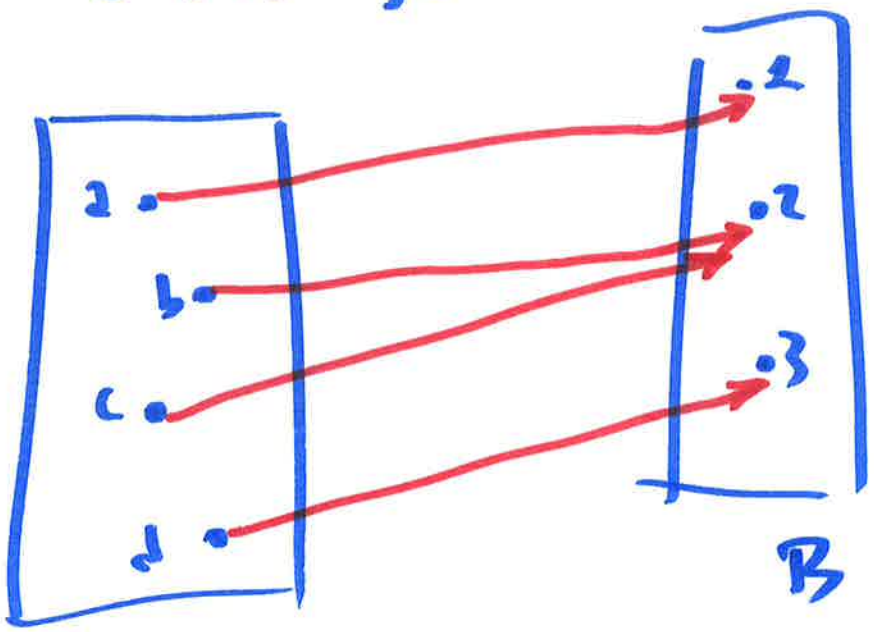
Funzione $f: A \to B$ è una corrispondenza funzionale ed ovunque definita $f \subseteq A \times B$ tale che $\forall a \in A \; \exists! b \in B$ con $(a,b) \in f$.

