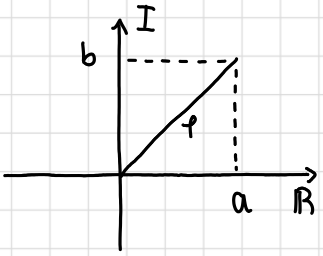
NUMERI COMPLESSI: dato $c \in \mathbb{C}$ (CAMPO: insieme dei numeri complessi) allora possiamo scrivere c nei seguenti 3 modi:



$c = a + ib$ con $\rho = \sqrt{a^2 + b^2}$

$c = \rho(\cos(\theta) + i\,\mathrm{sen}(\theta))$

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

TEOREMA FONDAMENTALE OMOMORFISMO

Dati $(G, *)$ e $(\bar{G}, \circ)$ con $\varphi: (G, *) \longrightarrow (\bar{G}, \circ)$, definiamo $H \trianglelefteq G$ con $H = \mathrm{Ker}(\varphi)$.

Sia $(G, *)$ gruppo e $H = \mathrm{Ker}(\varphi)$ $\Rightarrow$

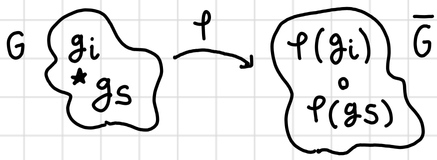
$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \bar{G} \\ G/\mathrm{Ker}\varphi \arrow[ur, "\psi"'] & \end{tikzcd}$$

ossia

$$\begin{tikzcd} (G, *) \arrow[r, "\varphi"] \arrow[d, "\pi"'] & (\bar{G}, \circ) \arrow[dl, "\psi := (\varphi \circ \pi^{-1})"] \\ (G, *)/H & \end{tikzcd}$$

se prendiamo $g_i, g_s \in G$ allora $\varphi(g_i * g_s) = \varphi(g_i) \circ \varphi(g_s)$ e $\varphi(\lambda g_i) = \lambda \circ \varphi(g_s)$

$\mathrm{Ker}\varphi = \{g \in (G, *) \mid \varphi(g) = \{e\}_{(\bar{G}, \circ)}\}$



Più precisamente, data $f: G \to H$ definiamo:

- $\mathrm{Ker}(f) := \{g \in G \mid f(g) = 1_H\}$
- $\mathrm{Img}(f) := \{y \in H \mid f(x) = y, \exists x \in G\}$

Un omomorfismo è iniettivo se $\mathrm{Ker}(f) = \{1_G\}$

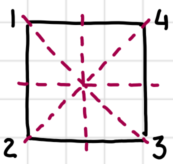
GRUPPI DEADRALI: è un gruppo formato da ROTAZIONI e SIMMETRIE

Possiamo dire che in S_n, dove $n \in \mathbb{R}$, allora rotazioni $= n$.

Sappiamo che $\sigma^n = id = \frac{2\pi}{n}$ e $\rho^2 = id = (2n - \frac{2\pi}{n})$

In generale $|D_n| = 2n$

ESEMPIO:



$id = (1\,2\,3\,4)$	$f_1 = (12)(34)$
$\sigma_1 = (4\,1\,2\,3)$	$f_2 = (14)(23)$
$\sigma_2 = (3\,4\,1\,2)$	$f_3 = (42)(13)$
$\sigma_3 = (2\,3\,4\,1)$	$f_4 = (13)(42)$

ISOMORFISMO: se è un omomorfismo e biettiva

ENDOMORFISMO: se è un omomorfismo e $G = H$, ossia è un omomorfismo sullo stesso gruppo.

AUTOMORFISMO: se è un isomorfismo e un endomorfismo.

