

CHAPITRE 8

Ensemble relations et lois de compo

Hugo SALOU MP2I

Dernière mise à jour le 9 mai 2022

TABLE DES MATIÈRES

I	Théorie naïve des ensembles	2
II	Applications	7
III	Relations binaires	15
IV	Lois de composition	24
V	Divers	29

Première partie

Théorie naïve des ensembles

Définition: Un ensemble est une collection finie ou infinie d'objets de même nature ou non. L'ordre de ces objets n'a pas d'importance.

EXEMPLE: 1. $\{1, x \mapsto x^2, \{1\}\}$ est un ensemble : ses éléments sont l'entier 1, la fonction $x \mapsto x^2$ et un ensemble contenant uniquement 1 (un singleton).

2. \mathbb{N} est un ensemble infini

REMARQUE (Notation):

Soit E un ensemble et x un objet de E .

On écrit $x \in E$ ou bien $x \ni E$.

REMARQUE (Δ Paradoxe):

On note Ω l'ensemble de tous les ensembles. Alors, $\Omega \in \Omega$.

Ce n'est pas le cas de tous les ensembles :

$$\mathbb{N} \notin \mathbb{N} \text{ car } \mathbb{N} \text{ n'est pas un entier}$$

On distingue donc 2 types d'ensembles :

- ceux qui vérifient $E \notin E$, on dit qu'ils sont ordinaires
- ceux qui vérifient $E \in E$, on dit qu'ils sont extra-ordinaires

On note O l'ensemble de tous les ensembles ordinaires.

- Supposons O ordinaire. Alors, $O \notin O$
Or, O est ordinaire et donc $O \in O$ \nmid
- Supposons O extra-ordinaire.
Alors $O \in O$ et donc O ordinaire \nmid

C'est un paradoxe

Pour éviter ce type de paradoxe, on a donné une définition axiomatique qui explique quelles sont les opérations permettant de combiner des ensembles pour en faire un autre.

Définition: Soit E un ensemble et F un autre ensemble. On dit que E et F sont égaux (noté $E = F$) si E et F contiennent les mêmes objets.

EXEMPLE: 1. $E = \{1, 2, 3\}$ et $F = \{3, 2, 1, 2\}$

On a bien $E = F$.

2. $\mathbb{N} \neq \mathbb{Z}$ car $\begin{cases} -1 \in \mathbb{Z} \\ -1 \notin \mathbb{N} \end{cases}$

3. $E = \{0, \{0\}\} \neq \{0\} = F$

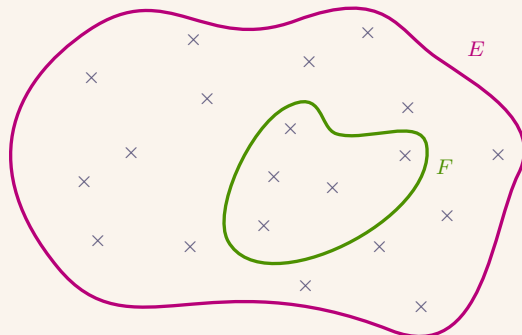
car $\begin{cases} \{0\} \in E \\ \{0\} \notin F \end{cases}$

mais, $F \in E$

Définition: L'ensemble vide, noté \emptyset est le seul ensemble à n'avoir aucun élément.

Définition: Soient E et F deux ensembles. On dit que F est inclus dans E , noté $F \subset E$ ou $E \supset F$ si tous les éléments de F sont aussi des éléments de E .

$$\forall x \in F, x \in E$$



Proposition: Pour tout ensemble E , $\emptyset \subset E$

Preuve (par l'absurde):

Si $\emptyset \not\subset E$ alors $\exists x \in \emptyset, x \notin E$: une contradiction \nmid

□

EXEMPLE: 1. $E = \{1, 2, 3\}$ et $F = \{1, 3\}$

On a $F \subset E$ mais pas $E \subset F$ car $\begin{cases} 2 \in E \\ 2 \notin F \end{cases}$

2. $F = \{0\}$ et $E = \{0, \{0\}\}$

— $F \in E$ car $\{0\} \in E$

— $F \subset E$ car $0 \in E$

3. $E = \{\{0\}\}$; $F = \{0\}$

— $F \not\subset E$ car $0 \notin E$

— $F \in E$

4. $E = \{\{\{0\}\}\}$; $F = \{0\}$

— $F \not\subset E$

— $F \not\in E$

— $\emptyset \subset F$

— $\emptyset \subset E$

Définition: Soit E un ensemble. On peut former l'ensemble de toutes les parties de E (une partie de E est un ensemble F avec $F \subset E$). On le note $\mathcal{P}(E)$

$$A \in \mathcal{P}(E) \iff A \subset E$$

EXEMPLE: 1. $E = \{42\}$

Les sous-ensembles de E sont \emptyset et $\{42\} = E$ donc

$$\mathcal{P}(E) = \{\emptyset, \{42\}\}$$

2. $\mathcal{P}(\emptyset) = \{\emptyset\}$

3. $E = \{0, 1\}$ donc $\mathcal{P}(E) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$

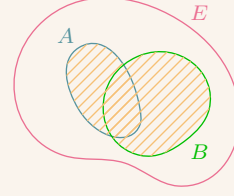
4. $E = \{\emptyset, \{\emptyset\}\}$ donc $\mathcal{P}(E) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$
5. $E = \{\emptyset, \{\emptyset\}\}$

$$\begin{aligned}\mathcal{P}(\mathcal{P}(E)) &= \mathcal{P}(\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, E) \\ &= \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \{E\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\{\emptyset\}\}\}, \{\emptyset, E\}, \{\{\emptyset\}, \{\{\emptyset\}\}\}, \{\{\emptyset\}, E\}, \{\{\{\emptyset\}\}, E\}, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}, \{\emptyset, \{\emptyset, E\}\}, \\ &\quad \{\emptyset, \{\{\emptyset\}\}, E\}, \{\{\emptyset\}, \{\{\emptyset\}\}, E\}, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}, \{\emptyset, \{\emptyset, E\}\}, \\ &\quad \{\emptyset, \{\{\emptyset\}\}, E\}, \{\{\emptyset\}, \{\{\emptyset\}\}, E\}, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, E\}\end{aligned}$$

Définition: Soit E un ensemble et $A, B \in \mathcal{P}(E)$

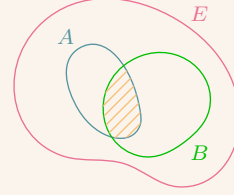
1. La réunion de A et B est

$$A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}$$



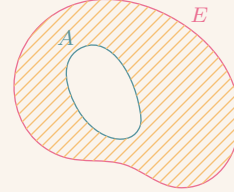
2. L'intersection de A et B est

$$A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\}$$



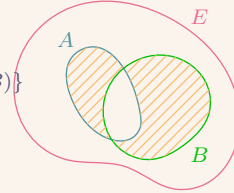
3. Le complémentaire de A dans E est

$$E \setminus A = \{x \in E \mid x \notin A\} = C_E A$$



4. La différence symétrique de A et B est

$$\begin{aligned}A \Delta B &= \{x \in E \mid (x \in A \text{ et } x \notin B) \text{ ou } (x \notin A \text{ et } x \in B)\} \\ &= (A \cup B) \setminus (A \cap B)\end{aligned}$$



