$\mathbb{Z}$ ciclico infinito

C, C' gruppi ciclici, $C \cong C' \iff o(C) = o(C')$

↑ isomorfi

$o(G) = \#G$

Prop. $\varphi : G \to G'$ omomorfismo $\Rightarrow$ $\ker \varphi \subset G$, $\operatorname{im} \varphi \subset G'$ sottogruppi

Inoltre φ monomorfismo $\iff \ker \varphi = \{1_G\}$ ($\ker \varphi$ banale)

(nucleo)

Dim $\ker \varphi = \varphi^{-1}(1_{G'}) = \{g \in G \mid \varphi(g) = 1_{G'}\}$

$\varphi(1_G) = 1_{G'} \Rightarrow 1_G \in \ker \varphi \neq \emptyset$

$g, h \in \ker \varphi \rightsquigarrow \varphi(gh^{-1}) = \varphi(g)\,\varphi(h)^{-1} = 1_{G'} \Rightarrow gh^{-1} \in \ker \varphi \Rightarrow \ker \varphi$

$\forall g, h \in \ker \varphi$ sottogruppo

$\operatorname{im}\varphi \subset G'$

$\|$

$\{ u \in G' \mid \exists\, g \in G \text{ con } \varphi(g) = u \}$

$1_{G'} = \varphi(1_G) \in \operatorname{im}\varphi \neq \emptyset$

$u, v \in \operatorname{im}\varphi \Rightarrow \exists\, g, h \in G \text{ t.c. } u = \varphi(g),\ v = \varphi(h)$

$\Rightarrow u v^{-1} = \varphi(g)\,\varphi(h)^{-1} = \varphi(g)\,\varphi(h^{-1}) = \varphi(g h^{-1}) \Rightarrow$

$u v^{-1} \in \operatorname{im}\varphi \quad \forall\, u, v \in \operatorname{im}\varphi$

$\Rightarrow \operatorname{im}\varphi \subset G'$ Sottogruppo.

Prop. $\varphi : G \to G'$ epimorfismo ($\operatorname{im}\varphi = G'$). 1) Se G abeliano $\Rightarrow G'$ abeliano; 2) se G ciclico $\Rightarrow G'$ ciclico.

Dim 1) $u, v \in G' \Rightarrow \exists\, g, h \in G$ t.c. $u = \varphi(g)$, $v = \varphi(h)$

$$\Rightarrow uv = \varphi(g)\varphi(h) = \varphi(gh) = \varphi(hg) = \varphi(h)\varphi(g) = vu$$

(G ab. nella seconda uguaglianza)

$\forall\, u, v \in G'$

2) (*)

CAMPI

Def Un campo $(\mathbb{K}, +, \cdot)$ è un insieme non vuoto $\mathbb{K}$ dotato di due operazioni binarie $+, \cdot$ t.c.:

1) $(\mathbb{K}, +)$ è un gruppo abeliano $\rightsquigarrow 0 \in \mathbb{K}$; $\mathbb{K}^* = \mathbb{K} - \{0\}$

→ 2) $(\mathbb{K}^*, \cdot)$ è un gruppo abeliano $\rightsquigarrow 1 \in \mathbb{K} - \{0\}$

3) $\cdot$ è distributiva rispetto a $+$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$\forall\, a, b, c \in \mathbb{K}.$$

Es $\begin{cases} 0 \cdot a = 0 \quad \forall\, a \in \mathbb{K}. \ (*) \\ a \cdot 0 = 0 \end{cases}$

Es $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

$\mathbb{K}$ campo

Def $\mathbb{H} \subset \mathbb{K}$ è detto sottocampo se è chiuso rispetto a $\cdot$ e $+$ e $-$.
e $\pm 1, 0 \in \mathbb{H}$.

$\mathbb{H} \subset \mathbb{K}$ sottocampo $\Rightarrow$ $\mathbb{H}$ è un campo.

