→ Ensembles, structures, complexes

{ Mathématiques cours 1 }

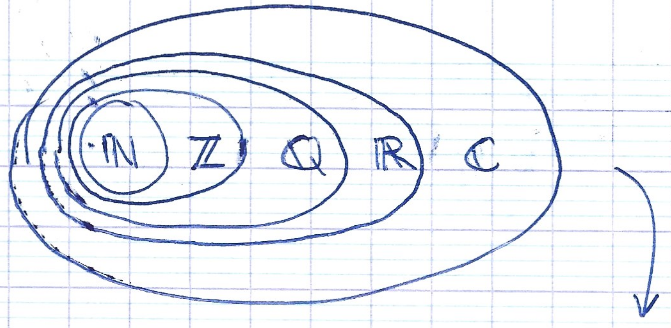
Ensembles de nombres :

−

apparus progressivement.

- $\mathbb{N} \rightarrow (0 ; 1 ; 2 \dots ; n)$ ensemble des entiers naturels.
- $\mathbb{Z} \rightarrow (-n \dots ; -1 ; 0 ; 1 ; \dots n)$ ensemble des entiers relatifs.
  ↳ solutionne les équations $x = b - a$ où $(b ; a) \in \mathbb{N}$
- $\mathbb{Q}$ ensemble des rationnels $\left(\frac{a}{b}\right)$ où $(a ; b) \in \mathbb{Z}$
  - ↳ sous ensemble des décimaux $\mathbb{D}$ $(\mathbb{D} \in \mathbb{Q})$
    - ↳ $\left[x \in \mathbb{Q} ; \exists n \in \mathbb{N} \Rightarrow 10^n x \in \mathbb{Z} \right.$ alors $\left. x \in \mathbb{D} \right]$
    - ↳ sous ensemble des diadiques $(\mathbb{D}_i \in \mathbb{D})$
      ↳ $\left[x \in \mathbb{Q} ; \exists n \in \mathbb{N} \Rightarrow 2^n x \in \mathbb{Z} \right.$ alors $\left. x \in \mathbb{D}_i \right]$
- $\mathbb{R}$ ensemble des nombres réels. $(\pi, e, \sqrt{2}, \varphi \dots)$
- $\mathbb{C}$ ensemble des nombres complexes.
  ↳ solutionne $x^2 + 1 = 0$

+



donc $\mathbb{N} \in \mathbb{Z}$; $\mathbb{Z} \in \mathbb{Q}$; $\mathbb{Q} \in \mathbb{R}$; $\mathbb{R} \in \mathbb{C}$

- problème de $\mathbb{N}$: $a+x=b$ n'a pas de solutions dans $\mathbb{N}$ si $a>b$
- problème de $\mathbb{Z}$: $a \times x = b$ n'a pas de solution dans $\mathbb{Z}$ si b n'est pas multiple de a.
- problème de $\mathbb{Q}$: $x^2 = a$ n'a souvent pas de solution (par exemple $a=2$)
- problème de $\mathbb{R}$: $x^2+a=0$ n'a pas de solutions si $a>0$.

$\downarrow$

2 solutions dans $\mathbb{C}$. si $a=-1$; $S = \{-i ; i\}$

définition de $\mathbb{C}$:

posons $\mathbb{C} = \mathbb{R}^2 = \{(a;b) \mid a \in \mathbb{R}$ et $b \in \mathbb{R}\}$

$\mathbb{R} \times \mathbb{R}$ = produit carthésien (def par descartes).

On définis 2 lois de composition interne.

↳

$$\left[\begin{array}{ll} \text{l'addition :} & (a;b)+(c;d)=(a+c;b+d) \\ \text{la multiplication :} & (a;b)\times(c;d)=(ac-bd;ad+bc) \end{array}\right]$$

On définis également une multiplication externe :

$a \in \mathbb{R}$; $a(b;c) = (ab;ac)$

$+ : \mathbb{C}^2 \longmapsto \mathbb{C}$	$\times : \mathbb{C}^2 \longmapsto \mathbb{C}$	$\times_e : \mathbb{R} \times \mathbb{C} \longrightarrow \mathbb{C}$

Définition :

Si E est un ensemble, alors la fonction f :
$f : E^2 \longmapsto E$, est appelée une loi de composition interne. (LCI)

Remarque.

relation ifixe.

On écrit souvent $x \, f \, y$ au lieu de $f(x;y)$

exemple : $x+y$ au lieu de $+(x;y)$

On pose par convention $i = (0;1)$

les complexes $(x;0)$ se comportent comme des réels.

on identifie $(x;a)$ et r.