Proposition: Soit E un ensemble et $A, B, C \in \mathcal{P}(E)$

- | | |
|--|---|
| 1. $A \cap A = A$ | 10. $A \cup E = E$ |
| 2. $B \cap A = A \cap B$ | 11. $(E \setminus A) \setminus A = E \setminus A$ |
| 3. $A \cap (B \cap C) = (A \cap B) \cap C$ | 12. $E \setminus (E \setminus A) = A$ |
| 4. $A \cap \emptyset = \emptyset$ | 13. $E \setminus \emptyset = E$ |
| 5. $A \cap E = A$ | 14. $E \setminus E = \emptyset$ |
| 6. $A \cup A = A$ | 15. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ |
| 7. $B \cup A = A \cup B$ | 16. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ |
| 8. $A \cup (B \cup C) = (A \cup B) \cup C$ | 17. $E \setminus (A \cup B) = (E \setminus A) \cap (E \setminus B)$ |
| 9. $A \cup \emptyset = A$ | 18. $E \setminus (A \cap B) = (E \setminus A) \cup (E \setminus B)$ |

Preuve: 16. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

— Soit $x \in A \cap (B \cup C)$ donc $x \in A$ et $x \in B \cup C$

CAS 1 $x \in B$, alors $x \in A \cap B$ et donc $x \in (A \cap B) \cup (A \cap C)$

CAS 2 $x \in C$, alors $x \in A \cap C$ et donc $x \in (A \cap B) \cup (A \cap C)$

On a prouvé

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$$

— Soit $x \in (A \cap B) \cup (A \cap C)$

CAS 1 $x \in A \cap B$ donc $x \in A$ et $x \in B$ donc $x \in B \cup C$ et donc $x \in A \cap (B \cup C)$

CAS 2 $x \in A \cap C$ donc $x \in A$ et $x \in C$ donc $x \in B \cup C$ et donc $x \in A \cap (B \cup C)$

On a prouvé

$$A \cap (B \cup C) \supset (A \cap B) \cup (A \cap C)$$

17. $E \setminus (A \cup B) = (E \setminus A) \cap (E \setminus B)$

— Montrons que $x \in E \setminus (A \cup B) \implies x \in (E \setminus A) \cap (E \setminus B)$

Soit $x \in E \setminus (A \cup B)$ donc $x \notin A \cup B$

— Si $x \in A$, alors $x \in A \cup B$ \nmid

donc $x \notin A$ i.e. $x \in E \setminus A$

— Si $x \in B$, alors, $x \in A \cup B$ \nmid

Donc $x \notin B$ i.e. $x \in E \setminus B$

On en déduit que $x \in (E \setminus A) \cap (E \setminus B)$

— $x \in (E \setminus A) \cap (E \setminus B)$. Montrons que $x \in E \setminus (A \cup B)$

On suppose que $x \notin E \setminus (A \cup B)$ donc $x \in A \cup B$

— Si $x \in A$, on a une contradiction car $x \in E \setminus A$

— Si $x \in B$, on a une contradiction car $x \in E \setminus B$

donc $x \in E \setminus (A \cup B)$

□

Deuxième partie

Applications

Définition: Une application f est la donnée de

- un ensemble E appelé ensemble de départ
- un ensemble F appelé ensemble d'arrivée
- une fonction qui associe à tout élément x de E un unique élément de F noté $f(x)$

L'application est notée

$$\begin{aligned} f : E &\longrightarrow F \\ x &\longmapsto f(x) \end{aligned}$$

EXEMPLE: 1. Soit \mathcal{P} le plan (affine) et $A \in \mathcal{P}$. Soit \mathcal{D} l'ensemble des droites.

$$\begin{aligned} f : \mathcal{P} \setminus \{A\} &\longrightarrow \mathcal{D} \\ B &\longmapsto (AB) \end{aligned}$$

2. $E = \mathcal{C}^1([0, 1], \mathbb{R})$ l'ensemble des fonctions à valeurs réelles de classe \mathcal{C}^1 sur $[0, 1]$
 $F = \mathcal{C}^0([0, 1], \mathbb{R})$

$$\begin{aligned} \varphi : E &\longrightarrow F \\ f &\longmapsto f' \end{aligned}$$

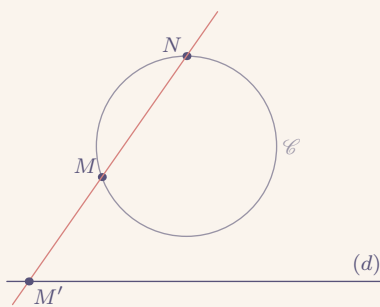
3. $E = \mathcal{C}^1([0, 1], \mathbb{R})$ et $F = \mathbb{R}$

$$\begin{aligned} \varphi : E &\longrightarrow F \\ f &\longmapsto f' \left(\frac{1}{2} \right) \end{aligned}$$

4. $E = [0, 1]$ et $F = \mathcal{C}^0([0, 1], \mathbb{R})$

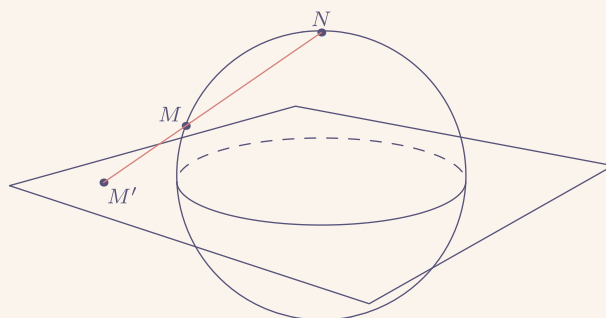
$$\begin{aligned} \varphi : E &\longrightarrow F \\ x &\longmapsto \int_a^x t^2 \ln(t) dt \end{aligned}$$

- 5.



$$\begin{aligned} \varphi : \mathcal{C} \setminus \{N\} &\longrightarrow (d) \\ M &\longmapsto M' \end{aligned}$$

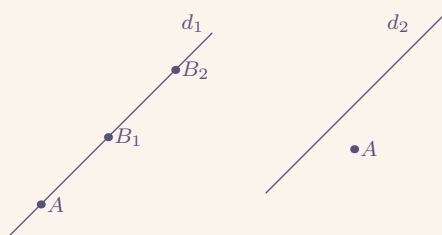
- 6.