ISOMORFISMO: è un sottogruppo dell'OMOMORFISMO, che può $G \to G$ oppure $G \to A$ ma deve poter tornare indietro ossia $A \to G$

GRUPPO SIMMETRICO: S_n

ossia n-permutazioni di cicli (finemente generati)

$|S_n| = n!$ e $|k\text{-cicli}| = \binom{n}{k} = \frac{n!}{k!(n-k)!}$

ESEMPIO: $\sigma \in S_n$, $S_3 = 1,2,3 \Rightarrow S_n = 3! = 6$

$S_3 = (1,2,3)(1\,3\,2)(\dots)\dots$

k-ciclo con $\left.\begin{matrix} k=2 \\ k=3 \\ k=6 \end{matrix}\right\} \to$ multipli di 6

$|S_2\text{-cicli}| = \binom{6}{2} = 15$ $\qquad |S_3\text{-cicli}| = \binom{6}{3} = \dots$

σ (identità): $\begin{matrix} 1 \to 1 \\ 2 \to 2 \\ 3 \to 3 \end{matrix}$, σ_1: $\begin{matrix} 1 \to 3 \\ 2 \to 1 \\ 3 \to 2 \end{matrix} = (1\,2)$, σ_2: $\begin{matrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{matrix} = (1\,3)$

OPERAZIONI TRA CICLI

$(1\,2\,3)(1\,2) = (1\,3) \neq (2\,3) = (1\,2)(1\,2\,3)$ GRUPPO NON ABELIANO

$(3\,2\,1)(3\,2) = (3\,1)$

Parità e Disparità: $\sum_{i=1}^{n} (h_i - 1) = \text{pari}$
$\quad \hookrightarrow$ lunghezza ciclo

Ordine: $k \in \mathbb{N} \mid \sigma^k = id$ dove $k = mcm(h_i)$

Ad ogni permutazione $\sigma \in S_n$ è possibile associare il suo coniugato $\tau \in S_n : \sigma \to \tau\sigma\tau^{-1}$
Due cicli sono coniugati se hanno la stessa struttura ciclica.

L'inversa: per calcolare l'inverso di un ciclo basta invertire l'ordine degli elementi, lasciando il primo elemento invariato.

OPERAZIONI di MODULI

$ax \equiv b \mod (c)$ ossia, b = resto della divisione tra $\frac{ax}{c}$

per trovare la x, o troviamo l'inverso di a, in modo tale che: $\cancel{a^{-1}a}x = ba^{-1} \Rightarrow x = ba^{-1}$

OSSERVAZIONE: $MCD(a,c) = k \mid b$

Bisogna verificare inoltre che in un sistema le c siano coprimi ossia $MCD(c_i) = 1$

TEOREMA CINESE DEL RESTO

$$\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 2 \mod 9 \end{cases}$$

$x = a + ck \Rightarrow x = 3 + 5k$

$\Rightarrow 3 + 5k \equiv 2 \mod 9$

$5k \equiv -3 + 2 \mod 9$

$5k \equiv -1 \mod 9 \Rightarrow 5k \equiv 8 \mod 9$ dove $k = -2$

$\Rightarrow k = -2 + 9h$

$\Rightarrow x = 3 + 5(-2 + 9h) \Rightarrow x = 3 - 10 + 45h \Rightarrow x = 35 + 45h \Rightarrow x = -7 + 45h$

TEOREMA di EULERO

Eulero conta quanti numeri interi positivi k tali che $1 \leq k \leq n$ e che sono coprimi con n $MCD(k,n) = 1$

$$\alpha(n) = 1 \mod n \quad \text{con } a \nmid n$$

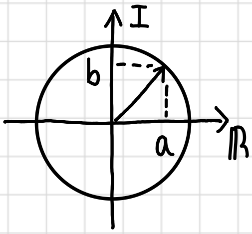
Ex: $\alpha(5) = 4$ poichè $1, 2, 3, 4$ sono coprimi con 5

ESERCIZIO: Verificare che $(\mathbb{R},+)/(\mathbb{Z},+) \sim U = \{c \in \mathbb{C} \mid \|c\| = 1\}$