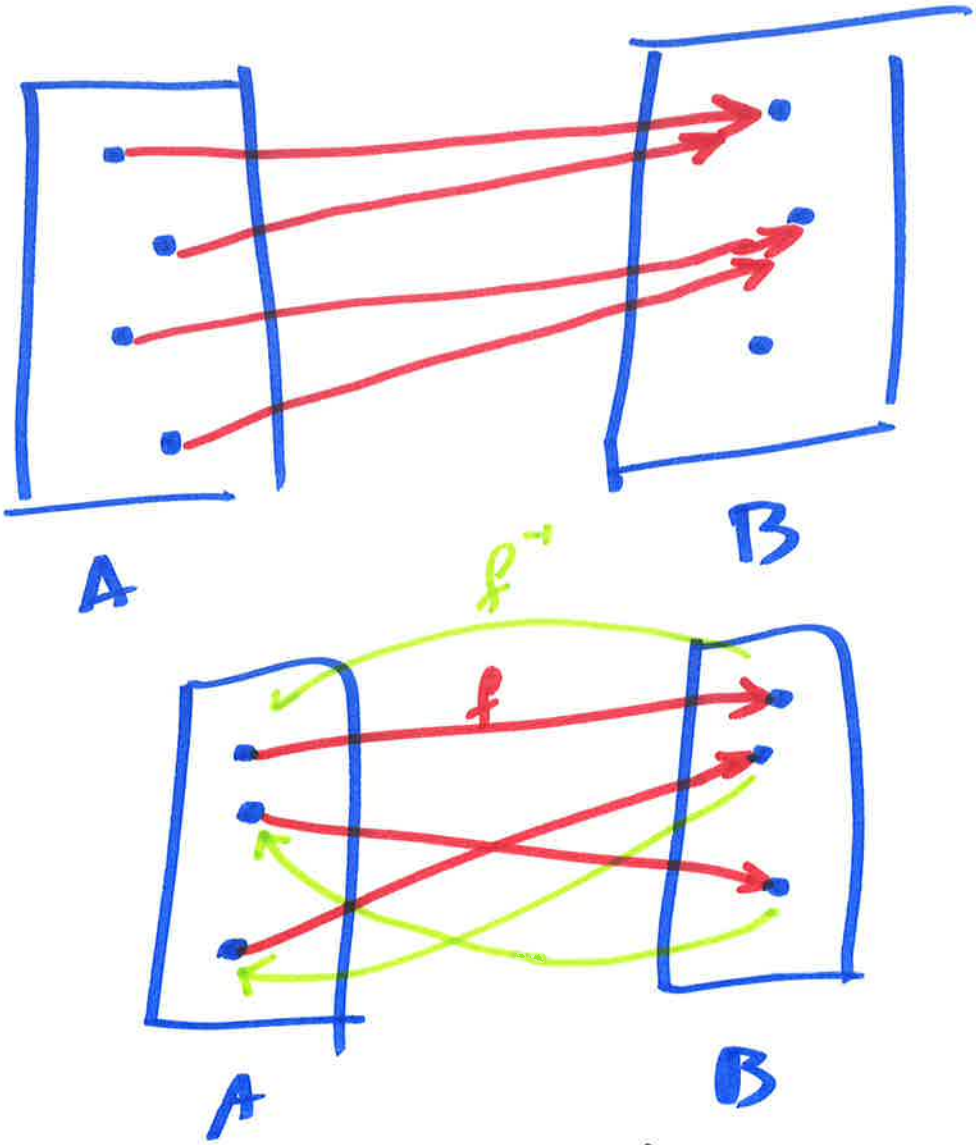


$x \to y$ se e solo se $(x,y) \in f$

Sia $X \subseteq A \times B$ si dice ${}^{t}X$ il sottoinsieme ${}^{t}X = \{(b,a) \in B \times A \mid (a,b) \in X\}$.

↑ trasposto di X

Oss: Sia $f \subseteq A \times B$ una funzione $\Rightarrow {}^t f$ è una funzione $\Leftrightarrow$ f è biiettiva.



Se f è biiettiva $\Rightarrow {}^t f$ è la funzione inversa di f e si denota con f^{-1}

Def: Siano $f: A \to B$ e $g: B \to C$ due funzioni.
Si dice funzione composta

$$(g \circ f) : A \longrightarrow C$$

$$(g \circ f) := \{(a,c) \in A \times C : \exists b \in B \text{ con } (a,b) \in f \ \& \ (b,c) \in g\}.$$

$$(g \circ f)(x) = g(f(x))$$

N.B f e g si possono comporre $\Leftrightarrow$ il codominio di f coincide col dominio di g.

Sia A un insieme

Una funzione $\iota_A : A \to A$ è detta funzione identica se

$\forall a \in A : \iota_A(a) = a$

Sia adesso $f : A \to B$ biiettiva.

$\Rightarrow f^{-1} \circ f : A \to A$ è la funzione identica su A e

$f \circ f^{-1} : B \to B$ è

la funzione identica su B.

N.B $f^{-1} \circ f \neq f \circ f^{-1}$

La composizione di funzioni NON è COMMUTATIVA!

Siano $f: A \to B$ $g: B \to C$

$h: C \to D$

tre funzioni $\Rightarrow$

$$h \circ (g \circ f) : A \to D$$

$$= (h \circ g) \circ f : A \to D$$

Esercizio: DIMOSTRARE CHE EFFETTIVAMENTE

$$h \circ (g \circ f) = (h \circ g) \circ f$$

IL PRODOTTO/ DI FUNZIONI COMPOSIZIONE

È ASSOCIATIVO

$$h \circ g \circ f$$

Richiamo le nozioni di sequenza e insieme.

sequenza → lista ordinata di oggetti.