Définition: Soit $f : E \rightarrow F$ une application. On dit que f est

- injective si tout élément de F a au plus un antécédent par f
- bijective si tout élément de F a un unique antécédent par f
- surjective si tout élément de F a au moins un antécédent par f

EXEMPLE (suite des exemples précédents): 1. L'application n'est ni injective ni surjective



B_1 et B_2 sont deux antécédants de d_1
 d_2 n'a pas d'antécédant par f

2. L'application n'est pas injective :

- $f : x \mapsto x$ est continue
- $x \mapsto \frac{x^2}{2}$ et $x \mapsto \frac{x^2}{2} + 42$ sont deux antécédants de f .

Mais, l'application est surjective d'après le théorème fondamental de l'analyse

3. L'application n'est pas injective ($x \mapsto 0$ et $x \mapsto 42$ sont deux antécédants de 0) mais elle est surjective ($\forall x \in \mathbb{R}, x \mapsto ax$ est un antécédant de a).
4. L'application est injective mais pas surjective (les images sont des primitives de $x \mapsto x^2 \ln(x)$)
5. et 6. sont bijectives

Définition: Soit $f : E \rightarrow F$ et $g : F \rightarrow G$. L'application notée $g \circ f$ est définie par

$$g \circ f : E \longrightarrow G$$

$$x \longmapsto g(f(x))$$

On dit que c'est la composée de f et g .

Proposition: Soient $f : E \rightarrow F, g : F \rightarrow G, h : G \rightarrow G$. Alors, $h \circ (g \circ f) = (h \circ g) \circ f$

Preuve:

Par définition, $g \circ f : E \rightarrow F$ donc $h \circ (g \circ f) : E \rightarrow H$

et $h \circ g : F \rightarrow H$ donc $(h \circ g) \circ f : E \rightarrow H$ Soit $x \in E$.

$$\begin{aligned} h \circ (g \circ f)(x) &= h(g \circ f(x)) \\ &= h(g(f(x))) \end{aligned}$$

$$\begin{aligned} (h \circ g) \circ f(x) &= h \circ g(f(x)) \\ &= h(g(f(x))) \end{aligned}$$

Donc, $h \circ (g \circ f)(x) = (h \circ g) \circ f(x)$

□

REMARQUE (A Attention):

En général, $g \circ f \neq f \circ g$

Par exemple, $f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & x^2 \end{array}$ et $g : \begin{array}{ccc} \mathbb{R}^+ & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \sqrt{x} \end{array}$

Alors, $f \circ g : \begin{array}{ccc} \mathbb{R}^+ & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & x \end{array}$ et $g \circ f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & |x| \end{array}$

donc $f \circ g \neq g \circ f$

Proposition: Soient $f : E \rightarrow F$ et $g : F \rightarrow G$

1. Si $g \circ f$ est injective, alors f est injective
2. Si $g \circ f$ est surjective, alors g est surjective
3. Si f et g sont surjectives, alors $g \circ f$ est surjective
4. Si f et g sont injectives, alors $g \circ f$ est injective

Preuve:

1. On suppose $g \circ f$ injective. On veut montrer que f est injective. Soient $(x, y) \in E^2$. On suppose $f(x) = f(y)$. Montrons que $x = y$.
Comme $f(x) = f(y)$, $g(f(x)) = g(f(y))$ i.e. $g \circ f(x) = g \circ f(y)$
Or, $g \circ f$ injective donc $x = y$
2. On suppose $g \circ f$ surjective. On veut montrer que g est surjective. Soit $y \in G$.
On cherche $x \in F$ tel que $g(x) = y$.
Comme $g \circ f : E \rightarrow G$ surjective, y a un antécédant $z \in E$ par $g \circ f$.
On pose $x = f(z) \in F$ et on a bien $g(x) = y$
3. On suppose f et g injectives. Montrons que $g \circ f$ injective. Soient $x, y \in E$. On suppose $g \circ f(x) = g \circ f(y)$. Montrons $x = y$
On sait que $g(f(x)) = g(f(y))$. Comme g est injective, $f(x) = f(y)$ et comme f est injective, $x = y$
4. On suppose f et g surjectives. Soit $y \in G$. On cherche $x \in E$ tel que $g \circ f(x) = y$
Comme g est surjective, y a un antécédant $z \in F$ par g
Comme f est surjectives, z a un antécédant $x \in E$ par f
On en déduit $g \circ f(x) = g(f(x)) = g(z) = y$

□

REMARQUE:

$f : E \longrightarrow F$

$$f \text{ injective} \iff \left(\forall (x, y) \in E^2, f(x) = f(y) \implies x = y \right)$$

Définition: Soit $f : E \rightarrow F$ une bijection. L'application $\begin{cases} F & \longrightarrow & E \\ y & \longmapsto & \text{l'unique antécédent de } y \text{ par } f \end{cases}$ est la réci-proque de f notée f^{-1}

Définition: L'identité de E est $\text{id}_E : \begin{cases} E & \longrightarrow & E \\ x & \longmapsto & x \end{cases}$

Proposition: Soient $f : E \rightarrow F$ et $g : F \rightarrow E$

$$\left. \begin{array}{l} f \circ g = \text{id}_F \\ g \circ f = \text{id}_E \end{array} \right\} \iff \begin{cases} f \text{ bijective} \\ f^{-1} = g \end{cases}$$

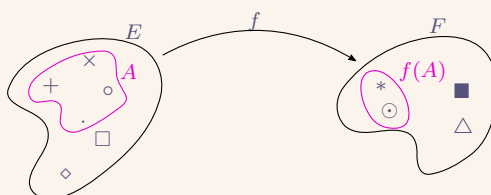
Preuve (déjà faite):

□

Définition: Soit $f : E \rightarrow F$

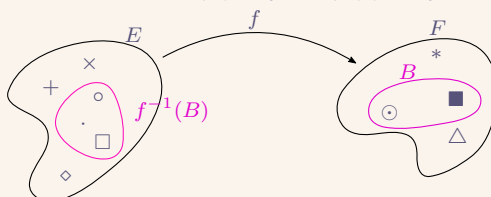
1. Soit $A \in \mathcal{P}(E)$. L'image directe de A par f est

$$f(A) = \{f(x) \mid x \in A\}$$



2. Soit $B \in \mathcal{P}(F)$. L'image réciproque de B par f est

$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}$$



REMARQUE:

- $y \in f(A) \iff \exists x \in A, y = f(x),$
- $x \in f^{-1}(B) \iff f(x) \in B.$

Proposition: Soient $f : E \rightarrow F$, $A \in \mathcal{P}(E)$ et $F \in \mathcal{P}(F)$.

1. $f^{-1}(f(A)) \supset A$,
2. Si f est injective alors $f^{-1}(f(A)) = A$,
3. $f(f^{-1}(B)) \subset B$,
4. Si f est surjective, alors $f(f^{-1}(B)) = B$.