$\|c\| = \sqrt{a^2+b^2} = 1$

sappiamo che $\mathbb{R}/\mathbb{Z} = \{r \in \mathbb{R} \mid r' = r + \mathbb{Z}\} \in \mathbb{R}/\mathbb{Z}$

osservazione: possiamo vedere U come tutti gli elementi della circonferenza con centro $C = (0,0)$



il Raggio: $r = 1 = \sqrt{a^2+b^2} = \|c\|$

possiamo riscrivere nel seguente modo: $u \in U \mid u = 1 \cdot [\cos(2\pi\theta) + i\,\text{sen}(2\pi\theta)]$

per il T.F.O:

$$\begin{tikzcd} (\mathbb{R},+) \arrow[r, "\varphi"] \arrow[d, "\pi"'] & U \\ (\mathbb{R},+)/(\mathbb{Z},+) \arrow[ur, "\psi"'] & \end{tikzcd}$$

, verifichiamo, dunque, $\ker(\varphi) = (\mathbb{Z},+) = ?$

$\ker(\varphi) = (r \in \mathbb{R} \mid \varphi(r) = 0)$

Abbiamo bisogno che $\cos(2\pi\theta) = 1$ e $i\,\text{sen}(2\pi\theta) = 0$. Notiamo che basta $\theta \in \mathbb{Z}$,

Ex: $\theta = 1 \Rightarrow \cos(2\pi) = 1$ e $i\,\text{sen}(2\pi) = 0$

$\Rightarrow (\mathbb{R},+)/(\mathbb{Z},+) \sim U$

ESERCIZIO 1, FOGLIO 5

Dato $(G, *)$ bisogna verificare che $\forall n \in \mathbb{N}$ la mappa $G \to G$ che manda $g \to g^n$ è un omomorfismo.

Quindi prendiamo $s, t \in \mathbb{N} \mid \varphi(s * t) = \varphi(s) * \varphi(t)$

- $\varphi(s * t) = g^{s*t} = g^s * g^t$
- $\varphi(s) * \varphi(t) = g^s * g^t$

$\Longrightarrow$ È UN OMOMORFISMO

ESEMPI di GRUPPI QUOZIENTE e i loro INDICI

- $\mathbb{Z}_3 \cong (\mathbb{Z},+) \big/ (3\mathbb{Z},+) = \{[0],[1],[2]\}$

In questo caso $\mathbb{Z}_3 = \{z \in \mathbb{Z} \mid z' = z + 3\mathbb{Z}\} \in \mathbb{Z}_3$ dove l'elemento generatore $3\mathbb{Z} = 3$

$$\Longrightarrow z+3 : \left.\begin{array}{l} z=0 \Rightarrow 0+3 = r0 \\ z=1 \Rightarrow 1+3 = r1 \\ z=2 \Rightarrow 2+3 = r2 \end{array}\right] = \{[0],[1],[2]\}$$
$$z=3 \Rightarrow 3+3 = r0$$

~~[0]~~

$[1] + \underbrace{[1]+[1]} = [0] = g^2$

$[2] + [1] = [0] = g^1$

$\Longrightarrow mcm(2,1) = 2$ (ordine)

- $\mathbb{Z}_4 = (\mathbb{Z},+) \big/ (4\mathbb{Z},+) = \{z \in \mathbb{Z} \mid z' = z + 4\mathbb{Z}\} \in \mathbb{Z}_4 \Rightarrow z' = z + 4$

$$\mathbb{Z}_4 = \{[0],[1],[2],[3]\} \Rightarrow \begin{array}{l} z=0 \Longrightarrow 0+4 = r0 \\ z=1 \Longrightarrow 1+4 = r1 \\ z=2 \Longrightarrow 2+4 = r2 \\ z=3 \Longrightarrow 3+4 = r3 \end{array}$$

verifichiamo l'ordine

$[0] = [0]$

$[1] + [1] + [1] + [1] = [0] = g^3$

$[2] + [1] + [1] = [0] = g^2$

$[3] + [1] = [0] = g^1$

$\Longrightarrow m.c.m(3,2,1) = 6$