Se A è un insieme, definiamo come A^n l'insieme di tutte le sequenze di n elementi di A.

$$\begin{cases} A^1 = A \\ \forall n \geq 2: \; A^n = A^{n-1} \times A \end{cases}$$

$$A^2 = A \times A$$

$$A^3 = A^2 \times A = (A \times A) \times A$$

$$A^4 = A^3 \times A = ((A \times A) \times A) \times A \quad \text{etc.}$$

$((a_1, a_2), a_3)$

$$A \times (A \times A) = \{(a_1, (a_2, a_3)) \dots\}.$$

$$A \times A \times A = \{(a_1\, a_2\, a_3) \mid a_i \in A\}.$$

A^n

N.B Noi possiamo vedere ~~A~~ le n-uple anche come una funzione

$$\{1, 2 \dots, n\} \to A$$

$$(1, a_1)$$
$$\vdots$$
$$(n, a_n)$$

Una n-upla è una "struttura dati" accessibile con un indice

$i \in \{1 \dots n\}$

↓

di elementi di A

$(A \times A) \times A$

$A \times (A \times A)$

$\{ \{1,2,3\} \xrightarrow{f} A \}$.

in tutti e 3 i casi

le proprietà che ci interessano

(ovvero di avere n elementi

in un ordine prefissato con

possibili ripetizioni)

valgono.

↘ le strutture sono

isomorfe

In particolare la seq.

$(a_1 a_2 \dots a_n)$ è la seq. in cui

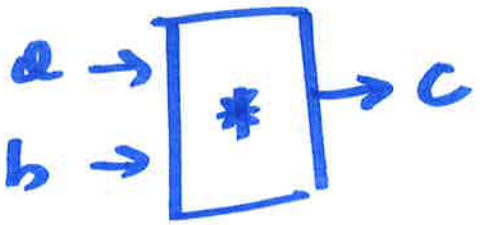
l'i-esimo elemento è a:

Struttura Algebrica

- OPERAZIONE * su DI UN INSIEME A

→ ~~[illegible]~~ $*: A \times A \longrightarrow A$

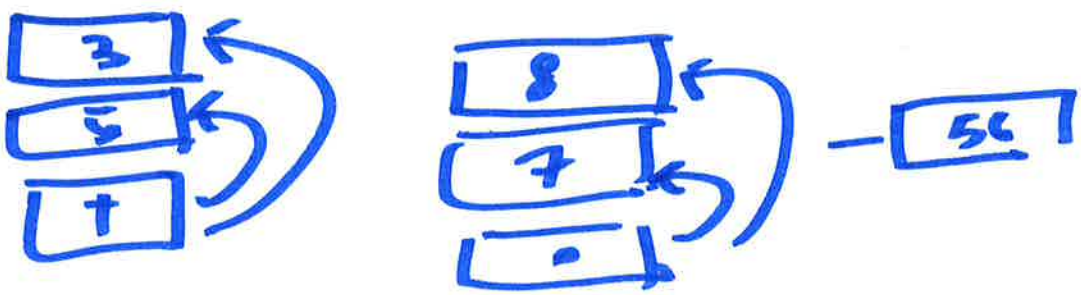
funzione da $A \times A \to A$.



$* \subseteq (A \times A) \times A$ $\quad *(a,b) = c$

$a * b = c$

$(3+5)\cdot 7$ $\qquad$ 3,5+7·



Esempio

$\mathbb{N}$ = insieme numeri naturali incluso 0.

$+ : (a,b) \longrightarrow a+b.$

$\cdot : (a,b) \longrightarrow a \cdot b.$

OPERAZIONI

$$\dot{-} : \begin{cases} \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (a,b) \longrightarrow \begin{cases} a-b \text{ se } a \geq b \\ b-a \text{ se } a < b. \end{cases} \end{cases}$$

$\mathbb{Z}$ = insieme dei numeri interi

Def: Si dice struttura algebrica una n-upla formata da un insieme A e da una o più [(n-1) in particolare] operazioni su A.

Es. $(\mathbb{N}, +)$ $(\mathbb{Z}, +)$

$(\mathbb{N}, \cdot)$ $(\mathbb{Z}, \cdot)$

$(\mathbb{Q}, +)$ $(\mathbb{Q}, \cdot)$

$(\mathbb{R}, +)$ $(\mathbb{R}, \cdot)$.

