09/10/2013

- Insiemi finiti e insiemi infiniti

+	a	b	c
a	a	c	a
b	c	b	c
c	a	b	c

• Tabelle di questo tipo ci permettono di studiare la struttura algebrica quando si ha un numero finito di elementi COME IN QUESTO CASO: $\mathcal{U} = \{a, b, c\}$

$\Rightarrow +: \mathcal{U} \times \mathcal{U} \longrightarrow \mathcal{U}$; $a + a = a$, $a + b = c$, $a + c = a$

$b + a = c$, $b + b = b$ etc..

• Consideriamo $(\mathbb{Z}; +)$, il quale è un gruppo commutativo. Diamo, ora, la relazione seguente in $\mathbb{Z}$: dati $p, q \in \mathbb{Z} \Rightarrow$ diciamo che p è in relazione con q, pRq, $\Leftrightarrow q - p = 2n$ (RELAZIONE RESTO RISPETTO ALLA DIVISIONE PER 2)

Esempio: ① considero 3 e 2, sono in relazione fra loro?

$\Rightarrow \exists n \in \mathbb{Z} / 2 - 3 = 2n$? $\longrightarrow$ no, allora 2 e 3 non sono in relazione fra loro

② considero 2 e 4, sono in relazione fra loro?

$\Rightarrow \exists n \in \mathbb{Z} / 2 - 4 = 2n \longrightarrow n = -1$

• R è una relazione di equivalenza?

① RIFLESSIVA: $\Rightarrow$ p deve essere in relazione con p : $\underline{pRp}$

Vero, per $n = 0$: $p - p = 2 \cdot 0$

② SIMMETRICA: $\underbrace{\text{se } pRq \Rightarrow qRp}$: $\forall (p, q) \in \mathbb{Z} \times \mathbb{Z}$

$\exists \hat{n} / q - p = 2\hat{n} \Rightarrow -(q - p) = -2\hat{n}$

$\Rightarrow p - q = (-2\hat{n}) \Rightarrow qRp$

③ TRANSITIVA: $\underline{\forall p, q, r \in \mathbb{Z}, \text{ se } pRq \text{ e } qRr \Rightarrow pRr}$

$- pRq : \exists n_1 / q - p = 2n_1$

$- qRr : \exists n_2 / r - q = 2n_2$

$\Rightarrow pRr : r - p = (r - q) + (q - p) = 2n_2 + 2n_1 = 2(n_2 + n_1)$

$\Rightarrow \exists\, n = n_2 + n_1 \,/\, p R r$; allora la relazione è transitiva.

- Data una relazione di equivalenza tra elementi di un insieme A, possiamo sempre definire le "CLASSI DI EQUIVALENZA" cioè sotto-insiemi dell'insieme dato A che contengono tutti gli elementi tra loro equivalenti.

DETERMINIAMO LE CLASSI DI EQUIVALENZA PER LA RELAZIONE: "RESTO DELLA DIVISIONE PER DUE"

$\mathbb{Z} = \{ \ldots, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, \ldots \}$

- $-3 R -2 \,? \rightarrow -2-(-3) = 1 \neq 2n \;\forall n \in \mathbb{Z} \Rightarrow -3 \not R -2$
- $-3 R -1 \,? \rightarrow -1-(-3) = 4 = 2n$
- $-2 R\, 0 \,? \rightarrow 0-(-2) = 2 = 2n$

$\Rightarrow$ Dagli infiniti elementi di $\mathbb{Z}$, per la nostra relazione, si possono formare 2 classi di equivalenza, una composta dai numeri pari (E LO ZERO) e l'altra dai dispari.

- Per una relazione di equivalenza, si ha sempre un insieme quoziente: l'insieme quoziente è l'insieme costituito dalle classi di equivalenza rispetto a R, nel nostro caso si indica $\mathbb{Z}/R$ E SI LEGGE "$\mathbb{Z}$ MODULO R"

<u>Esempio</u>: prendo un rappresentante degli elementi che si trovano in una classe di equivalenza. Considero 1 e 0 per le nostre classi che pertanto verranno indicate con $\bar{1}$ e $\bar{0}$ oppure $[1]$ e $[0]$

