29/11/2021

OPERAZIONE su $A \neq \emptyset$ (operazione $\underbrace{\text{BINARIA}}$ $\underbrace{\text{INTERNA}}$)

→ RISULTATO INTERNO allo STESSO INSIEME

⊕ SOMMA

$$\oplus : A \times A \longrightarrow A$$
$$(a,b) \longmapsto a \oplus b$$

$+ : \mathbb{N}_0 \times \mathbb{N}_0 \longrightarrow \mathbb{N}_0$ [1,2,4]

$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ [1,2,3,4]

$+ : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$ [1,2,3,4]

$+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ [1,2,3,4]

1) PROPRIETÀ ASSOCIATIVA

$\forall a,b,c \in A \Rightarrow \underbrace{(a \oplus b) \oplus c = a \oplus (b \oplus c)}$

→ ordine di ESECUZIONE OPERAZIONI

2) ∃ elemento NEUTRO

se $\exists\, 0 \in A : a \oplus 0 = 0 \oplus a = a \quad \forall a \in A$

3) ∃ elemento INVERSO (opposto)

$\forall a \in A \Rightarrow \exists\, a^{-1} : a^{-1} \oplus a = a \oplus a^{-1} = 0$

in un contesto di operazione SOMMA o altri uso $[-a]$

4) COMMUTATIVITÀ

$\forall a,b \in A \Rightarrow \underbrace{a \oplus b = b \oplus a}$

→ ordine dei POSTI

NATURALI

1) ☑
2) ☒ dipende se lo considero parte dell'insieme se $\mathbb{N}_0$ ☑
3) ☒ NON per TUTTI solo lo 0 ha il suo OPPOSTO
4) ☑

MOLTIPLICAZIONE

$\odot : \mathbb{N}_0 \times \mathbb{N}_0 \longrightarrow \mathbb{N}_0$ [1, , ,4]

$\odot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ [1,2, ,4]

$\odot : \mathbb{Q}^* \times \mathbb{Q}^* \longrightarrow \mathbb{Q}^*$ [1,2,3,4]

$\odot : \mathbb{R}^* \times \mathbb{R}^* \longrightarrow \mathbb{R}^*$ [1,2,3,4

* = tolto lo 0

1) PROPRIETÀ ASSOCIATIVA

2) ∃ elemento NEUTRO

per MOLTIPLICAZIONE è "1"

lo 0 non è RICHIESTO perché non è il EL. NEUTRO

3) ∃ elemento INVERSO (opposto)

$g^{-1} = \frac{1}{g}$ è opposto MOLT. e da $g^{-1} \odot g = 1$

4) COMMUTATIVITÀ

Quando un OPERAZIONE soddisfa su un certo INSIEME tutte e 4 le proprietà PRENDE il NOME di GRUPPO

Def: := $\boxed{\text{Un GRUPPO}}$ è una coppia $(A, \oplus)$ dove $\oplus$ 1), 2), 3) se $\oplus$ soddisfa anche 4) allora $(\underset{\text{insieme}}{A}, \underset{\text{operazione}}{\oplus})$ $\boxed{\text{GRUPPO COMMUTATIVO}}$

DEF := Un insieme A con due operazioni $\oplus, \odot$ tali che

$(A, \oplus)$ GRUPPO COMM.

$(A \setminus \{0\}, \odot)$ GRUPPO COMM.

e che VALGANO

$$\left.\begin{array}{l} \bullet\ (a \oplus b) \odot c = a \odot c \oplus b \odot c \\ \bullet\ a \odot (b \oplus c) = a \odot b \oplus a \odot c \end{array}\right\} \text{LEGGI DISTRIBUTIVE}$$

SI CHIAMA $\boxed{\text{CAMPO}}$

0 NEUTRO SOMMA

1 NEUTRO PRODOTTO

$(\mathbb{R}, +, \cdot, 0, 1)$ è un CAMPO

$(\mathbb{Q}, +, \cdot, 0, 1)$ è un CAMPO

DEF: Un insieme A con due OPERAZ. $\oplus, \odot$ tale che

$(A, \oplus)$ gruppo COMM

→ $(A \setminus \{0\}, \odot)$ soddisfa associativa

• VALE leggi Distributive

Si chiama $\boxed{\text{ANELLO}}$

$(\mathbb{Z}, +, \cdot)$ è un anello

→ Un anello TALE CHE $\odot$ è COMMUTATIVA si chiama ANELLO COMMUTATIVO

→ Un anello tale che $\exists$ 1. (el. NEUTRO rispetto alla MOLTIPLICAZIONE) Si CHIAMA ANELLO UNITARIO