$(\mathbb{C}, +)$ $(\mathbb{C}, \cdot)$

•) Una operazione $*: A \times A \to A$ ammette elemento neutro $e \in A$ se $\forall a \in A: a * e = e * a = a$

ESEMPIO: $(\mathbb{N}, +)$ ammette 0 come el. neutro.

N.B: Se esiste l'elemento neutro è unico. Infatti se e, e' fossero 2 el. neutri distinti

$$\Rightarrow e = e * e' = e'$$

↑ perché e' el. neutro

↑ perché e el. neutro.

..) Una operazione $*$ è associativa se $\forall a, b, c \in A$

$$a * (b * c) = (a * b) * c.$$

$(\mathbb{N}, +)$ $\quad (a+b)+c = a+(b+c)$.

N.B $(\mathbb{Z}, -)$ non è associativa.

$$a-(b-c) = (a-b)+c \neq$$

$$(a-b)-c$$

∴) Una operazione $*$ è commutativa (o Abeliana) se $\forall a, b \in A$

$$a * b = b * a$$

$(\mathbb{N}, +)$ è commutativa.

$(\mathbb{N}, \cdot)$ è commutativa.

Es. non commutativo:

Sia X un insieme

$$S(X) = \{ f : X \to X \mid X \text{ è biiettiva} \}.$$

$(S(X), \circ)$

↑ composizione di funzioni.

<u>OSS</u>. Se $f, g \in S(X) \Rightarrow g \circ f \in S(X)$

$\exists\, \iota \in S(X) : \iota(x) = x \quad \forall x \in X$

funzione identica

$(f \circ \iota) = f \qquad \iota \circ f = f$

$\forall f \in S(X)$

ι è l'identità per $(S(X), \circ)$

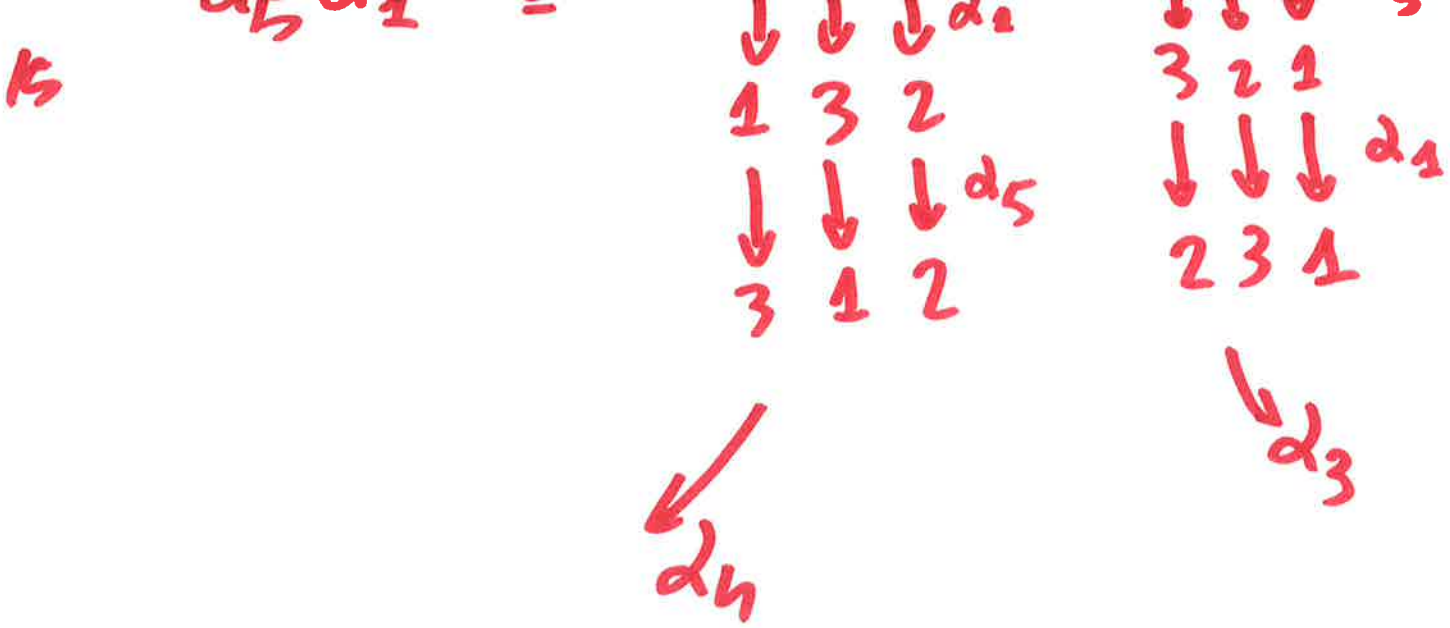
- la composizione di funzioni è associativa.
- la composizione di funzioni non è commutativa.