$(a;b) \in \mathbb{C}$;

$$(a;b) = (a;0) + (0;b)$$

$$(a;b) = a + b(0;1)$$

$$\underbrace{(a;b)}_{\text{afixe.}} = \underbrace{a+ib}_{\text{algébrique}}.$$

$\mathbb{R} \in \mathbb{C}$ avec la convention dérivée et $+, \times$ sur $\mathbb{C}$ sont des prolongements de $+, \times$ dans $\mathbb{R}$

↳ On utilise les mêmes symboles dans $\mathbb{R}$ et $\mathbb{C}$

Def : $f : \underset{\overset{\uparrow}{\text{source}}}{A} \longmapsto \underset{\overset{\uparrow}{\text{but}}}{B}$ est une f°

si à tout élément x de A elle associe un unique élément y de B. donc :

$$\underset{\overset{\nearrow}{\text{image}}}{y} = \underset{\overset{\uparrow}{\text{un antécédant de } y \text{ par } f.}}{f(x)}$$

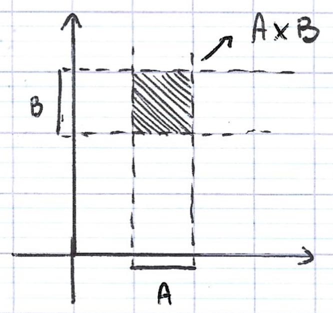
exemple : $f : \mathbb{R} \mapsto [-1 ; 1]$ $f(x) = \sin(x)$

alors 2 n'a pas d'antecedants.
0 à pour antecedants tout elements de l'ensemble des $k\pi$ → $\{k\pi \mid k \in \mathbb{Z}\}$ (appelé $\pi\mathbb{Z}$)

Def : $f(A) = \{f(x) \mid x \in \mathbb{R}\}$ est appelé ensemble image de f.

exemple : ensemble image d'e^x.

$\{e^x \mid x \in \mathbb{R}\} = \mathbb{R}^*_+$



Def. si A, B 2 ensembles.

$$A \times B = \underset{\overset{\uparrow}{\text{ensemble de}}}{\{}(a ; b) \underset{\overset{\uparrow}{\text{tel que}}}{\mid} a \in A, b \in B\}$$

Def: $B = \left\{ \begin{vmatrix} \text{true} \\ \text{oui} \\ \text{vrai} \end{vmatrix} ; \begin{vmatrix} \text{false} \\ \text{non} \\ \text{faux} \end{vmatrix} \right\}$ est l'ensemble des bouléens.

$f : E \mapsto B$ est un prédicat sur E

exemples: $f = \mathbb{R} \mapsto B$; $\overset{\text{bouléen}}{f(x)} \Leftrightarrow \overset{\text{bouléen}}{x \geq 0}$

égalité dans les bouléens.

$g : \mathbb{R}^2 \mapsto B \;\Big|\; f(x;y) \Leftrightarrow \underbrace{\begin{cases} x \geq 0 \\ y \geq 0 \end{cases}}_{B^2 \mapsto B}$

les fonctions "et" et "ou" sont des LCI prédicats.

def : $f : A^2 \mapsto A$ $\quad f((x;y))$ est noté $f(x;y)$

on dit que f est une fonction 2 variable.

on utilise souvent la notation infixe : $x f y$

exemple :

$+ : \mathbb{N}^2 \mapsto \mathbb{N}$ est une LCI sur $\mathbb{N}$.

$1+3 = +(1;3)$.

il existe d'autres notations.

$\%(a;b) = \dfrac{a}{b}$

$\% : \mathbb{R} \times \mathbb{R}^*$

$$\frac{x}{\frac{a}{b} + c} = \%(x ; +(5 ; \%(a;b)))$$

def = $f : A \mapsto B$ $g : B \mapsto C$

on def $g \times f : A \mapsto C$ par

$\forall x \in A$ $g \circ f(x) = g(f(x))$

$\circ$ s'appelle la composition.

exemple : $\cos^2(x) =$ carré $(\cos(x))$ = carré $\circ \cos(x)$

VOCABULAIRE LCI

$\boxed{*} \rightarrow * : A^2 \mapsto A$

Def :

$e \in A$ est un neutre pour $*$ si $\forall x \in A$ $x * e = x$ ①

$e \in A$ est un neutre pour $*$ si $\forall x \in A$ $e * x = x$ ②

théorème :

le neutre, s'il existe est unique.

soit $* : A^2 \mapsto A$ Un neutre pour $*$ s'il existe, doit être unique.

preuve :

soit e_1, e_2 2 neutres pour $*$

$$e_1 \overset{①}{=} e_1 * e_2 \overset{②}{=} e_2 \qquad e_1 = e_2$$

par transitivité de l'égalité ↗ ainsi le neutre est unique.

7

Une LCI n'a pas forcément un neutre.

$+ : \mathbb{N}^{*2} \mapsto \mathbb{N}^*$

~~[illegible] $\square : A^2 \mapsto A$ $A+x$~~

Def : $(E ; *)$ où $*$ est une LCI est appelé un magma

muni de

si $(E ; *)$ est un magma de nature e

on dit que $x \in E$ est inversible par x si et si il existe $x' \in E$

tel que $x * x' = x' * x = \underset{}{e}$ neutre de $*$

(pas rigoureux ↑ :)

$$\begin{cases} x * x' = e \\ x' * x = e \end{cases}$$ mieux

ici, x' est un inverse.