Preuve: 1. Soit $x \in A$. Montrons que $x \in f^{-1}(f(A))$ i.e. montrons que $f(x) \in f(A)$.
Comme $x \in A$, $f(x) \in f(A)$.

2. On suppose f injective. Montrons que $f^{-1}(f(A)) = A$. Soit $x \in f^{-1}(f(A))$, montrons que $x \in A$. On sait que $f(x) \in f(A)$. Donc, il existe $a \in A$ tel que $f(x) = f(a)$. Or, f est injective et donc $x = a$. On en déduit que $x \in A$.
D'après 1., on sait que $f^{-1}(f(A)) \supset A$. On a montré $f^{-1}(f(A)) \subset A$. Donc

$$f^{-1}(f(A)) = A.$$

3. Soit $y \in f(f^{-1}(B))$. Montrons $y \in B$. On sait qu'il existe $x \in f^{-1}(B)$ tel que $y = f(x)$. On a donc $f(x) \in B$ et donc $y \in B$.
4. On suppose f surjective, montrons $B \subset f(f^{-1}(B))$. Soit $y \in B$, montrons $y \in f(f^{-1}(B))$. On cherche $x \in f^{-1}(B)$ tel que $y = f(x)$. C'est à dire, on cherche $x \in E$ tel que $f(x) \in B$ et $y = f(x)$. On sait que f est surjective donc y a un antécédant $x \in E$ tel que $B \ni y = f(x)$.
On vient de montrer $B \subset f(f^{-1}(B))$ et on a montré dans 3. que $B \supset f(f^{-1}(B))$.
On en déduit que

$$f(f^{-1}(B)) = B.$$

□

Proposition: Soit $f : E \rightarrow F$ et $(A, B) \in \mathcal{P}(F)^2$. Alors

$$\begin{cases} f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B), & (1) \\ f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B). & (2) \end{cases}$$

Preuve:
Soit $x \in E$.

$$\begin{aligned} x \in f^{-1}(A \cup B) &\iff f(x) \in A \cup B \\ &\iff f(x) \in A \text{ ou } f(x) \in B \\ &\iff x \in f^{-1}(A) \text{ ou } x \in f^{-1}(B) \\ &\iff x \in f^{-1}(A) \cup f^{-1}(B). \end{aligned}$$

$$\begin{aligned} x \in f^{-1}(A \cap B) &\iff f(x) \in A \cap B \\ &\iff f(x) \in A \text{ et } f(x) \in B \\ &\iff x \in f^{-1}(A) \text{ et } x \in f^{-1}(B) \\ &\iff x \in f^{-1}(A) \cap f^{-1}(B). \end{aligned}$$

□

Proposition: Soient $f : E \rightarrow F$ et $(A, B) \in \mathcal{P}(E)^2$.

1. $f(A \cap B) \subset f(A) \cap f(B)$
2. Si f est injective, $f(A \cap B) = f(A) \cap f(B)$
3. $f(A \cup B) = f(A) \cup f(B)$.

Preuve: 1. Soit $y \in f(A \cap B)$. Soit $x \in A \cap B$ tel que $y = f(x)$. Comme $x \in A$, $f(x) \in f(A)$ et comme $x \in B$, $f(x) \in f(B)$ et donc $y \in f(A) \cap f(B)$

2. On suppose f injective. Soit $y \in f(A) \cap f(B)$.
 Comme $y \in f(A)$, il existe $a \in A$ tel que $y = f(a)$.
 Comme $y \in f(B)$, il existe $b \in B$ tel que $y = f(b)$.
 Comme f est injective, $a = b$ et donc $a \in A \cap B$. On en déduit que

$$y = f(a) \in f(A \cap B).$$

3. Soit $y \in F$. Alors

$$\begin{aligned} y \in f(A \cup B) &\iff \exists x \in A \cup B; y = f(x) \\ &\iff (\exists x \in A \text{ ou } \exists x \in B), y = f(x) \\ &\iff y \in f(A) \text{ ou } y \in f(B) \\ &\iff y \in f(A) \cup f(B). \end{aligned}$$

□

REMARQUE (Contre-exemple pour 2.):

Cas d'une application qui n'est pas injective

On pose $A = \mathbb{R}_*^+$, $B = \mathbb{R}_*^-$ et

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R}^+ \\ x &\longmapsto x^2 \end{aligned}$$

On a $A \cap B = \emptyset$ donc $f(A \cap B) = \emptyset$.

Or, $\left. \begin{array}{l} f(A) = \mathbb{R}_*^+ \\ f(B) = \mathbb{R}_*^+ \end{array} \right\}$ donc $f(A) \cap f(B) = \mathbb{R}_*^+$.

On a

$$f(A \cap B) \neq f(A) \cap f(B).$$

Définition: Soit $f : E \rightarrow F$ et $A \in \mathcal{P}(E)$.

La restriction de f à A est

$$\begin{aligned} f|_A : A &\longrightarrow F \\ x &\longmapsto f(x) \end{aligned}$$

On dit aussi que f est un prolongement de $f|_A$.

REMARQUE (Notation):

L'ensemble des applications de E dans F est noté F^E .

EXEMPLE:

On pose $f : \mathbb{R}^* \longrightarrow \mathbb{R}$
 $x \longmapsto \frac{1}{x}$ et $g : \mathbb{R} \longrightarrow \mathbb{R}$
 $x \longmapsto \begin{cases} \frac{1}{x} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$ un prolongement de f car
 $g|_{\mathbb{R}^*} = f$.

L'application $h : \mathbb{R} \longrightarrow \mathbb{R}$
 $x \longmapsto \begin{cases} \frac{1}{x} & \text{si } x \neq 0 \\ 1 & \text{si } x = 0 \end{cases}$ est un autre prolongement de f .

Troisième partie

Relations binaires

Définition: Soit E un ensemble. Un relation (binaire) sur E est un prédicat défini sur E^2 .

EXEMPLE: 1. Avec $E = \mathbb{C}$, $=$ est une relation binaire,
 2. Avec $E = \mathbb{R}$, \leq est une relation binaire,
 3. Avec E l'humanité et la relation binaire \wedge :

$$x \wedge y \iff x \text{ et } y \text{ ont la même mère.}$$

Définition: Soit E un ensemble, \diamond une relation sur E . On dit que \diamond est un relation d'équivalence si

- | | |
|---|----------------|
| 1. $\forall x \in E, x \diamond x,$ | (réflexivité) |
| 2. $\forall x, y \in E, x \diamond y \implies y \diamond x,$ | (symétrie) |
| 3. $\forall x, y, z \in E, \left. \begin{array}{l} x \diamond y \\ y \diamond z \end{array} \right\} \implies x \diamond z$ | (transitivité) |

EXEMPLE:

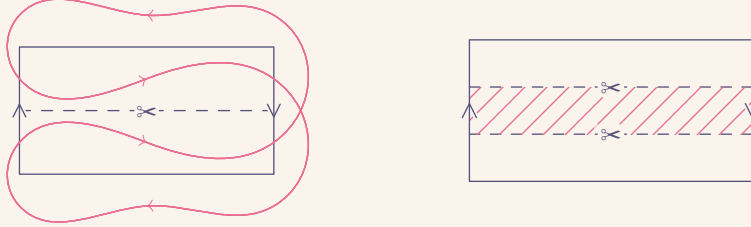
Avec $E = \mathbb{Z}$ et

$$x \diamond y \iff x \equiv y \text{ [3]}$$

“ \diamond ” est une relation d'équivalence.