Es. $X = \{1, 2, 3\}$.

$S(X)$ $\iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$\alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$



$(\mathbb{N}, +)$ el. neutro
prop. associativa
prop. commutativa.

$\forall a, b \in \mathbb{N} \quad a + b \geq \max(a, b)$

Def: In una struttura algebrica $(A, *)$ sia $a \in A$ e supponiamo che esista el. neutro e.
Si dice <u>inverso</u> di a (se esiste) un $b \in A$ tale che
$a * b = b * a = e$

Si dice che esistono gli inversi in $(A,*)$ se $\forall a \in A \ \exists \bar{a}$ tale che $a * \bar{a} = \bar{a} * a = e$ (e ogni el. ammette inverso).

Es. $(\mathbb{N},+)$ → l'unico el. che ammette inverso è 0

$0+0=0$

$a>0$

$(\mathbb{N},\cdot)$ → l'unico el. che ammette inverso è 1

$(\mathbb{Z},+)$ → ogni elemento $a \in \mathbb{Z}$ ammette inverso $(-a)$

$(\mathbb{Z}, \cdot)$ → gli unici 2 elementi che ammettono inverso sono $+1$ e -1

$(\mathbb{Q}, +)$ → ogni el. ammette inverso.

$(\mathbb{Q}, \cdot)$ → ogni elemento diverso da 0 ammette inverso.

pongo $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$.

$\mathbb{R}^* := \mathbb{R} \setminus \{0\}$.

$\mathbb{C}^* := \mathbb{C} \setminus \{0\}$.

$(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$

ogni elemento ammette inverso.

In $S(X)$ ogni elemento ammette inverso.

Def: Una struttura algebrica $(A, *)$ è detta **gruppo** se

1) $\exists$ elemento neutro $e \in A$:
$\forall a \in A: a*e = e*a = a$

2) Ogni elemento di A ammette inverso.
$\forall a \in A \; \exists \bar{a} \in A:$
$a*\bar{a} = \bar{a}*a = e$

3) Vale la proprietà associativa.
$\forall a,b,c \in A: a*(b*c) = (a*b)*c$

Un gruppo è **abeliano** (o commutativo) se $\forall a,b \in A: a*b = b*a$

NON ABELIANO ↓

$(\mathbb{Z},+)$, $(\mathbb{Q},+)$ $(\mathbb{R},+)$ $(\mathbb{C},+)$ $S(x)$
$(\mathbb{Q}^*,\cdot)$ $(\mathbb{R}^*,\cdot)$ $(\mathbb{C}^*,\cdot)$

$\mathbb{F}_2 = \{0, 1\}$.

+	0	1
0	0	1
1	1	0

$(\mathbb{F}_2, +)$ è un gruppo

$\mathbb{F}_2 \setminus \{0\} = \{1\}$.

