \equiv 1 \mod 16$$

<u>Osservazione</u>: nuova dimostrazione del **teorema di Eulero-Fermat**:

$$(a, n) = 1 \quad a^{\phi(n)} \equiv 1 \mod n$$

Infatti $U(n)$ ha carindalità $\phi(n)$ e quindi la relazioni precedente è il **corollario 3** in questo caso.

Isomorfismo

$\Phi : G \to G$' è un **omomorfismo** se

$$\Phi(g_1 g_2) = \Phi(g_1)\Phi(g_2) \qquad \forall g_1, g_2 \in G$$

Φ è un **isomorfismo** se è **biunivoca.**

Proprietà che si conservano per isomorfismo

- Abelianità

- Cardinalità
- Ordine dei sottogruppi e degli elementi

<u>Esempi</u>: $(\mathbb{Z}, +)$ e $(\mathbb{Q} \setminus 0, \cdot)$ **non sono isomorfi**.

In $(\mathbb{Z}, +)$ tutti gli elementi **non nulli** hanno **ordine infinito**, mentre in $(\mathbb{Q} \setminus \{0\}, \cdot)$ gli elementi 1 e -1 hanno **ordine** 2.

Più formalmente, se esistesse

$$f : \mathbb{Q} \setminus \{0\} \to \mathbb{Z} \text{ isomorfismo}$$

$f(-1)$ dovrebbe avere ordine 2, ma **nessun elemento non nullo** di $\mathbb{Z}$ ha **ordine finito**.

Classificazione dei gruppi di ordine ≤ 7 a meno di isomorfismo

1. $\{e\}$
2. $\mathbb{Z}_2$
3. $\mathbb{Z}_3$
4. $\mathbb{Z}_4,\ V = \mathbb{Z}_2 \times \mathbb{Z}_2\ (*)$
5. $\mathbb{Z}_5$
6. $\mathbb{Z}_6,\ S_3$ (la vedremo in futuro)
7. $\mathbb{Z}_7$

Classificazione dei gruppi di ordine 4 (*)

Se **esiste un elemento di ordine** 4, allora il gruppo è **ciclico**. Altrimenti tutti gli elementi non identici hanno ordine 2.

$$\begin{array}{lccccc} & G = \{Id, a, b, c\} & a^2 = b^2 = c^2 = e & & & \\ & e \quad \rightsquigarrow & ab = e & \Rightarrow & a = b^{-1} = b & \text{No} \\ ab = & a \quad \rightsquigarrow & ab = a & \Rightarrow & b = e & \text{No} \\ & b \quad \rightsquigarrow & ab = b & \Rightarrow & a = e & \text{No} \\ & c \quad \rightsquigarrow & ab = c & & & \text{Sì} \end{array}$$

Con $ab = c$ si ha

$$\begin{gathered} ab = c = ba \\ bc = a = cb \\ ac = b = ca \end{gathered}$$

Ker e Im

Sia $\Phi : G \to G'$ un **omomorfismo**. Definiamo

$$\begin{aligned} \mathrm{Ker}\Phi &= \{g \in G : \Phi(g) = e'\} \\ \mathrm{Im}\Phi &= \{g \in G' : \exists g \in G : \Phi(g) = g'\} \end{aligned}$$

Proprietà

1. $\Phi(e) = e'$

$$e'\Phi(g) = \Phi(g) = \Phi(eg) = \Phi(e)\Phi(g) = e'\Phi(g)\Phi(g)^{-1} = \Phi(e)\Phi(g)\Phi(g)^{-1} = e' = \Phi(e)$$

2. $\Phi(g^{-1}) = \Phi(g)^{-1}$

$$\Phi(g)\Phi(g^{-1}) = \Phi(gg^{-1}) = \Phi(e) = e' \rightsquigarrow \Phi(g^{-1}) = \Phi(g)^{-1}$$

<u>Esercizio</u>: $\mathrm{Ker}\Phi \leq G,\ \mathrm{Im}\Phi \leq G'$

- $\mathrm{Ker}\Phi \leq G$: devo mostrare che

$$a, b \in \mathrm{Ker}\Phi \Rightarrow ab^{-1} \in \mathrm{Ker}\phi$$

  - **Ipotesi**: $\Phi(a) = \Phi(b) = e'$
  - **Tesi**: $\Phi(ab^{-1}) = e'$

$$\Phi(ab^{-1}) = \Phi(a)\Phi(b^{-1}) = \Phi(a)\Phi(b)^{-1} = e'e'^{-1} = e'$$

- $\mathrm{Im}\Phi \leq G'$: devo mostrare che

$$a', b' \in \mathrm{Im}\Phi \Rightarrow a'b'^{-1} \in \mathrm{Im}\Phi$$

  - **Ipotesi**: $a' = \Phi(a),\ b' = \Phi(b)$
  - **Tesi**: $\exists c \in G : \Phi(c) = a'b'^{-1}$

$$a'b'^{-1} = \Phi(a)\Phi(b)^{-1} = \Phi(a')\Phi(b'^{-1}) = \Phi(\underbrace{ab^{-1}}_{c})$$

Proposizione

Sia $\Phi : G \to G'$ un **isomorfismo**. Allora Φ è **iniettiva** se e solo se $\mathrm{Ker}\Phi = \{e\}$.