dans $(\mathbb{R} ; +)$ l'inverse pour $+$ de x est $-x$
(opposé de x)

dans $(\mathbb{R} ; \times)$ l'inverse de x pour $\times$ est $\frac{1}{x}$
(inverse de x)

def : $* : E^2 \mapsto E$ est associative si

$$\forall (x ; y ; z) \in E^3 \text{ on a } x*(y*z) = (x*y)*z$$

ex : $(\mathbb{N} ; +)$ est associative $a+(b+c) = (a+b)+c$

$(\mathbb{N} ; \times)$ est associative $a \times (b \times c) = (a \times b) \times c$

$(\mathbb{R} ; \%)$ en général $\dfrac{\frac{a}{b}}{c} \neq \dfrac{a}{\frac{b}{c}}$

où $c \neq 0 ; b \neq 0$ $\iff$ $\dfrac{a}{bc} \neq \dfrac{ac}{b}$

La division n'a pas de neutre

Def: un magma $(E ; *)$ est appelé un monoïde si et seulement si il possède un neutre et est associatif.

ex : $(\mathbb{N} ; +)$ est un monoïde. seul inversible est 0
$(\mathbb{N} ; \times)$ est un monoïde
$(\mathbb{N}^* ; \%)$ n'est pas un monoïde. (pas associatif)
$(\mathbb{Z} ; \times)$ est un monoïde l'ensemble des inversibles est $\{-1 ; 1\}$

$(\mathbb{Z} ; -)$ n'est pas un monoïde (pas associatif)

$$1-(2-3) \neq (1-2)-3$$
$$2 \neq -4$$

Propriété (théorème)

$(E ; *)$ un monoïde, si $x \in E$ est inversible, son inverse est unique.

On l'appelera $\boxed{x^{*-1}}$

preuve : soit x'_1 et x'_2 2 inverses de x par $*$

$x'_1 = x'_1 * e = x'_1 * (x * x'_2) = (x'_1 * x) * x'_2 = e * x'_2 = x'_2$
par transitivité de l'égalité.

Def: F^E est l'ensemble des fonctions de $E \to F$

propriété: $(E^E ; \overset{\text{composition}}{\circ})$ est un monoïde de neutre Id :

$(\forall x \in E \quad Id(x) = x)$

preuve: soit $f \in E^E$ soit $x \in E$ $(f \circ Id)(x) = f(Id(x)) = f(x)$

donc $f \circ Id = f$

$Id \circ f = f$

car $\forall x \in E$ $(Id \circ f)(x) = Id(f(x)) = f(x)$.

~~composition est associative car~~

ainsi: Id est bien le neutre de $(E^E ; \circ)$.

car $\left| \begin{array}{ll} \forall x \in E ; & f \circ Id(x) = f(x) \\ \forall f \in E^E & Id \circ f(x) = f(x) \end{array} \right.$

$$\left.\begin{array}{ll} f \circ (g \circ h)(x) & = f \circ (g(h(x))) = f(g(h(x))) \\ (f \circ g) \circ h(x) & = (f(g)(x)) \circ h = f(g(h(x))) \end{array}\right\} (f, g, h) \in (E^E)^3$$

alors $f \circ (g \circ h)(x) = (f \circ g) \circ h(x)$. $\forall x \in E$

par transitivité de l'égalité

ainsi: $\circ : E^E \to E$ est une fonction associative.

donc $(E^E ; \circ)$ est un monoïde car LCI + 1 seul neutre + associative.

Remarque : soit $(E ; *)$ un monoïde, Inv la f° qui à x inversible fait correspondre son inverse.

on pose E' l'ensemble des inversibles de E $(E' \in E)$

$\text{Inv} : E' \mapsto E'$ on a $\text{Inv} \circ \text{Inv} = \text{Id}$

$\forall x \in E' ; \text{Inv} \circ \text{Inv}(x) = x$

exemple : en $(\mathbb{R}, +)$ ici, $E = \mathbb{R}$ et $E' \mathbb{R}$

$\text{Inv}(x) = -x$, | $\text{Inv} \circ \text{Inv}(x) = x$

$\text{Inv} \circ \text{Inv} = \text{Id}.$ | $\text{Inv}(\text{Inv}(x)) = \text{Inv}(-x) = x.$

même chose avec $(\mathbb{R}^* ; \times)$

Propriété : $\forall (x;y) \in E'^2$ $\text{Inv}(x * y) = \text{Inv}(y) * \text{Inv}(x)$

preuve : $(x * y) * (\text{Inv}(y) * \text{Inv}(x))$
$= x * (y * \text{Inv}(y)) * \text{Inv}(x)$
$= x * e * \text{Inv}(x)$
$= x * \text{Inv}(x) = \boxed{e.}$

de même : $(\text{Inv}(y) * \text{Inv}(x)) * (x * y) = \boxed{e}$

donc $x * y$ est inversible d'inverse $\text{Inv}(y) * (\text{Inv}(x))$

exemple f et g inversibles pour $\circ$ des E^E

$(f \circ g)^{\circ -1} = g^{\circ -1} \circ f^{\circ -1}$ (applicable avec ↷ $(\mathbb{R} ; +) ; (\mathbb{R}^* ; \times)$)

propriété : Si $* : E^2 \mapsto E$ est associative

on définit une fonction $f : E^n \mapsto E$
définie par ~~$f(x_1 * x_2 * x_3 * x_4 \dots * x^n)$~~
$f(x_1 ; x_2 ; x \dots ; x_m) = x_1 * x_2 * \dots * x_n$