·	1
1	1

$(\mathbb{F}_2 \setminus \{0\}, \cdot)$ è un gruppo

$(\mathbb{Z}, +, \cdot)$ $\left\{\right.$ $(\mathbb{Q}, +, \cdot)$ $(\mathbb{R}, +, \cdot)$ $(\mathbb{C}, +, \cdot)$ $\left.\right.$ $(\mathbb{F}_2, +, \cdot)$

Def: Una struttura algebrica $(A, \tilde{+}, \tilde{\cdot})$ è detta anello se

1) $(A, \tilde{+})$ è un gruppo abeliano.

2) $(A, \tilde{\cdot})$ vale la proprietà associativa.

3) Valgono le proprietà distributive.

$\forall a, b, c \in A$:

$$(a \tilde{+} b) \tilde{\cdot} c = (a \tilde{\cdot} c) \tilde{+} (b \tilde{\cdot} c)$$

$$a \tilde{\cdot} (b \tilde{+} c) = (a \tilde{\cdot} b) \tilde{+} (a \tilde{\cdot} c).$$

→ Un anello è detto con unità se $(A, \tilde{\cdot})$ ammette elemento neutro.

→ Un anello è commutativo se $(A, \tilde{\cdot})$ è commutativo.

→ Un anello commutativo con unità è un CAMPO se posto $\tilde{0}$ l'elemento neutro $\tilde{+}$, $(A \setminus \{\tilde{0}\}, \tilde{\cdot})$ è un gruppo abeliano.

OSS: l'elemento $\tilde{0}$ non è mai invertibile in un anello.

Supponiamo

$$\tilde{0} \cdot a = \tilde{1} \Rightarrow$$

$$\Rightarrow (\tilde{0} \cdot a) = (\tilde{0} + \tilde{0}) \cdot a =$$

$$\Rightarrow \boxed{(\tilde{0} \cdot a)} = (\tilde{0} \cdot a) + \boxed{(\tilde{0} \cdot a)}$$

$$\Rightarrow \tilde{0} \cdot a = \tilde{0}$$

$$\| \quad \lightning$$

$$\tilde{1}$$

$$\Rightarrow \tilde{0} = \tilde{1} \text{ e } \forall a \in A \quad a \cdot \tilde{0} = \tilde{0}$$

NE SEGUE $A = \{\tilde{0}\}$.

Esempi di CAMPO

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

$(\mathbb{C}, +, \cdot)$

NON É CAMPO MA ANELLO

$(\mathbb{Z}, +, \cdot)$

Esempio di campo

+	0	1
0	0	1
1	1	0

XOR

·	0	1
0	0	0
1	0	1

AND.

$(\mathbb{F}_2, +, \cdot)$

15 $\mathbb{F}_5 = \{0\,1\,2\,3\,4\}$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$(\mathbb{F}_5, \dot{+}, \dot{\cdot})$

$a \dot{+} b := (a+b)\,\%\,5$

$(a \dot{\cdot} b) = (a \cdot b)\,\%\,5$

↑ divido per 5 e prendo il resto.

$\mathbb{Z}_6$

·	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Def di spazio vettoriale.

→ Vogliamo poter lavorare su n-uple di elementi.

Sia $(V, \oplus)$ un gruppo abeliano.

Si dice che $(V, \oplus)$ è uno spazio vettoriale su di un campo $(\mathbb{K}, +, \cdot)$ rispetto il prodotto per scalare

$$* : \mathbb{K} \times V \longrightarrow V$$

se valgono le seguenti proprietà

zz $\forall \bar{v} \in V, \alpha, \beta \in \mathbb{K}$

1) $1 * \bar{v} = \bar{v}$

2) $\forall \alpha, \beta \in \mathbb{K}, \forall \bar{v} \in V$

$(\alpha + \beta) * \bar{v} = \alpha * \bar{v} \oplus \beta * \bar{v}$

3) $(\alpha \cdot \beta) * \bar{v} = \alpha * (\beta * \bar{v})$

4) $\forall \alpha \in \mathbb{K}, \forall \bar{v}, \bar{w} \in V$:

$\alpha * (\bar{v} \oplus \bar{w}) = (\alpha * \bar{v}) \oplus (\alpha * \bar{w})$