REMARQUE:

Le but d'une relation d'équivalence est d'identifier des objets différents.



Définition: Soit E un ensemble et \diamond une relation d'équivalence sur E . Soit $x \in E$. La classe de x (modulo \diamond) est

$$\mathcal{C}_\diamond(x) = \mathcal{C}(x) = \bar{x} = \{y \in E \mid y \diamond x\}.$$

EXEMPLE: 1. Avec $E = \mathbb{C}$ et $\diamond = “=”$,

$$\forall z \in \mathbb{C}, \bar{z} = \mathcal{C}(z) = \{z\}.$$

2. Avec $E = \mathbb{Z}$ et $\diamond =$ congruence modulo 5, on a

$$\begin{array}{ll} \bar{0} = \{5k \mid k \in \mathbb{Z}\} & \bar{1} = \{5k + 1 \mid k \in \mathbb{Z}\} \\ \bar{2} = \{5k + 2 \mid k \in \mathbb{Z}\} & \bar{3} = \{5k + 3 \mid k \in \mathbb{Z}\} \\ \bar{4} = \{5k + 4 \mid k \in \mathbb{Z}\} & \bar{5} = \bar{0} \end{array}$$

On constate que

$$x \equiv y \text{ [5]} \iff \bar{x} = \bar{y}.$$

Proposition: Soit E un ensemble muni d'une relation d'équivalence \diamond . Alors

$$\forall x, y \in E, x \diamond y \iff \bar{x} = \bar{y}.$$

Preuve:

Soient $x, y \in E$.

- On suppose $x \diamond y$. Soit $z \in \bar{x}$. On sait que $z \diamond x$ et $y \diamond x$. Par transitivité, on en déduit que $z \diamond y$ et donc $z \in \bar{y}$.
- Soit $z \in \bar{y}$, donc $y \diamond z$. Or $x \diamond y$. Comme \diamond est symétrique, on a $y \diamond x$ et par transitivité, on a donc $z \diamond x$. Donc $z \in \bar{x}$.
- On suppose $\bar{x} = \bar{y}$. \diamond réflexive donc $x \diamond x$ et donc $x \in \bar{x} = \bar{y}$ donc $x \in \bar{y}$ et donc $x \diamond y$.

□

HORS-PROGRAMME

Définition: Soit E un ensemble et \diamond une relation d'équivalence.

L'ensemble

$$\{\bar{x} \mid x \in E\} = E/\diamond$$

est appelé quotient de E modulo \diamond .

EXEMPLE: 1. $E = \mathbb{Z}$ et $\diamond =$ congruence modulo 5 :

$$E/\diamond = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \mathbb{Z}/5\mathbb{Z}$$

2. *Construction de \mathbb{Q}*

On suppose avoir déjà construit \mathbb{Z} mais pas \mathbb{Q} : on veut donc donner une définition de p/q sans parler de division.

On pose

$$E = \mathbb{Z} \times \mathbb{N}^* = \{(p, q) \mid p \in \mathbb{Z}, q \in \mathbb{N}^*\}.$$

Soit \sim la relation définie par

$$(p, q) \sim (p', q') \iff pq' = p'q$$

Montrons que \sim est une relation d'équivalence.

- Soient $(p, q) \in E$. \sim est réflexive car $(p, q) \sim (p, q) \iff pq = pq$.
- Soient $(p, q), (p', q') \in E$. On suppose $(p, q) \sim (p', q')$.

$$\begin{aligned} (p, q) \sim (p', q') &\iff pq' = p'q \\ &\iff p'q = pq' \\ &\iff (p', q') \sim (p, q) \end{aligned}$$

Donc \sim est symétrique.

- Soient $(p, q), (p', q'), (p'', q'') \in E$. On suppose

$$\begin{cases} (p, q) \sim (p', q') \\ (p', q') \sim (p'', q'') \end{cases}$$

On sait que

$$(p, q) \sim (p'', q'') \iff pq'' = p''q$$

Or,

$$\begin{cases} pq' = qp' \\ p'q'' = p''q' \end{cases} \quad \text{donc } pq'p'q'' = p'q'p''q'$$

Donc

$$p'q'(pq'' - p''q) = 0$$

et donc

$$p' = 0 \quad \text{ou} \quad pq'' - p''q = 0$$

Si $p' = 0$, alors $\begin{cases} pq' = 0 \\ p''q' = 0 \end{cases}$ et donc $\begin{cases} p = 0 \\ p'' = 0 \end{cases}$. On a donc

$$pq'' = 0 = p''q$$

Si $p' \neq 0$, on a $pq'' - p''q = 0$ et donc

$$pq'' = p''q$$

On a donc $(p, q) \sim (p'', q'')$.

On pose $\mathbb{Q} = E/\sim$ et

$$\forall (p, q) \in E, \quad \frac{p}{q} = \mathcal{C}\ell((p, q)).$$

Ainsi,

$$\begin{aligned} \frac{p}{q} = \frac{p'}{q'} &\iff \mathcal{C}\ell((p, q)) = \mathcal{C}\ell((p', q')) \\ &\iff (p, q) \sim (p', q') \\ &\iff pq' = p'q \end{aligned}$$

3. *Construction de \mathbb{Z} à partir de \mathbb{N}*

On pose $E = \mathbb{N} \times \mathbb{N}^*$ et \sim la relation $(p, q) \sim (p', q') \iff p + q' = p' + q$.

\sim est une relation d'équivalence. On pose donc $\mathbb{Z} = \mathbb{N}/\sim$ et pour $n \in \mathbb{N}$, on définit n par $\mathcal{C}\ell((n, 0))$ et $-n$ par $\mathcal{C}\ell((0, n))$.

4. *Construction de \mathbb{C} à partir de \mathbb{R}*

On pose E l'ensemble des polynômes à coefficients réels ($E = \mathbb{R}[X]$) et \diamond la relation d'équivalence

$$P \diamond Q \iff P \equiv Q \pmod{x^2 + 1}$$

On pose $\mathbb{C} = E/\diamond$.

Il manque une partie du cours ici

Définition: Soit E un ensemble et $(A_i)_{i \in I}$ une famille de parties de E .