$(\mathbb{Z}, +, \cdot)$ è un anello COMM. UNITARIO perché non ha ELEMENTI INVERSI

LA legge di ANNULLAMENTO del PRODOTTO non vale SEMPRE

DEF := Un ANELLO in cui vale la LEGGE DI annullamento del PRODOTTO si chiama DOMINIO (di INTEGRITÀ) $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$

$\mathbb{Z}$ dominio unitario commutativo

$\mathbb{Z}_n$ l'insieme delle classi resto modulo n $\equiv_n$

INSIEME QUOZIENTE di $\mathbb{Z}$ rispetto alla relazione di equivalenza "essere divisibile per"

$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ → numeri interi di $\mathbb{Z}$ che se gli si sottrae 1 diventano divisibili per 3

gli elementi di $\mathbb{Z}_n$ sono classi di eq.

in $\mathbb{Z}_n$ POSSIAMO definire delle OPERAZIONI

$\bar{i} + \bar{j} := \overline{i+j}$

$\bar{i} \cdot \bar{j} := \overline{i \cdot j}$

ES

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

$\bar{4} + \bar{2} = \overline{4+2} = \bar{6} = \bar{0}$

$\bar{1} + \bar{4}$ equivalenti

$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\bar{2} + \bar{3} = \bar{5}$

$\bar{3} + \bar{4} = \bar{7} = \bar{1}$

$\bar{3} \cdot \bar{3} = \bar{9} = \bar{3}$

opposto di

$\bar{i} \rightarrow \overline{n-i}$

$\bar{4} + \bar{2} = \bar{6} = \bar{0}$

non vale LEGGE ann. PRODOTTO

$\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$

ciò significa che non è un $\boxed{\text{DOMINIO}}$

$(\mathbb{Z}_n, +, \cdot)$ ANELLO comm. con UNITÀ no dominio

se $(\mathbb{Z}_{\underbrace{p \cdot q}_{n}}, \oplus, \odot)$ non è un DOMINIO

$$\overline{p} \cdot \overline{q} = \overline{n} = \overline{0}$$

se $(\mathbb{Z}_p, \oplus, \odot)$ con p primo è un DOMINIO, è anche un campo

$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ è un campo

INV

$\overline{1}^{-1} = \overline{1}$

$\overline{4}^{-1} = \overline{4} \Rightarrow \overline{4} \cdot \overline{4} = \overline{16} = \overline{1}$

$\overline{2}^{-1} = \overline{3}$

$\overline{3}^{-1} = \overline{2} \qquad \overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$

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

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

$\overline{2}^{-1} = 2 \quad \overline{2} \cdot \overline{2} = 1$

FARE PROVE in $\mathbb{Z}_6$ trovare elementi INVERTIBILI

SiA $(A, \oplus, \odot)$ un anello COMMUTATIVO

$\oplus$: GRUPPO COMM.

$\odot$: VALE SOLO ASSOCIA. e leggi DISTRIBUTIVE

$a^{\neq 0} \in A$ è un elemento PRIMO

se $a \mid b \odot c \Rightarrow a \mid b \vee a \mid c$

$x \mid y \Leftrightarrow \exists z \in A \quad y = z \odot x$

$a^{\neq 0} \in A$ è un elemento IRRIDUCIBILE

se $a = b \odot c \Rightarrow$ b oppure c sono INVERTIBILI in A

in $\mathbb{Z}$ ogni elemento PRIMO è IRRIDUCIBILE e VICEVERSA

quando si scrive come prodotto di due numeri in $\mathbb{Z}$ uno dei due è invertibile

---

DEF:= Sia A un DOMINIO di INTEGRITÀ e siano $a, b \in A$

$m = mcm(a,b)$

$d = MCD(a,b)$:

1) $d \mid a \wedge d \mid b$
2) se $\exists\, d'^{+MAX} : d' \mid a \wedge d' \mid b \Rightarrow d' \mid d$

$MCD(8, 12) =$

$4 \mid 8 \wedge 4 \mid 12 \Rightarrow 4 \nmid 2$ NO

anche -4 è MCD

A MENO di un elemento INVERT.