On adaptera les notations :

$\underset{i=1}{\overset{n}{*}} x$: pour $x_1 * x_2 * \dots * x_n$

Exemple de notation voisine :

sur $\mathbb{R}$: $\underset{i=1}{\overset{n}{+}} x_i = x_1 + x_2 + \dots x_m$ est notée $\sum_{i=1}^{n} x_i$

$\underset{i=1}{\overset{m}{\times}} x_i = x_1 \times x_2 \dots \times x_m$ est notée $\prod_{i=1}^{n} x_i$

si $m = 1$: $\underset{i=1}{\overset{1}{*}} x_i = x_1$

si $m = 0$: $\underset{i=1}{\overset{0}{*}} x_i = e \curvearrowright$ neutre du monoïde

exemple : $m! = \prod_{i=1}^{m} i$ $(E ; \times)$ de neutre $e = 1$.

$1! = \prod_{i=1}^{1} = 1$

$0! = \prod_{i=1}^{1} = e = \boxed{1}$

définition Si $(E ; *)$ est un monoïde et $x \in E, n \in \mathbb{N}$

on pose $x^{*n} = \underset{i=1}{\overset{n}{*}} x$
(l'itéré n fois de x par $*$)

e le neutre de $(E; *)$

Propriété : $x^{*0} = e$

$x^{*n} * x^{*m} = x^{*(n+m)}$

exemple $(\mathbb{R}; +)$ | $x^{+n} = nx$

$x^{+n} + x^{+m} = nx + mx = (n+m)x$

$(\mathbb{R}^*; \times)$ | $x^{\times n} = x^n$

$x^{\times n} \times x^{\times m} = x^n \times x^m = x^{n+m}$

Lien entre itéré et suite récurrente.

x_0 est donné, $f : E \to E$. $\forall n \in \mathbb{N}$ $x_{n+1} = f(x_n)$

$\forall n \in \mathbb{N}$, $x_n = f^{\circ n}(x_0)$

Ex : soit $f(x) = 4x + 3$. $f : \mathbb{R} \to \mathbb{R}$

$f^{\circ 10}(x) =$

$f(x) = 4x + 3$

$f(f(x)) = 4(4x+3)+3$

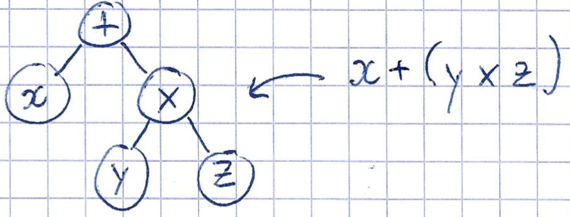
$f(f(f(x))) = 4(4(4x+3)+3+3$

$f^{\circ n}(x) = 4^n x + 4^n - 1$ $\begin{cases} \forall x \in \mathbb{R} \\ \forall n \in \mathbb{N} \end{cases}$

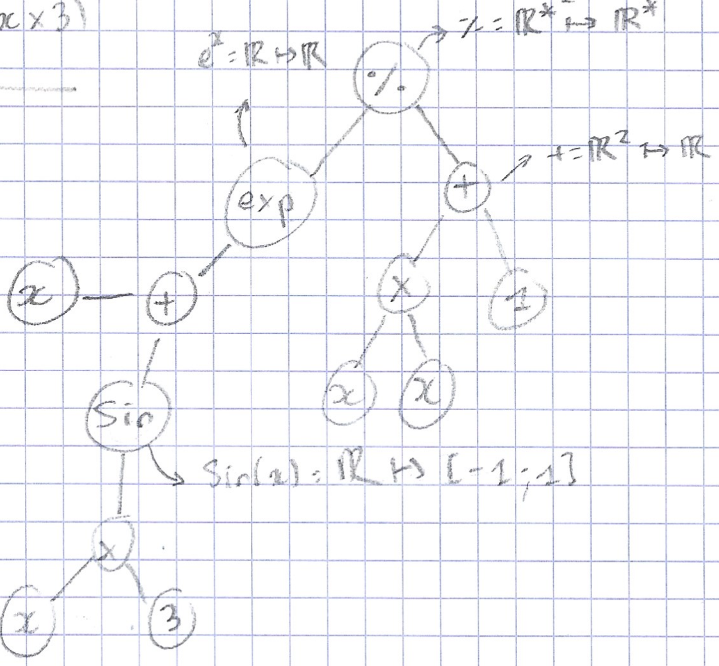
Remarque : On note $f^{[n]}(x) = f^{\circ n}(x)$ parfois.