On dit que $(A_i)_{i \in I}$ est une partition de E si

$$\begin{cases} E = \bigcup_{i \in I} A_i \\ \forall i \neq j, A_i \cap A_j = \emptyset \end{cases}$$

On a donc

$$\forall x \in E, \exists ! i \in I, x \in A_i.$$

Proposition: Soit E un ensemble muni d'une relation d'équivalence \diamond . Les classes

d'équivalences de E modulo \diamond forment une partition de E .

Preuve: — Soit $x \in E$. On sait que $x \diamond x$ donc $\bar{x} \ni x$. On a montré $E \subset \bigcup_{y \in E} \bar{y}$.

— $\forall y \in E, \bar{y} \subset E$ donc $E \supset \left(\bigcup_{y \in E} \bar{y} \right)$.

— Soit $x, y \in E$ tel que $\bar{x} \neq \bar{y}$. Montrons que $\bar{x} \cap \bar{y} = \emptyset$. Soit $z \in \bar{x} \cap \bar{y}$. $z \in \bar{x}$ donc $z \diamond x$. De même, $z \in \bar{y}$ donc $z \diamond y$. Par transitivité, $x \diamond y$ et donc $\bar{x} = \bar{y}$: une contradiction.

□

Proposition: Soit E un ensemble et $(A_i)_{i \in I}$ une partition de E telle que

$$\forall i \in I, A_i \neq \emptyset.$$

Alors il existe une relation d'équivalence \diamond telle que pour tout $i \in I$, A_i est une classe d'équivalence modulo \diamond .

Preuve:

Soit \diamond la relation définie par

$$x \diamond y \iff \exists i \in I, \begin{cases} x \in A_i \\ y \in A_i \end{cases}$$

— Soit $x \in E$. Comme $E = \bigcup_{i \in I} A_i$, il existe $i \in I$ tel que $x \in A_i$ donc $x \diamond x$.

— Soient $x, y \in E$. On suppose $x \diamond y$. Soit $i \in I$ tel que $\begin{cases} x \in A_i \\ y \in A_i \end{cases}$ donc $\begin{cases} y \in A_i \\ x \in A_i \end{cases}$ et donc $y \diamond x$.

— Soit $x, y, z \in E$. On suppose $x \diamond y$ et $y \diamond z$.

Soit $i \in I$ tel que $\begin{cases} x \in A_i \\ y \in A_i \end{cases}$.

Soit $j \in I$ tel que $\begin{cases} y \in A_j \\ z \in A_j \end{cases}$.

On a donc $y \in A_i \cap A_j$. Si $i \neq j$, alors $y \in \emptyset$: une contradiction. Donc $i = j$ et

donc $\begin{cases} x \in A_i \\ z \in A_i \end{cases}$. On en déduit que $x \diamond z$.

Ainsi \diamond est une relation d'équivalence.

— Soit $i \in I$ et soit $x \in A_i \neq \emptyset$.

$$\bar{x} = \{y \in E \mid y \diamond x\} = \{y \in E \mid y \in A_i\} = A_i.$$

□

Définition: Soit E un ensemble et \diamond . On dit que \diamond est une relation d'ordre sur E si

1. \diamond est réflexive ($\forall x \in E, x \diamond x$),

2. \diamond est anti-symétrique :

$$\forall x, y \in E, \left. \begin{array}{l} x \diamond y \\ y \diamond x \end{array} \right\} \implies x = y,$$

3. \diamond est transitive $(\forall x, y, z \in E, (x \diamond y \text{ et } y \diamond z) \implies x \diamond z)$.

En général, la relation \diamond est notée \leq ou \preceq . On dit aussi que (E, \diamond) est un ensemble ordonné.

EXEMPLE: 1. (\mathbb{R}, \leq) est un ensemble ordonné.

2. $(\mathcal{P}(E), \subset)$ est un ensemble ordonné.

3. $(\mathbb{N}, |)$ est un ensemble ordonné.

4. $(MP2I, \preceq)$ avec

$$x \preceq y \iff \text{note de } x \leq \text{note de } y$$

n'est un ensemble ordonné car \preceq n'est pas anti symétrique.

5. $E = \mathbb{N}^2$ et \preceq définie par

$$(x, y) \preceq (x', y') \iff x < x' \text{ ou } \begin{cases} x = x' \\ y \leq y' \end{cases}$$

(E, \preceq) est un ensemble ordonné.

Définition: Soit (E, \leq) un ensemble ordonné. Soient $x, y \in E$. On dit que x et y sont comparables si

$$x \leq y \text{ ou } y \leq x.$$

On dit que \leq est un ordre total si tous les éléments de E sont comparables 2 à 2.

EXEMPLE: — (\mathbb{R}, \leq) est totalement ordonné

— $(\mathcal{P}(E), \subset)$ n'est pas totalement ordonné en général :

Soient $a, b \in E$ avec $a \neq b$. $\{a\}$ et $\{b\}$ ne sont pas comparables.

— $(\mathbb{N}, |)$ n'est pas totalement ordonné :

$2 \nmid 5$ et $5 \nmid 2$ donc 2 et 5 ne sont pas comparables.

Définition: Soit (E, \leq) un ensemble ordonné, $A \in \mathcal{P}(E)$ et $M \in E$. On dit que A est majorée par M , que M majore A ou que M est un majorant de A si

$$\forall a \in A, a \leq M.$$

Soit $m \in E$. On dit que A est minorée par m , que m minore A ou que m est un minorant de A si

$$\forall a \in A, m \leq a.$$

Il manque une partie du cours ici

EXEMPLE: 1. $E = \mathbb{R}$ muni de \leq et $A = [2, 5]$.

On sait que $\sup A = 5$ car

$$\forall x \in A, x \leq 5$$

et

$$\forall y \leq 5, \quad 5 > \frac{y+5}{2} > y$$

donc y ne majore pas A .

2. $E = \mathbb{R}$ avec \leq et $A =]2, 5[$. $A \not\exists \sup A = 5$ par le même raisonnement.

3. $E = \mathbb{N}^*$ avec $|$ et $A = \{p, q\}$ avec $p \neq q \in E$. $\sup A = \text{PPCM}(p, q) = p \vee q$ (c.f. chapitre 10 arithmétique)
4. $\mathcal{P}(E)$ avec \subset et $A = \{P, Q\}$ avec $P, Q \in \mathcal{P}(E)$ et $P \neq Q$. $\sup A = P \cup Q$.
5. $E = \{0, 1\} \times \mathbb{Z}$ muni de \leq défini par

$$(x_1, y_1) \leq (x_2, y_2) \iff x_1 < x_2 \text{ ou } \begin{cases} x_1 = x_2 \\ y_1 \leq y_2 \end{cases}$$

et $A = \{0\} \times \mathbb{Z}$. (x, y) majore $A \iff x = 1$ donc A est majorée mais n'a pas de borne supérieure.

Proposition: Soit (E, \leq) un ensemble ordonné et $A \in \mathcal{P}(E)$. Si A a une borne supérieure, alors celle-ci est unique. On la note $\sup A$.