$\Rightarrow$ INSIEME QUOZIENTE: $\mathbb{Z}/R = \{ \bar{0}, \bar{1} \}$

- Definisco una nuova operazione in $\mathbb{Z}/R$, $\bar{+} \Rightarrow$

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

- Un'operazione "ben definita" vuol dire che indipendentemente dalle scelta dei rappresentanti di una classe di equivalenza, l'operazione fra i rappresentanti mi dà come risultato LO STESSO elemento, LA STESSA classe di equivalenza CHE È LA CLASSE DI EQUIVALENZA DEL RISULTATO DATO DALL'OPERAZIONE FRA DUE QUALUNQUE RAPPRESENTANTI, CIOÈ

POSTO $\bar{a} \hat{*} \bar{b} = \overline{a*b} \Rightarrow$

SE $\bar{a}_1 = \bar{a}$ e $\bar{b}_1 = \bar{b} \Rightarrow \overline{a*b} = \overline{a_1 * b_1}$

- Nel nostro caso $\mathbb{Z}/_\rho = \mathbb{Z}_2$

$(\mathbb{Z}; \bar{+})$ è un gruppo?

① ASSOCIATIVA: $0 + (0+1) = (0+0)+1 \Rightarrow 0+1 = 0+1$

$1 + (0+1) = (1+0)+1 \Rightarrow 1+1 = 1+1$

$\vdots$

- vale la proprietà associativa

② COMMUTATIVA: è valida la proprietà commutativa perché la tabella è simmetrica

③ ∃ ELEMENTO NEUTRO: esiste l'elemento neutro ed è $\bar{0}$

④ ∃ IL RECIPROCO: esiste il reciproco; ogni elemento ha in se stesso il suo reciproco

$\Rightarrow (\mathbb{Z}; \bar{+})$ è un gruppo commutativo!

- <u>Altro esempio</u>

Considero l'insieme $\{f : [a,b] \longrightarrow \mathbb{R}\} = \mathcal{F}_{[a,b]}$

$\Rightarrow$ definisco la "somma": $f+g : [a,b] \longrightarrow \mathbb{R}$

$x \longrightarrow f(x)+g(x)$

$(\mathcal{F}_{[a,b]} ; +)$ è un gruppo?

SÌ, DA DIMOSTRARE

Esercizio:

$\mathbb{R}[x]$ = polinomi nella variabile x con grado r e n

=> considero $p(x)$ e $q(x) \in \mathbb{R}[x] \Rightarrow p+q \in \mathbb{R}[x]$

—> Se $p(x) = a_0 + a_1 x + \dots + a_n x^n$ e $q(x) = b_0 + b_1 x + \dots + b_r x^r$

=> $(p+q)(x) = a_0 + a_1 x^1 + \dots + a_n x^n + b_0 + b_1 x^1 + \dots + b_r x^r$ è un polinomio di grado il $\max\{r, n\}$

$(\mathbb{R}[x] ; +)$ è un gruppo commutativo (DA DIMOSTRARE)

Su un insieme Q definisco due operazioni "$*$" e "$\square$" e voglio verificare che valgano le seguenti proprietà:

1) $(Q ; *)$ sia un gruppo commutativo;

2) "$\square$" sia associativa;

3) deve valere la distributività: $\forall a_1, a_2, a_3 \in Q \Rightarrow a_1 \square (a_2 * a_3) = (a_1 \square a_2) * (a_1 \square a_3)$

Se valgono le tre proprietà => $(Q ; *, \square)$ è detta ANELLO

- Se $\exists$ elemento neutro in Q per "$\square$" => $(Q ; *, \square)$ è anello con unità
- Se vale per "$\square$" la commutatività => $(Q ; *, \square)$ è anello commutativo

Se per "$*$" e "$\square$" definite su G valgono le proprietà:

1) $(G, *)$ sia un gruppo commutativo;

2) $(G - \{\text{elemento neutro di } "*"\}, \square)$ sia gruppo;

3) Vale la proprietà distributiva di "$\square$" rispetto a "$*$"

$\Rightarrow (G, *, \square)$ è un **CORPO**

Un corpo nel quale vale la proprietà commutativa per "$\square$" $\Rightarrow$

$\Rightarrow (G, *, \square)$ è detto CAMPO.

ESERCIZIO

STUDIARE LE SEGUENTI STRUTTURE ALGEBRICHE:

$(\mathbb{Z}; +, \cdot)$; $(\mathbb{Q}; +, \cdot)$; $(\mathbb{R}; +, \cdot)$