Gruppi $g + h \in \mathbb{H}$

$h \in \mathbb{H} \Rightarrow (-1)\, h = -h \in \mathbb{H}$

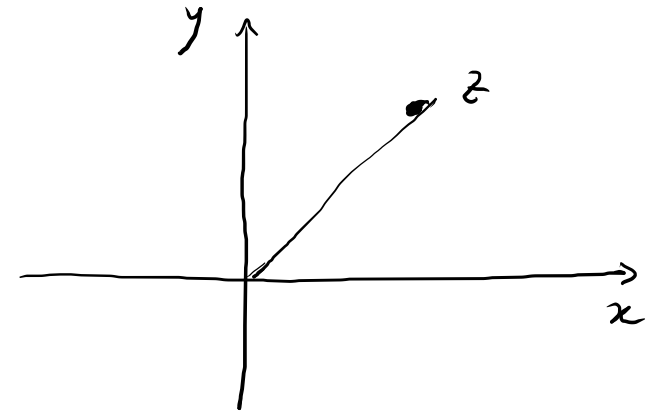
$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sottocampi

$\mathbb{C}$ $\quad z \in \mathbb{C}$

Piano di Gauss

$z = x + iy \qquad x, y \in \mathbb{R}$

$i^2 = -1$



$\mathbb{C} \cong \mathbb{R}^2$ iso di sp. vett.

$\mathbb{C}$ è uno spazio vett. su $\mathbb{R}$

$\dim_{\mathbb{R}} \mathbb{C} = 2$

$\dim_{\mathbb{C}} \mathbb{C} = 1$

$\{1, i\}$ base reale di $\mathbb{C}$

$\{1\}$ base complessa

$\mathbb{Z}$ $\boxed{n \in \mathbb{N}, \ n \geq 2}$

$a \equiv b \pmod n$ se $a - b = kn$, $k \in \mathbb{Z}$ $\iff n \mid (a-b)$

$(\equiv_n)$ ↑ modulo

(n divide $(a-b)$)

Prop. $\equiv_n$ è rel. d'equivalenza.

1) $a - a = 0 \cdot n \Rightarrow a \equiv a \pmod n \quad \forall a \in \mathbb{Z}$ (riflessiva)

2) $a \equiv_n b \Rightarrow a - b = kn \Rightarrow b - a = -kn \Rightarrow b \equiv_n a$ (simmetrica)

$k \in \mathbb{Z}$

3) $a \equiv_n b, \ b \equiv_n c \Rightarrow a - b = kn, \ b - c = hn \Rightarrow a - c = (k+h)n$

$k, h \in \mathbb{Z}$

$\Rightarrow a \equiv_n c$.

(transitiva)

Insieme quoziente

Si pone $\mathbb{Z}/\equiv_n \;=:\; \mathbb{Z}_n \;=\; \mathbb{Z}/n\mathbb{Z}$

(notazioni)

$$n\mathbb{Z} = \{ nk \mid k \in \mathbb{Z} \} \subset \mathbb{Z}$$

è la classe d'equivalenza di 0

$$a \in \mathbb{Z} \rightsquigarrow [a] = a + n\mathbb{Z} = \{ a + nk \mid k \in \mathbb{Z} \}$$

Definiamo $+$, $\cdot$ su $\mathbb{Z}_n$

$$[a], [b] \in \mathbb{Z}_n \rightsquigarrow [a] + [b] := [a+b]$$

$$[a] \cdot [b] := [ab]$$

$+$, $\cdot$ sono ben definite (non dipendono dai rappresentanti a, b)

Dim (+) $a' \equiv_n a$, $b' \equiv_n b \Rightarrow a' = a + kn$, $b' = b + hn$, $k, h \in \mathbb{Z}$

$$a' + b' = a + b + (k+h)n \equiv_n a + b$$

(·) $$a'b' = (a+kn)(b+hn) = ab + ahn + bkn + khn^2 =$$

$$= ab + \underbrace{(ah + bk + khn)}_{\in \mathbb{Z}} n \equiv_n ab$$

$$\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_n$$

$$a \longmapsto [a] = a + n\mathbb{Z}$$

$$\pi(a+b) = [a+b] = [a] + [b] = \pi(a) + \pi(b)$$

$$\pi(ab) = \pi(a)\,\pi(b)$$

$(\mathbb{Z}_n, +)$ è gruppo abeliano

- è distributiva rispetto a $+$

$[a] \in \mathbb{Z}_n$

$a = nq + r$ $\quad$ r resto della divisione di a per n

$0 \leq r < n$

$\Rightarrow a \equiv r \pmod n$

ogni classe di $\mathbb{Z}_n$ ammette un rappresentante in $\{0, 1, \dots, n-1\}$

