INSIEMI CON PIÙ OPERAZIONI

Def.: Sia S un insieme con due operazioni binarie
$\bullet : S \times S \longrightarrow S$ e $* : S \times S \longrightarrow S$

(1) Si dice $*$ è distributiva rispetto a $\bullet$ se $\forall s, s', s'' \in S$

$s * (s' \bullet s'') = (s * s') \bullet (s * s'')$ — a sinistra

$(s' \bullet s'') * s = (s' * s) \bullet (s'' * s)$ — a destra

(2) $(S; \bullet, *)$ si dice semianello se

(2.1) $(S; \bullet)$ è monoide commutativo,

(2.2) $(S; *)$ è semigruppo,

(2.3) $*$ è distributiva rispetto a $\bullet$.

INOLTRE, un semianello $(S; \cdot, *)$ si dice anello se la (2.1) è sostituita dalla condizione (più forte)

(2.1+) $(S; \cdot)$ è gruppo commutativo

((N.B.: la (2.2) e la (2.3) restano uguali))

(3) un semianello (eventualmente anello) $(S; \cdot, *)$ si dice commutativo, risp. unitario, se $(S; *)$ è commutativo, risp. $(S; *)$ è monoide

CIOÈ $*$ è commutativa, risp. $*$ ha elemento neutro

NOTA: in un semianello $(S; \cdot, *)$

(I) l'elemento neutro per $\cdot$ (che $\exists$ sempre!) si dice "zero", indicato 0

(II) l'eventuale elemento neutro per $*$ (se $\exists$) si dice "unità", indicata 1

(4) $(S; \bullet, *)$ si dice campo se è un anello commutativo unitario in cui, detto $\emptyset$ l'elemento neutro di $(S; \bullet)$, si ha che ogni $s \in S^* := S \setminus \{\emptyset\}$ è invertibile in $(S; *)$. IN ALTRE PAROLE,

(4.1) $(S; \bullet)$ è gruppo commutativo, con elemento neutro $\emptyset_S$,

(4.2) $(S \setminus \{\emptyset_S\}; *)$ è gruppo commutativo,

(4.3) $*$ è distributiva rispetto a $\bullet$.

ESEMPI:

① Insiemi numerici ($\mathbb{N}_+$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}^*$, $\mathbb{Q}_+$, ...):
$\cdot$ è distributiva rispetto a $+$, ma non lo è $+$ rispetto a $\cdot$

② In $\mathbb{Z}$, $\wedge$ (:= "min") è distributiva rispetto a $\vee$ (:= "max")

③ In $\mathbb{Z}$, $\vee$ è distributiva rispetto a $\vee$

④ In $\mathbb{Z}$, $\wedge$ non è distributiva risp. a $+$, né $\vee$ risp. a $+$

⑤ $\forall$ insieme E, in $\mathcal{P}(E)$ si ha che
$\cap$ è distributiva risp. a $\cup$, $\cup$ è distrib. risp. a $\cap$
$\cap$ è distributiva risp. a $\oplus$, $\cup$ non è distribut. risp. a $\oplus$

(6) $(\mathbb{N}_+ ; +, \cdot)$ <u>non</u> è semianello

(7) $(\mathbb{N}; +, \cdot)$ è semianello commutativo unitario, <u>non</u> anello

(8) $(\mathbb{Z}; +, \cdot)$ è anello commutativo unitario, <u>non</u> campo

(9) Posto $3\mathbb{Z} := \{3z \mid z \in \mathbb{Z}\} = \{\dots, -6, -3, 0, 3, 6, 9, \dots\}$,

$(3\mathbb{Z}; +, \cdot)$ è anello commutativo, <u>non</u> unitario (né campo)

(10) Posto $\mathbb{Q}_+ := \{q \in \mathbb{Q} \mid q > 0\}$ e $\mathbb{Q}_{\geq} := \mathbb{Q}_+ \cup \{0\}$, si ha

$(\mathbb{Q}_+ ; +, \cdot)$ <u>non</u> è semianello,

$(\mathbb{Q}_{\geq} ; +, \cdot)$ è semianello commutativo unitario, <u>non</u> anello

(11) $(\mathbb{Q}; +, \cdot)$ è campo

« sia E un insieme »

(12) $(\mathcal{P}(E); \cup, \cap)$ e $(\mathcal{P}(E); \cap, \cup)$ <u>non</u> sono semianelli

(13) $(\mathcal{P}(E); \oplus, \cap)$ è anello commutativo unitario, <u>non</u> campo:

- l'elemento neutro per $\oplus$ è $\emptyset$, $(F \oplus \emptyset = F = \emptyset \oplus F, \forall F \in \mathcal{P}(E))$
- $\forall F \in \mathcal{P}(E)$, l'inverso di F rispetto a $\oplus$ è F stesso $(F \oplus F = \emptyset)$
- l'elemento neutro per $\cap$ è E

(14) $\mathbb{Z}_2 := \{p, d\}$ con ~~operazioni~~ $+$ e $\cdot$ date da

$p+p := p \qquad p+d := d \qquad d+p := d \qquad d+d := p$

$p \cdot p := p \qquad p \cdot d := p \qquad d \cdot p := p \qquad d \cdot d := d$

è campo $\quad$ el. neutro per $\begin{cases} + \text{ è } p \\ \cdot \text{ è } d \end{cases}$

(15) $\mathbb{Z}_7 := \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ con operazioni $+$ e $\cdot$ date da: $\forall\, \bar{x}, \bar{y} \in \mathbb{Z}_7$

$$\bar{x} + \bar{y} := \overline{x+y}\,, \quad \bar{x} \cdot \bar{y} := \overline{x \cdot y}$$

dove $\forall z \in \mathbb{Z}$, $\bar{z} := \overline{r(z,7)} \in \{\bar{0}, \bar{1}, \dots, \bar{6}\} =: \mathbb{Z}_7$

con $r(z,7) :=$ resto della divisione per 7 di z

Ad esempio $\quad \overline{5} + \overline{6} := \overline{5+6} = \overline{11} := \overline{4} \in \mathbb{Z}_7$

$\overline{6} \cdot \overline{3} := \overline{6 \cdot 3} = \overline{18} = \overline{4} \in \mathbb{Z}_7$

<u>ORA</u> $(\mathbb{Z}_7; +, \cdot)$ è un campo $\quad \bar{3} \cdot \bar{5} = \overline{15} = \bar{1} \Rightarrow \bar{5} = \bar{3}^{-1}$, $\bar{3} = \bar{5}^{-1}$