REPRESENTATION DES FONCTIONS PAR LES GRAPHS

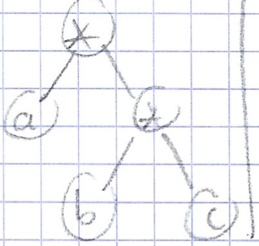
ex : $+ : \mathbb{R}^2 \mapsto \mathbb{R}$



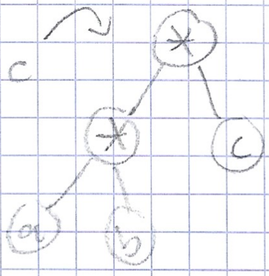
$$\frac{e^{x+\sin(x\times 3)}}{x^2+1}$$



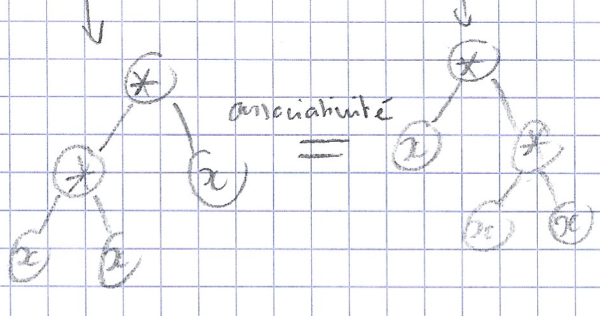
$a * (b * c) \longrightarrow$

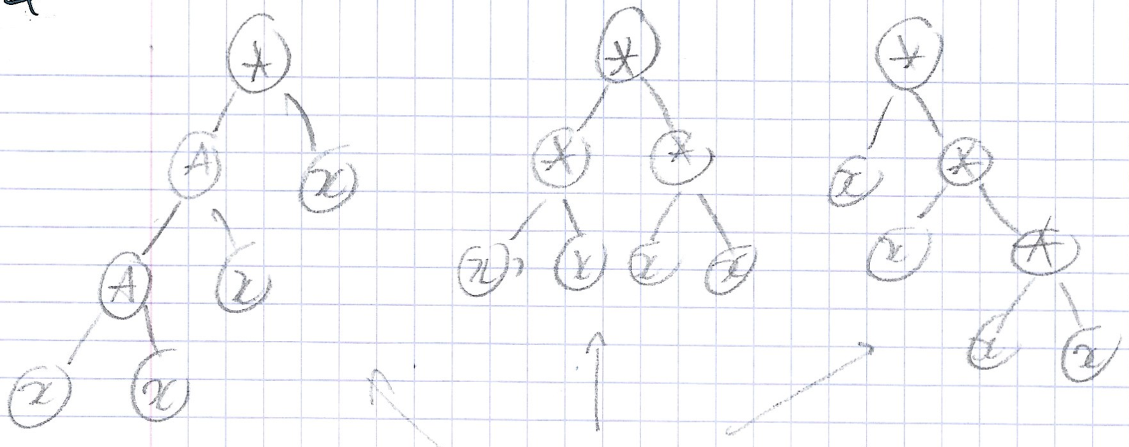


$(a * b) * c$



$x^{*3} = (x * x) * x = x * (x * x)$





3 arbres de x^{*4}

Définition : $(E;*)$ magma. $*$ est commutative si $\forall (x,y)\in E^2 \quad x*y = y*x$

exemples : $(\mathbb{R};\times)$, $(\mathbb{R}^{\mathbb{R}};\circ)$

↓ commutatif ↓ non commutatif

$4\times\pi = \pi\times 4$

$f : x\mapsto 2x \quad g : x\mapsto x^2$

$f\circ g = (2x)^2 \neq g\circ f = 2x^2$

Remarque : On utilise aussi "abélien" pour commutatif.

ex : $(\mathbb{R};+)$ est un monoïde abélien.

Définition : $\top : A^2 \mapsto A$ et $* : A^2 \mapsto A$

2 LCI dans A.

on dit que $*$ est distributive par rapport à $\top$ si $\forall (x;y;z)\in A^3$

$$\left|\begin{array}{l} x*(y\top z) = (x*y)\top(x*z) \\ (x\top y)*z = (x*z)\top(y*z) \end{array}\right|$$

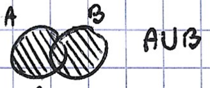
exemple : La multiplication est distributive par rapport à l'addition.

$\forall (x;y;z)\in\mathbb{R}^3 \quad x\times(y+z) = xy + xz$

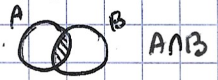
définition: soit E un ensemble, on appelle, on note

$\mathcal{P}(E)$ | l'ensemble des sous ensembles de E
l'ensemble des parties de E

$\cup$, l'union est une LCI sur $\mathcal{P}(E)$



$\cap$, l'intersection est une LCI sur $\mathcal{P}(E)$



Le neutre de l'union est l'ensemble vide.

ensemble vide

$(\mathcal{P}(E) ; \cup)$ est un monoïde abélien de neutre $\emptyset$

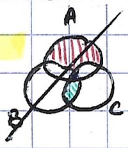
$(\mathcal{P}(E) ; \cap)$ est un monoïde abélien de neutre E

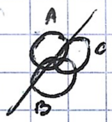
ensemble plein

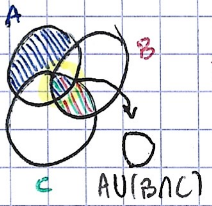
↳ ces neutres sont uniques et les seuls inversibles de ces monoïdes.