Preuve:

Soit M_1 et M_2 deux bornes supérieures de A .

Donc M_2 majore A . Comme M_1 est une borne supérieure de A , on a $M_1 \leq M_2$.

De même, on en déduit que $M_2 \leq M_1$.

Comme \leq est antisymétrique, $M_1 = M_2$. □

Proposition – Définition: Soit (E, \leq) un ensemble ordonné et $A \in \mathcal{P}(E)$ minorée par $m \in E$. On dit que m est une borne inférieure de A si

$$\begin{cases} \forall a \in A, m \leq a, \\ \forall x \in E, (\forall a \in A, x \leq a) \implies x \leq m. \end{cases}$$

Dans ce cas, m est unique et on la note $\inf(A)$. □

Définition: Soit (E, \leq) un ensemble ordonné et $A \in \mathcal{P}(E)$.

1. Soit $M \in E$. On dit que M est le plus grand élément de A ou que M est le maximum de A si

$$\begin{cases} \forall a \in A, a \leq M, \\ M \in A. \end{cases}$$

Dans ce cas, on le note $M = \max(A)$.

2. Soit $m \in E$. On dit que m est le plus petit élément de A ou que m est le minimum de A si

$$\forall a \in A, a \geq m \text{ et } m \in A$$

Dans ce cas, on le note $m = \min(A)$.

Proposition: En cas d'existence, il y a unicité du minimum et du maximum.

Preuve:

Soient M_1 et M_2 deux maxima. On a $M_1 \in A$ donc $M_1 \leq M_2$. Or, $M_2 \in A$ donc $M_2 \leq M_1$. On en déduit que $M_1 = M_2$. □

Proposition: Soit (E, \leq) un ensemble ordonné, $A \in \mathcal{P}(E)$ et $M \in E$.

$$M = \max(A) \iff \begin{cases} M = \sup(A), \\ M \in A; \end{cases}$$

$$M = \min(A) \iff \begin{cases} M = \inf(A), \\ M \in A. \end{cases}$$

Preuve: “ \implies ” On suppose $M = \max(A)$. On sait déjà que $M \in A$ et que M est un majorant de A .
 Soit M' un majorant de A . $M \in A$ donc $M' \geq M$. On en déduit que $M = \sup(A)$.
 “ \impliedby ” On suppose $M = \sup(A) \in A$. Alors M majore A et $M \in A$ donc $M = \max(A)$. □

EXEMPLE:

$E = \mathbb{N}^*$ muni de $|$ et $A = \{3, 5\}$. $\sup(A) = 3 \vee 5 = 15 \notin A$ donc A n'a pas de maximum.

Définition: Soit (E, \leq) un ensemble ordonné, $A \in \mathcal{P}(E)$ et $M \in A$.

On dit que M est un élément maximal de A si aucun élément de A n'est strictement supérieur à M :

$$\nexists a \in A, \begin{cases} M \leq a, \\ M \neq a. \end{cases}$$

On dit que M est un élément minimal de A si aucun élément de A n'est strictement inférieur à M :

$$\nexists a \in A, \begin{cases} M \geq a, \\ M \neq a. \end{cases}$$

EXEMPLE:

$E = \{n \in \mathbb{N} \mid n \geq 2\} = \mathbb{N} \setminus \{0, 1\}$ muni de $|$ et $A = E$. Les éléments minimaux de E sont les nombres premiers, il y en a une infinité. Il n'y a donc pas d'élément maximal.

Proposition: Avec les notations précédentes, si A a un maximum M alors M est le seul élément maximal de A .

Preuve:

Soit $M = \max(A)$. Soit $a \in A$ tel que $M \leq a$ et $M \neq a$. Comme $a \in A$ et $M = \max(A)$, on sait que $a \leq M$. Par antisymétrie, on en déduit que $a = M$: une contradiction.

Donc M est un élément maximal de A .

Soit M' un élément maximal de A . $M' \in A$ donc $M' \leq M$ et donc $M = M'$. □

Définition: Soient (E, \leq) et (F, \preccurlyeq) deux ensembles ordonnés et $f : E \rightarrow F$. On dit que

1. f est croissante si

$$\forall (x, y) \in E^2, x \leq y \implies f(x) \preccurlyeq f(y);$$

2. f est décroissante si

$$\forall (x, y) \in E^2, x \leq y \implies f(x) \geq f(y).$$

EXEMPLE:

$E = \mathbb{N}^*$ muni de $|$, $F = \mathbb{N}^*$ muni de \leq et $f : \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & x. \end{array}$

Soit $(x, y) \in E^2$ tels que $x | y$. Alors $x \leq y$ donc f est croissante.

On pose

$$\begin{array}{ccc} g : F & \longrightarrow & E \\ n & \longmapsto & n. \end{array}$$

$2 \leq 3$ mais $2 \nmid 3$ donc g n'est pas croissante et $2 \leq 5$ mais $5 \nmid 2$ donc g n'est pas décroissante.

Définition: Soit (E, \leq) un ensemble ordonné et $A \in \mathcal{P}(E)$. On dit que A est bornée si A est à la fois majorée et minorée.

Définition: Avec les notations précédentes, un extremum de A (sous réserve d'existence) est un maximum ou un minimum de A .

Quatrième partie

Lois de composition

Définition: Une loi de composition interne est une application f de $E \times E$ dans E .
On la note $x * y$ au lieu de $f(x, y)$ (on est libre de choisir le symbole).

Définition: Soit E un ensemble muni d'une loi de composition interne \boxtimes .
On dit que \boxtimes est associative si

$$\forall (x, y, z) \in E^3, (x \boxtimes y) \boxtimes z = x \boxtimes (y \boxtimes z).$$

Dans ce cas, on écrit plutôt $x \boxtimes y \boxtimes z$.

EXEMPLE: — $+$ et \times dans \mathbb{C} sont associatives;
— \circ est associative;
— la multiplication matricielle est aussi associative.

Définition: On dit que \boxtimes est commutative si

$$\forall (x, y) \in E^2, x \boxtimes y = y \boxtimes x.$$

EXEMPLE: — $+$ et \times dans \mathbb{C} sont commutatives;
— \circ n'est pas commutative;
— la multiplication matricielle n'est pas commutative.

Définition: Soit $e \in E$. On dit que e est un
— élément neutre à gauche si

$$\forall x \in E, e \boxtimes x = x;$$

— élément neutre à droite si

$$\forall x \in E, x \boxtimes e = x;$$

— élément neutre si

$$\forall x \in E, e \boxtimes x = x \boxtimes e = x.$$

Proposition: Sous réserve d'existence, il y a unicité de l'élément neutre.

Preuve:

Soient e et e' deux éléments neutres.

— $e \boxtimes e' = e'$ car e est neutre,

— $e \boxtimes e' = e$ car e' est neutre.