Inoltre se $a, b \in \{0, \dots, n-1\}$ e $a \equiv b \bmod n \Rightarrow a = b$

$\mathbb{Z}_n$ è in corrispondenza biunivoca con $\{0, 1, \dots, n-1\}$

$$\boxed{O(\mathbb{Z}_n) = n}$$

$(\mathbb{Z}_n, +)$ è ciclico

$(\mathbb{Z}_n, +) \cong T_n$

$$\mathbb{Z}_n \xrightarrow{\text{iso}} T_n \qquad (*)$$
$$[a] \longmapsto e^{2\pi i \frac{a}{n}}$$

$(\mathbb{Z}_n - \{0\}, \cdot)$ non è sempre un gruppo ($\Rightarrow \mathbb{Z}_n$ non sempre campo)

$\boxed{n = pq}$, $2 \le p, q \le n-1$

(n composto)

$[p]\,[q] = [n] = [0]$ con $[p], [q] \neq [0]$ in $\mathbb{Z}_n$

divisori dello zero

Teorema $\mathbb{Z}_p$ è un campo $\iff$ p primo

$\mathbb{Z}_2 = \{0, 1\}$ campo

$\mathbb{Z}_3 = \{0, 1, 2\}$ SI

$\vdots$

$\mathbb{Z}_4$ non è campo

$\mathbb{Z}_5$ SI

$\mathbb{Z}_6$ NO

$\mathbb{Z}_7$ SI

$\mathbb{Z}_8$ NO

$\mathbb{Z}_9, \mathbb{Z}_{10}$ NO

$\mathbb{Z}_4$ SI

$(\mathbb{Z}_p)^n$ Spazio vett. su $\mathbb{Z}_p$ (p primo) di dimensione n

$(\mathbb{Z}_p)^n = \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ volte}}$

$$\boxed{\#(\mathbb{Z}_p)^n = p^n}$$

Teorema $a, b \in \mathbb{Z} - \{0\}$, $d = (a,b) = MCD(a,b) \in \mathbb{N}$

$\Rightarrow \exists\ r, s \in \mathbb{Z}$ t.c.

$$\boxed{d = ra + sb}$$

Dim A meno di cambiare i segni di r e s possiamo assumere $a, b \geq 1$.

1) $a = q_1 b + r_1 \qquad 0 \leq r_1 < b \qquad q_1, r_1 \in \mathbb{N}$

$r_1 = a - qb$ r_1 è comb. lin. di a, b e coeff. interi

2) $b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1 \qquad r_2 = b - q_2 r_1$

3) $r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 < r_2$ r_i è comb. lin di a, b $\forall i$ (in $\mathbb{Z}$)

$a = 17 \quad , b = 12$

$(a, b) = 1$

$$\boxed{1 = \underline{2} \cdot 17 + \underline{-3} \cdot 12}$$

$17 = 12 + 5$ $\qquad q_1 = 1 \quad , \quad r_1 = 5$

$12 = 2 \cdot 5 + 2$ $\qquad q_2 = 2 \quad , r_2 = 2$

$5 = 2 \cdot 2 + 1$ $\qquad q_3 = 2 \quad , \boxed{r_3 = 1} \quad = (17, 12)$

$2 = 2 \cdot 1$ $\qquad q_4 = 2, \quad r_4 = 0$

$5 = 17 - 12 = a - b$

$2 = b - 2(a-b) = -2a + 3b$

$a - b = 2(-2a + 3b) + 1 \Rightarrow \boxed{1 = 5a - 7b}$

Teorema $\mathbb{Z}_p$ campo $\iff$ p primo

Dim 1) p non primo $\Rightarrow p = m\,n$ $2 \le m, n < p$

$[m]\,[n] = [p] = 0$ in $\mathbb{Z}_p$ $\Rightarrow$ $\mathbb{Z}_p$ non campo

2) Supponiamo p primo

$[a] \in \mathbb{Z}_p - \{0\}$

$\Rightarrow p \nmid a \Rightarrow (p, a) = 1 \Rightarrow 2p + 5a = 1$

↑ non divide

$\Rightarrow [5]\,[a] = [1] \Rightarrow$

$[5] = [a]^{-1}$.