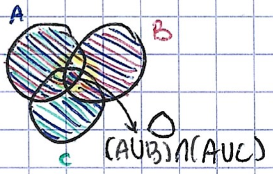
exemple: $\mathcal{P}(\{1;2;3\}) = \{\emptyset ; \{1\} ; \{2\} ; \{3\} ; \{1;2\} ; \{2;3\} ; \{1;3\} ; \{1;2;3\}\}$

propriété: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$



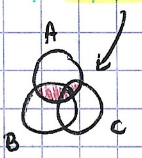


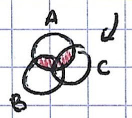




$\forall (A, B, C) \in \mathcal{P}(E)$

de même, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$





~~alors $\cup$ et $\cap$ distributifs dans $(E ; \cup)$ et $(E ; \cap)$~~

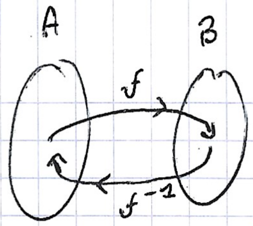
l'union est distributif par rapport à l'union et inversement.

définition: soit $f : A \mapsto B$ une fonction tel qu'il existe

$g \circ f : A \mapsto A$ $\quad g : B \mapsto A$ avec $f \circ g : B \mapsto B$

$g \circ f = Id_A$ $\quad f \circ g = Id_B$

On dit que f est une bijection de bijection réciproque g.
on notera f^{-1} (bijection réciproque de f)



On a : $\forall y \in B, \exists! x \in A$ tel que $f(x) = y$

f^{-1} est la fonction qui à $y \in B$ fait correspondre x l'unique antécédent de y par f

méthode : $y = f(x) \iff \dots \iff x = g(y)$ avec $g \circ f^{-1}$ et f est bijective.

exemple : $f(x) = 4x + 3$ montrer que ~~on a~~ : $f : \mathbb{R} \to \mathbb{R}$ est une bijection et trouver f^{-1}

$\iff y = 4x + 3$

$\iff y - 3 = 4x$

$\iff \frac{y-3}{4} = x$ → preuve de la bijectivité de f

$f^{-1}(y) = \frac{1}{4}y - \frac{3}{4} \quad \forall y \in \mathbb{R}$

$f^{-1} \circ f(x) = \frac{1}{4}(4x+3) - \frac{3}{4} = \frac{4}{4}x + \frac{3}{4} - \frac{3}{4} = x$

$f^{-1} \circ f(x) = x \quad \forall x \in \mathbb{R}$ donc $f^{-1} \circ f = Id_x$

$f \circ f^{-1}(y) = 4\left(\frac{1}{4}y - \frac{3}{4}\right) + 3 = \frac{4}{4}y - 3 + 3 = y \quad \forall y \in \mathbb{R}$

$f \circ f^{-1}(y) = y \quad \forall y \in \mathbb{R}$ donc $f \circ f^{-1} = Idy$

Prop : Dans le monoïde $(E^E ; \circ)$,

$f : E \mapsto E$ f est bijective (admet une bijection récipr.) si et seulement si f est inversible pour les composition. Et f^{-1} est l'expression de l'inverse.

$f^{-1} = f^{\circ -1}$

preuve : Les dit, coïncident $\exists g \in E^E$ tel que

$f \circ g = g \circ f = Id_E$

booliens

Definition: soit $f : E^2 \mapsto B$. f est une relation binaire

exemple: $(\mathbb{R}^2 ; =)$ la fonction égalité $(=)$ est une relation binaire.

Def: soit $R : E^2 \mapsto B$ est une relation binaire sur E

R est reflexive $\Leftrightarrow \forall x \in E \quad xRx$ est vrai

R est symétrique $\Leftrightarrow \forall (y;x) \in E^2 \quad xRy \Leftrightarrow yRx$

R est antisymétrique $\Leftrightarrow \forall (y;x) \in E^2 \quad xRy$ et $yRx \Rightarrow x = y$

R est transitive $\Leftrightarrow \forall (x;y;z) \in E^3 \quad xRy$ et $yRz \Rightarrow xRz$

exemple: la fonction égalité est : $= : \mathbb{R}^2 \mapsto B$

$(=) : B^2 \mapsto B$

reflechive: $\forall x \in \mathbb{R} \quad x = x$

symétrique : $\forall (x;y) \in \mathbb{R}^2 : x = y \Leftrightarrow y = x$

antisymétrique : $\forall (x;y) \in \mathbb{R}^2 : x = y$ et $y = x \Rightarrow x = y$

transitive : $\forall (x;y;z) \in \mathbb{R}^3 : x = y$ et $y = z$ alors $x = z$

~~l' inf~~

inferieur striche $< : \mathbb{R}^2 \mapsto B$

$\emptyset$ reflective $\quad \forall x \in \mathbb{R} \quad x < x \longrightarrow$ faux

$\emptyset$ symétrique $\quad \forall (x;y) \in \mathbb{R}^2 \quad x < y \Leftrightarrow y < x \rightarrow$ faux

