Lezione 4 ottobre 2023

mercoledì 4 ottobre 2023 11:15

Operazioni in $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

Def: $+ : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

$$\bar{x} + \bar{y} := \overline{x+y}$$

$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

$$\bar{x} \cdot \bar{y} := \overline{x \cdot y}$$

LEMMA: $+$ e $\cdot$ sono BEN DEFINITE, cioè non dipendono dalla scelta dei rappresentanti delle classi.

Dim.:

$+$: devo dimostrare che se $\bar{x} = \bar{x}_1$ e $\bar{y} = \bar{y}_1$, allora $\bar{x} + \bar{y} = \bar{x}_1 + \bar{y}_1$

Sia quindi $\bar{x} = \bar{x}_1$; questo è equivalente a $x \equiv_n x_1$; per definizione si ha $x_1 - x = kn$, per un opportuno $k \in \mathbb{Z}$, cioè $x_1 = x + kn$
sia poi $\bar{y} = \bar{y}_1$; quindi $y \equiv_n y_1$ e per definizione si ha $y_1 - y = hn$, per un opportuno $h \in \mathbb{Z}$, cioè $y_1 = y + hn$
Consideriamo ora $(x_1 + y_1) - (x+y) = (x + kn + y + hn) - (x+y$

$$= (k+h)n$$

$$\Rightarrow x_1 + y_1 \equiv_n x + y \Rightarrow \overline{x_1+y_1} = \overline{x+y}$$

$$= \Big(\bar{x}_1 + \bar{y}_1 \Big) = \bar{x} + \bar{y} \Big) =$$

Es: • in $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

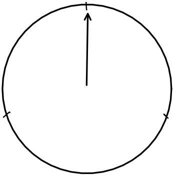
$$\bar{2} + \bar{2} = \overline{2+2} = \bar{4} = \bar{0}$$

• in $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

$$\bar{2} + \bar{2} = \overline{2+2} = \bar{4} = \bar{1}$$

$$\overset{\shortparallel}{\overline{5}} + \overset{\shortparallel}{\overline{8}} = \overline{13} = \overline{1}$$

$$\dots = \overline{-9} = \overline{-6} = \overline{-3} = \overline{0} = \overline{3} = \overline{6} = \overline{9} = \overline{12} = \dots$$



$$14 = \overline{11} = \overline{8} = \overline{5} = \overline{2}$$

$$\overline{-10} = \overline{-7} = \overline{-4} = \overset{\shortparallel}{\overline{-1}}$$

$$\overline{1} = \overline{4} = \overline{7} = \overline{10} = \overline{13}$$
$$= \overline{-2} = \overline{-5} = \overline{-8} = \dots$$

Dim. che $\cdot$ è ben definito:

$\overline{x} = \overline{x_1}$, $\overline{y} = \overline{y_1}$, è vero che

$$\overline{x}\cdot\overline{y} \overset{?}{=} \overline{x_1}\cdot\overline{y_1}$$

$$\overline{x} = \overline{x_1} \Rightarrow x \equiv_n x_1 \Leftrightarrow x_1 - x = kn \Leftrightarrow x_1 = x + kn$$
$$\overline{y} = \overline{y_1} \Rightarrow y \equiv_n y_1 \Leftrightarrow y_1 - y = hn \Leftrightarrow y_1 = y + hn$$

$$\overline{x}\cdot\overline{y} = \overline{x\cdot y}$$
$$\overline{x_1}\cdot\overline{y_1} = \overline{x_1\cdot y_1}$$

$$\underbrace{x_1 y_1 - x\cdot y = (x+kn)\cdot(y+hn)}_{\text{in } \mathbb{Z}} - x\cdot y = \cancel{x\cdot y} + (xh+yk)n + khn^2 - \cancel{xy}$$

$$= \underbrace{(xh + yk + khn)\cdot n}_{\in \mathbb{Z}}$$

$$\Rightarrow x_1\cdot y_1 \equiv_n x\cdot y$$

PROPRIETÀ DI $+$ in $\mathbb{Z}_n$:

① ASSOCIATIVA (fare per esercizio)

② $\bar{0}$ è NEUTRO per $+$:

$\forall \bar{x} \in \mathbb{Z}_n$, $\quad \bar{x} + \bar{0} = \overline{x+0} = \bar{x} = \bar{0} + \bar{x}$

③ $-\bar{x} = \overline{-x} \quad (= \overline{n-x})$

es. in $\mathbb{Z}_3$: $\bar{x} = \bar{2}$, $\quad -\bar{2} = \overline{-2} = \bar{1}$

$\bar{2} + \bar{1} = \bar{3} = \bar{0} = \bar{1} + \bar{2}$

$-x \equiv_n n-x \quad$ infatti $\quad -x-(n-x) = -n = (-1)\cdot n$

④ COMMUTATIVA (esercizio)

COROLLARIO (= CONSEGUENZA): $(\mathbb{Z}_n, +)$ è un GRUPPO ABELIANO.