<u>Dimostrazione</u>: **Supponiamo Φ iniettiva** e consideriamo $g \in \mathrm{Ker}\Phi$.
Vogliamo dimostrare che $g = e$. Abbiamo

$$\Phi(g) = e' = \Phi(e)$$

Poichè Φ **è iniettiva**, $g = e$.

Viceversa, supponiamo che $\mathrm{Ker} = \{e\}$ e proviamo che Φ è inieittiva, ovvero

$$
\begin{aligned}
\Phi(g_1) = \Phi(g_2) &\Rightarrow g_1 = g_2 \\
\Phi(g_1)\Phi(g_2)^{-1} &= \Phi(g_2)\Phi(g_2)^{-1} \quad \text{molt. a dx per } \Phi(g_2)^{-1} \\
\Phi(g_1)\Phi(g_2^{-1}) &= e' \\
\Phi(g_1 g_2^{-1}) &= e' \\
g_1 g_2^{-1} \in \mathrm{Ker}\Phi &= \{e\} \\
g_1 g_2^{-1} &= e \\
g_1 g_2^{-1} g_2 &= e g_2 \quad \text{molt. a dx per } g_2 \\
g_1 &= g_2
\end{aligned}
$$

Definizione - Sottogruppo normale

$N \leq G$ si dice **normale** in G ($N \trianglelefteq G$) se

$$xN = Nx \quad \forall x \in G$$

ovvero se i **laterali destri e sinistri coincidono**, ovvero

$$
\begin{gathered}
\forall n_1 \in \mathbb{N}\ \exists n_2 \in \mathbb{N} : xn_1 = n_2 x \\
\forall n_2 \in \mathbb{N}\ \exists n_1 \in \mathbb{N} : xn_2 = n_1 x
\end{gathered}
$$

Esempi:

1. In un **gruppo abeliano**, ogni sottogruppo è normale
2. In S_3 abbiamo verificato direttamente che
   - $\{\mathrm{Id}, (1,2,3), (1,3,2)\} \trianglelefteq S_3$ in quanto:

$$
\begin{aligned}
H = H(1,2,3) = H(1,3,2) &= (1,2,3)H = (1,3,2)H \\
H(1,2) &= (1,2)H \\
H(2,3) &= (2,3)H \\
H(1,3) &= (1,3)H
\end{aligned}
$$

   - $\{\mathrm{Id}, (1,2)\} \not\trianglelefteq S_3$ in quanto ad esempio:

$$H(2,3) = \{(2,3)(1,2,3)\} \neq \{(2,3)(1,3,2)\} = (2,3)H$$

Ricordiamo che $x, y \in G$ si dicono **coniugati** se

$$\exists g \in G : y = gxg^{-1}$$

Notazione: Se $H \leq G$

$$H^x = xHx^{-1} = \{xhx^{-1} : h \in H\}$$

Proposizione

Sia $N \leq G$. Sono equivalenti

1. $N \trianglelefteq G$
2. $N^x = N \; \forall x \in G$
3. $xnx^{-1} \in N, \; \forall x \in G, \forall n \in N$
4. N è un **unione di classi di coniugio**.

Dimostrazione: bisogna vedere che $1. \Rightarrow 2. \Rightarrow 3. \Rightarrow 4. \Rightarrow 1.$

- $1. \Rightarrow 2.$

$$\begin{aligned} xN &= Nx \; \forall x \\ xNx^{-1} &= Nxx^{-1} = N \\ N^x &= N \end{aligned}$$

- $2. \Rightarrow 3.$

  Ovvio. Sappiamo che $xNx^{-1} = N$; in particolare, dato $n_1 \in N \; \exists n_2 \in N$ tale che

$$xn_1x^{-1} = n_2 \in N$$

- $3. \Rightarrow 4.$

  Basta vedere che per ogni elemento $n \in N$ la sua classe di coniugio è contenuta in N. Ma questa è proprio l'ipotesi.

- $4. \Rightarrow 1.$

  Dimostrata nella prossima lezione.