$\emptyset$ antisymétrique $\forall (x;y) \in \mathbb{R}^2 \quad x < y$ et $y < x \Rightarrow x < y$ faux

transitive : $\forall (x;y;z)$: $x < y$ et $y < z$ alors $x < z \rightarrow$ vrai

définition: $f = A \mapsto B$ avec $(A;*)$ et $(B;\top)$ 2 monoïdes.

une fonction est un morphisme d'un monoïde si et si :

$\forall (x;y) \in A \quad \boxed{f(x * y) = f(x) \top f(y)}$

exemples: $Id : E \mapsto E$ est un morphisme de $(E;*)$ dans $(E;*)$ $\quad Id(x * y) = x * y = Id(x) * Id(y)$

ex : ~~f(3x)~~ $f(x)=3x$ est un morphisme de $(\mathbb{R};+)$ dans $(\mathbb{R};+)$

$f(x+y) = 3(x+y) = 3x+3y = f(x)+f(y)$ $\forall (x;y)\in\mathbb{R}^2$

$f\circ g(x) = a$ $g^{-1}\circ f^{-1}(a) = x$

ex : $\ln : \mathbb{R}_+^* \to \mathbb{R}$ vérifie $\ln(xy) = \ln(x)+\ln(y)$
ln est un morphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R};+)$

ex : $f : \mathbb{R} \to \mathbb{C}$ déf par $f(x) = e^{ix} = \cos(x)+i\sin(x)$
est un morphisme de $(\mathbb{R};+)$ dans $(\mathbb{C};\times)$

prop : Si $f : E \to F$ est un morphisme de $(E;*)$

si $f(e_1)$ inversible

→ vers $(F;T)$ deux monoïdes alors $\begin{cases} f(e_1) = e_2 \\ \forall n\in\mathbb{N} \quad f(x^{*n}) = f(x)^{Tn} \end{cases}$

si x est inversible : $f(x^{*-1}) = f(x)^{T-1}$

preuve : $f(e_1) = f(e_1 * e_1) = f(e_1)\,T\,f(e_1)$

$\iff f(e_1)^{T-1}\,T\,f(e_1) = f(e_1)^{T-1}\,T\,f(e_1)\,T\,f(e_1)$

$\iff e_2 = e_2\,T\,f(e_1)$

$\iff e_2 = f(e_1)$

soit $H_n \iff f(x^{*n}) = f(x)^{Tn}$

H_0 vrai car $x^{*0} = e_1$ et $f(x)^{T0} = e_2$ or $f(e_1) = e_2$

supposons H_α : $f(x^{*\alpha}) = f(x)^{T\alpha}$

$\Rightarrow f(x)\,T\,f(x^{*\alpha}) = f(x)^{T(\alpha+1)}$

$\Rightarrow f(x * x^{*\alpha}) = f(x)^{T(\alpha+1)}$

$\Rightarrow f(x^{*\alpha+1}) = f(x)^{T(\alpha+1)}$

$\Rightarrow H_{\alpha+1}$

Si x est inversible

$f(e_2) = e_2 \Rightarrow f(x * x^{-1}) = e_1 \Rightarrow f(x) \top f(x^{-1}) = e_2$

de même $f(x^{-1}) \top f(x) = e_2$ donc $f(x^{-1})$ est l'inverse de $f(x)$ par $\top$

exemple: si $f(x) = 3x$ $f : \mathbb{R} \mapsto \mathbb{R}$ $f(0) = 0$ avec $x^{+n} = nx$

$f(nx) = f(x)^{+n} \Rightarrow f(nx) = n f(x)$.

$f(x^{+-1}) = f(-x) = f(x)^{+-1} = -f(x)$

si $f(x) = x^2$ $f(1) = 1$ avec $x^{\times n} = x^n$

$f(x^{\times n}) = f(x^n) = f(x)^{\times n} = f(x)^n$

$f(x^{\times -1}) = f(\frac{1}{x}) = f(x)^{\times -1} = \frac{1}{f(x)}$

si $f : \mathbb{R} \mapsto \mathbb{C}$ $f(x) = e^{ix}$. ici f est un morphisme de $(\mathbb{R} ; +)$ dans $(\mathbb{C} ; \times)$

$\underline{f(0) = 1}$ → vrai.

$f(nx) = f(x)^n$ $\cos(nx) + i\sin(nx) = (\cos(x) + i\sin(x))^n$ (de Moivre)

$f(-x) = f(x^{-1}) \Leftrightarrow \cos(-x) + i\sin(-x) = \frac{1}{\cos(x) + i\sin(-x)}$

" " " $\Leftrightarrow$ [illegible] $\cos(x) - i\sin(x) = \frac{1}{\cos(x) + i\sin(x)}$

propriété : soit $(E ; *)$ un monoïde et $x \in E$

$f : \mathbb{N} \mapsto E$ def par $f : n = x^{*n}$

f est un morphisme de $(\mathbb{N} ; +)$ dans $(E ; *)$

preuve : En effet : $f(n + m) = x^{*(n+m)}$

avec $(n ; m) \in \mathbb{N}^2$ $f(n) \times (f(m)) = x^{*n} * x^{*m} = x^{*(n+m)}$

Remarque : si $(E ; *)$ est un monoïde Abélien

soit $f : E \mapsto E$ définie par $f_n : x \mapsto x^{*n}$

alors f_n est également un morphisme de $(E ; *)$

dans $(E ; *)$.

preuve : $f(x*y) = (x*y)^{*n} = x*y*x*y \dots *x*y$.