1) $a \mid m \wedge b \mid m$
2) se $\exists\, m' : a \mid m' \wedge b \mid m' \Rightarrow m \mid m'$

$\mathbb{Z}$ è un DOMINIO a FATTORIZZAZIONE UNICA

a meno dell' ordine

DEF:= sia A un DOMINIO di INTEGRITÀ allora una FATTORIZZAZIONE di $a \neq 0$ $a \in A$ è $\boxed{a = z \cdot p_1^{i_1} \dots p_r^{i_r}}$ DOVE z è INVERTIBILE e p_i è un elemento PRIMO e $i_j \geq 1$

$p_i \neq p_j \quad \forall i \neq j$

p_i è RIPETUTO una sola volta

$-6 = -1 \cdot 2^1 \cdot 3^1$

$8 = 2 \cdot 4$ non è fattorizzazione

$8 = 2^3$

$12 = 2^2 \cdot 3$

$\cancel{2 \cdot 6}$ NO

DEF:= DOMINIO è detto a fattorizzazione unica se

$\forall a \neq 0 \quad a \in A \Rightarrow \exists!\, p_1 \dots p_r$ EL. PRIMI DISTINTI $: a = z \cdot p_1^{i_1} \dots p_r^{i_r}$

con z invertibile e $i_j \geq 1$

a meno dell'ordine di $p_1 \dots p_r$

$\mathbb{Z}$ è un dominio A FATT. UNICA

se $a \cdot b = 0$ $a, b \neq 0$ $\Rightarrow a, b$ si chiamano divisori dello 0

un DOMINIO NON NE HA

ALGORITMO EUCLIDEO delle DIVISIONI successive

$\mathbb{Z}$ MCD (a,b)

MCD $(0,g) = g$ $\qquad g \mid 0 \Leftrightarrow 0 = g \cdot 0$

MCD (a,b) $\quad a,b \neq 0 \qquad a \geq b > 0$

MCD $(a,b) = $ MCD $(\pm a, \pm b)$

PROPOSIZIONE:

$\forall\ a \geq b > 0 \Rightarrow \exists!\ q, r$ in $\mathbb{N}_0$ con $0 \leq r < b$ t.c. $a = b\underbrace{q}_{\text{quozient}} + \underbrace{r}_{\text{resto}}$

$$7 = 2 \cdot \underbrace{3}_{q} \underbrace{+1}_{r} \qquad \underset{\text{dim } 4}{8} = 4 \cdot \underbrace{2}_{q} \underbrace{+0}_{r}$$

MCD (a,b) $\quad a \geq b$

$a = b \cdot q_1 + r_1 \qquad 0 \leq r_1 < b$

prendo b e lo DIVIDO per r_1

$b = r_1 \cdot q_2 + r_2 \qquad 0 \leq r_2 < r_1 < b$

$r_1 = r_2 \cdot q_3 + r_3 \qquad 0 \leq r_3 < r_2 < r_1 < b$

$\vdots$

$r_{n-2} = r_{n-1} \cdot q_n + r_n$

$r_{n-1} = r_n \cdot q_{n+1} + r_{n+1} \qquad r_{n+1} = 0$

MCD $(a,b) = r_n$

$MCD(121, 54)$

$$121 = 54 \cdot \overset{q}{2} + \overset{r}{13}$$
$$54 = 13 \cdot 4 + 2$$
$$13 = 2 \cdot 6 + 1$$
$$2 = 1 \cdot 2 + \cancel{0}$$

$MCD(121, 54) = \boxed{1}$

$MCD(164, 48)$

$$164 = 48 \cdot \overset{q}{3} + \overset{r}{20}$$
$$48 = 20 \cdot 2 + 8$$
$$20 = 8 \cdot 2 + 4$$
$$8 = 4 \cdot 2 + \cancel{0}$$

$MCD(164, 48 = \boxed{4}$

$MCD(3522, 321)$

$$3522 = 321 \cdot \overset{r}{10} + \overset{q}{312}$$
$$321 = 312 \cdot 1 + 9$$
$$312 = 9 \cdot 30 + 42$$

IDENTITÀ di BEZOUT

Sia $d = MCD(a, b)$ $\quad a, b \in \mathbb{Z}$

$\Rightarrow \exists\ \alpha, \beta \in \mathbb{Z}$ t.c. $\boxed{d = \alpha a + \beta b}$

SE $MCD(a, n) = 1 \Leftrightarrow$ allora $\bar{a}$ è invertibile in $\mathbb{Z}_n$

$\bar{1} = \bar{\alpha}\bar{a} + \boxed{\cancel{\bar{\beta}\bar{n}}} \Rightarrow \bar{n} = \bar{0}$