Esempi:

tutti i PARI

tutti DISPARI

$\mathbb{Z}_2$:

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\mathbb{Z}_3$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\mathbb{Z}_4$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

PROPRIETÀ DI $\cdot$ IN $\mathbb{Z}_n$

① ASSOCIATIVO

② $\bar{1}$ è NEUTRO PER $\cdot$

$$\bar{1}\cdot\bar{x} = \overline{1\cdot x} = \bar{x} = \bar{x}\cdot\bar{1}$$

③ COMMUTATIVO

④ DISTRIBUTIVA DI $\cdot$ RISP. ALLA $+$

$$\bar{x}\cdot(\bar{y}+\bar{z}) = \bar{x}\cdot\bar{y} + \bar{x}\cdot\bar{z}$$

Vogliamo capire quando succede che in $\mathbb{Z}_n$ ogni elemento non nullo ammette inverso (in $\mathbb{Z}$ solo ± 1 hanno inverso. invece in $\mathbb{Q}$ tutti $a \neq 0$ hanno inverso, e anche in $\mathbb{R}$, in $\mathbb{C}$)

in $\mathbb{Z}$: $a \in \mathbb{Z}$, cerco $b \in \mathbb{Z}$ tale che $a \cdot b = 1 \iff a = \pm 1$

CAMPI

Def: Sia $K \neq \emptyset$ insieme, con 2 operazioni interne $+$ e $\cdot$

$(K, +, \cdot)$ è CAMPO se:

(K1) $(K, +)$ è gruppo abeliano

(K2) $(K \setminus \{0\}, \cdot)$ è gruppo abeliano

0 $\downarrow$ neutro risp. a $+$

(K3) Distributiva di $\cdot$ risp. a $+$

Es: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono CAMPI

PROPOSIZIONE: Sia $(K, +, \cdot)$ campo

Allora si ha:

① $\forall a \in K$, $0 \cdot a = 0$

② se $a \cdot b = 0 \Rightarrow a = 0$ oppure $b = 0$

③ se -1 è l'opposto di 1, allora $\forall\, a \in K$ si ha:

$$(-1)\cdot a = -a$$

Dim. ① $0\cdot a \overset{\boxed{k1}}{=} (0+0)\cdot a \overset{\boxed{k3}}{=} 0\cdot a + 0\cdot a$

$$0\cdot a = 0\cdot a + 0\cdot a$$

cons. l'opposto di $0\cdot a$: $-0\cdot a$

$$\underbrace{-0\cdot a + 0\cdot a} = \underbrace{-0\cdot a + 0\cdot a} + 0\cdot a$$

$$=0 \qquad = \qquad \underbrace{0 + 0\cdot a}$$

$$0 = 0\cdot a$$

② provare per esercizio

③ provare per esercizio

NOTAZIONE :

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

somma di a e l'opposto di b

$$a\cdot b = ab$$

$$a\cdot b^{-1} = a/b$$

PROBLEMA: Per quali n si ha che

$\mathbb{Z}_n$ è campo?

Es.: $\mathbb{Z}_2$: so che in $\mathbb{Z}_n$

$\bar{x}\cdot\bar{0} = \bar{0}\cdot\bar{x} = \overline{0\cdot x} = \bar{0} \quad \forall\, \bar{x}\in\mathbb{Z}_n$

in $\mathbb{Z}_n$ considero solo $\bar{x}\neq\bar{0}$

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

$\cdot$	$\bar{1}$
$\bar{1}$	$\bar{1}$

è campo

oss: $\exists$ anche 1 campo con un elemento

$\{*\}$: definiamo $* + * = *$

$= \{0\}$ $\quad\quad\quad\quad\quad\quad\quad\;\; * \cdot * = *$

CAMPO BANALE, si usa scrivere

$\mathbb{K} = \{0\}$

$\mathbb{Z}_3$:

$\cdot$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{1}$

$\Rightarrow (\bar{1})^{-1} = \bar{1}$

$(\bar{2})^{-1} = \bar{2}$

$\Rightarrow \mathbb{Z}_3$ è CAMPO

$\mathbb{Z}_4$:

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\bar{2}\cdot\bar{2} = \bar{0} \Rightarrow \mathbb{Z}_4$ non è campo per la Proposizione, punto ②

Esercizio: $\bar{2}$ non ammette inverso invece $(\bar{1})^{-1} = \bar{1}$

$(\bar{3})^{-1} = \bar{3}$ (oss. $\bar{3} = \overline{-1}$)

- $\mathbb{Z}_5$

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\boxed{\bar{1}}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\boxed{\bar{1}}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\boxed{\bar{1}}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

oss: che ora invece ogni $\bar{x} \neq \bar{0}$ ammette inverso:

$(\bar{1})^{-1} = \bar{1}$

$(\bar{2})^{-1} = \bar{3}$

$(\bar{3})^{-1} = \bar{2}$

$(\bar{4})^{-1} = \bar{4}$

$\Rightarrow \mathbb{Z}_5$ è un CAMPO