" " " $= x*x*x \dots *y*y*y$

" " " $= x^{*n} * y^{*n}$

" " " $= f(x) * f(y)$

définition : f morphisme de (E ; $*$) dans (E ; $*$) est un endomorphisme.

si en plus il est bijectif, c'est un automorphisme.

exemple $f(x) = x^2$ $f : \mathbb{R}_+ \to \mathbb{R}_+$ est un automorphisme de $(\mathbb{R}_+ ; \times)$

définition : f un morphisme bijectif de (E ; $*$) vers (F, T) est appelé un isomorphisme.

les structures principales :

définition : (E ; $*$) est un magma ssi $*$ est une LCI

définition : (E ; $*$) est un monoïde ssi c'est un magma associatif, et un neutre.

définition : (E ; $*$) est un groupe ssi c'est un monoïde dans lequel tout élément est inversible.

exemple de structure de groupe :

Dans un groupe $\text{Inv}(x) = x^{*-1}$ est une f° de $E \to E$.

et si $*$ est commutative, c'est un automorphisme de (E ; $*$)

preuve : $\text{Inv}(x*y) = \text{Inv}(x) * (\text{Inv}(y))$

En toute généralité, on a $\text{Inv}(x*y) = \text{Inv}(x) * \text{Inv}(y)$.

def: si x inversible dans le monoïde $(E ; *)$ alors on étend l'itéré par $\mathbb{Z}$

$$\forall n \in \mathbb{N},\ x^{*-n} = (x^{*-1})^{*n}$$

on a encore $\forall (n,m) \in \mathbb{Z}^2$ $x^{*(n+m)} = x^{*n} * x^{*m}$

c'est un morphisme de groupe

exemple: $2^{-5} = (2^{-1})^5 = \frac{1}{2^5}$

exemple: si $f \in E^E$ est une bijection on a par ex:

$$f^{\circ -2} = (f^{\circ -1})^2$$

propriété: si $x \in E$, $(E ; *)$ monoïde $(n ; m) \in \mathbb{N}$

$$(x^{*n})^{*m} = x^{*(n\times m)}$$

preuve:

$$\underbrace{\underbrace{(x*x\dots*x)}_{\substack{m\times x\\(x^{*n})}} * \dots * (x*x\dots*x)}_{m\text{ fois}} = x^{*(n\times m)}$$

$$(x^{*n})^{*m} = x^{*(n\times m)}$$

Exemple de groupe: $(\mathbb{Z} ; +)$ est un groupe

$(\mathbb{R}^* ; \times)$ est un groupe $(\mathbb{Q}^* ; \times)$ est un groupe

propriété: l'ensemble des inversibles d'un monoïde forme un groupe

preuve: $(x ; y) \in \hat{E}$ ou $\hat{E}$ est l'ensemble des inv. des monoïde $(E ; *)$

$x * y \in \hat{E}$ car $x * y$ a pour inverse $y^{*-1} * x^{*-1}$

$*$ est une LCI en $\hat{E}$

si $x \in \hat{E}$ $x^{*-1} \in \hat{E}$ car l'inverse de x^{*-1} est x

c'est donc un groupe (associativité et neutre) le gr des inversibles de $(\mathbb{N} ; \times)$ est $(\{1\} ; \times)$

$(\mathbb{Z} ; \times)$ est $(\{-1 ; 1\} ; \times)$

$(E^E ; \circ)$ est l'ensemble des fonctions bijectives de E dans E.

Remarque : si $E = [\![1 ; n]\!]$ $\mathfrak{B}(E ; E)$ est appelé le groupe des , groupe symétrique appelé parfois S_n

$$\sigma \in S_3 \qquad \sigma = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

Remarque : si $(E ; *)$ et $(F ; T)$ ~~st~~ sont 2 groupes et f un morphisme, alors :

$$\forall n \in \mathbb{Z} : f(x^{*n}) = f(x)^{Tn}$$

preuve : si $n < 0$ $f(x^{*n}) = f((x^{*-1})^{*-n}) = f(x^{*-1})^{T-n}$
$= f(x)^{Tn}$

si $g(n) = x^{*n}$ $g : \mathbb{Z} \to E$ est un morphisme de groupe de $(\mathbb{Z} ; +)$ dans $(E ; *)$

Définition : $(A ; + ; *)$ est un anneau si

- $(A ; +)$ est un groupe abelien
- $(A ; *)$ est un monoïde
- $*$ est distributive par rapport à l'addition.

Définition : $(A ; + ; *)$ est un corps si c'est un anneau tel que $(A - \{0\} ; *)$ est un groupe.

exemples : $(\mathbb{Z} ; + ; \times)$ est un anneau commutatif mais pas un corps.

en revanche $(\mathbb{Q} ; + ; \times)$ est un corps