On a donc $e = e'$. □

Axiome (axiome du choix): Soit E un ensemble non vide. Il existe $f : \mathcal{P}(E) \setminus \{\emptyset\} \rightarrow E$ telle que

$$\forall A \in \mathcal{P}(E) \setminus \{\emptyset\}, f(A) \in A.$$

Définition: Soit $f : E \rightarrow F$. Le graphe de f est

$$\{(x, f(x)) \mid x \in E\} \subset E \times F.$$

Proposition: Soit $G \subset E \times F$. G est le graphe d'une application si et seulement si

$$\forall x \in E, \exists! y \in F, (x, y) \in G.$$

Preuve: “ \implies ” par définition d'une application

“ \impliedby ” On pose $f(x)$ le seul élément y de F qui vérifie $(x, y) \in G$. Alors $f \in F^E$ et son graphe vaut G .

□

Définition: Soit $A \in \mathcal{P}(E)$. L'indicatrice de A est

$$\begin{aligned} 1_A : E &\longrightarrow \{0, 1\} \\ x &\longmapsto \begin{cases} 1 & \text{si } x \in A, \\ 0 & \text{si } x \notin A. \end{cases} \end{aligned}$$

EXEMPLE: 1. Dans \mathbb{C} , le neutre de $+$ est 0 et le neutre de \times est 1.

2. Dans E^E , le neutre de \circ est id_E .

3. Dans $\mathcal{M}_n(\mathbb{C})$ (l'ensemble des matrices carrées $n \times n$ à valeurs dans \mathbb{C}), le neutre de \times est I_n :

$$I_n = \begin{pmatrix} 1 & & (0) \\ & \ddots & \\ & & \ddots & \\ (0) & & & 1 \end{pmatrix}$$

Définition: Soit E un ensemble muni d'une loi de composition interne \boxtimes et $x \in E$.

1. On dit que x est simplifiable à gauche si

$$\forall (y, z) \in E^2, (x \boxtimes y = x \boxtimes z) \implies x = z.$$

et que x est simplifiable à droite si

$$\forall (y, z) \in E^2, (y \boxtimes x = z \boxtimes x) \implies y = z.$$

2. On dit que x est symétrisable à gauche s'il existe $y \in E$ tel que $y \boxtimes x = e$ où e est l'élément neutre de \boxtimes .

De même, on dit que x est symétrisable à droite s'il existe $y \in E$ tel que $x \boxtimes y = e$.

On dit que x est symétrisable s'il est symétrisable à gauche et à droite, donc s'il existe $y \in E$ tel que $x \boxtimes y = y \boxtimes x = e$.

EXEMPLE:

$E = \mathbb{N}$ muni de la loi $+$, tous les éléments de E sont simplifiables. 0 est le seule élément de E symétrisable.

Proposition: Avec les notations précédentes, si \boxtimes est associative, et x est symétrisable, alors x est simplifiable.

Preuve:

Soient $y, z \in E$.

— On suppose $x \boxtimes y = x \boxtimes z$. Soit $a \in E$ tel que $a \boxtimes x = e$. Alors

$$a \boxtimes (x \boxtimes y) = a \boxtimes (x \boxtimes z).$$

Or,

$$\begin{aligned} a \boxtimes (x \boxtimes y) &= (a \boxtimes x) \boxtimes y \\ &= e \boxtimes y \\ &= y. \end{aligned}$$

De même, $a \boxtimes (x \boxtimes z) = z$.

Donc $y = z$.

— De même, si $y \boxtimes x = z \boxtimes x$, on “multiplie” x à droite par a et on obtient $y = z$. \square

Proposition – Définition: On suppose \boxtimes associative. Soit $x \in E$ symétrisable. Alors

$$\exists! y \in E, x \boxtimes y = y \boxtimes x = e.$$

On dit que y est le symétrique de x et on le note $y = x^*$.

Preuve:

Soient $x, y, z \in E$ tels que

$$\begin{cases} x \boxtimes y = y \boxtimes x = e \\ x \boxtimes z = z \boxtimes x = e \end{cases}$$

Alors, $x \boxtimes y = x \boxtimes z$ et, en simplifiant par x , on a $y = z$. \square

EXEMPLE:

Les fonctions symétrisables de (E^E, \circ) sont les bijections et le symétrique d’une bijection est sa réciproque.

REMARQUE: 1. Si la loi est notée $+$, on parle d’opposé plutôt que de symétrique et on le note $-x$ au lieu de x^* . L’élément neutre est noté 0_E .

2. Si la loi est notée \times , on parle d’élément inversible au lieu de symétrisable, d’inverse au lieu de symétrique et on note x^{-1} au lieu de x^* . On note le neutre 1_E .

EXERCICE:

Soient $x, y \in E = \mathbb{R}_*^+$. On définit la loi de composition interne \oplus :

$$x \oplus y = \frac{1}{\frac{1}{x} \oplus \frac{1}{y}}.$$

Cette loi peut-être utile en physique pour le calcul de résistances équivalentes en parallèles.

— ASSOCIATIVITÉ : soient $x, y, z \in E$.

D’une part, on a

$$x \oplus (y \oplus z) = \frac{1}{\frac{1}{x} + \frac{1}{\frac{1}{\frac{1}{y} + \frac{1}{z}}}} = \frac{1}{\frac{1}{x} + \frac{1}{y} + \frac{1}{z}}.$$

D'autre part, on a

$$(x \oplus y) \oplus z = \frac{1}{\frac{\frac{1}{x} + \frac{1}{y}}{\frac{1}{x} + \frac{1}{y}} + \frac{1}{z}} = \frac{1}{\frac{1}{x} + \frac{1}{y} + \frac{1}{z}}.$$

La loi \oplus est associative.

— COMMUTATIVITÉ : soient $x, y \in E$.

$$x \oplus y = \frac{1}{\frac{1}{x} + \frac{1}{y}} = \frac{1}{\frac{1}{y} + \frac{1}{x}} = y \oplus x.$$

Donc la loi \oplus est commutative.

— ÉLÉMENT NEUTRE : soit e l'élément neutre de \oplus .

$$\forall x \in E, x \oplus e = e \oplus x = x.$$

Comme la loi est commutative, seul l'égalité $x \oplus e = x$ est utile.

Soit $x \in E$. On a donc $\frac{1}{\frac{1}{x} + \frac{1}{e}} = x$ donc $\frac{ex}{e+x} = x$ donc $ex = x(e+x)$ et donc $\cancel{ex} = \cancel{ex} + x^2$. On en déduit que $x^2 = 0$, ce qui n'est pas possible car $x \in \mathbb{R}_*^+$. Donc, il n'y a pas d'élément neutre pour \oplus .

Cinquième partie

Divers

Définition: Soient E et F deux ensembles. Un couple (x, y) est la donnée d'un élément x de E et d'un élément y de F où

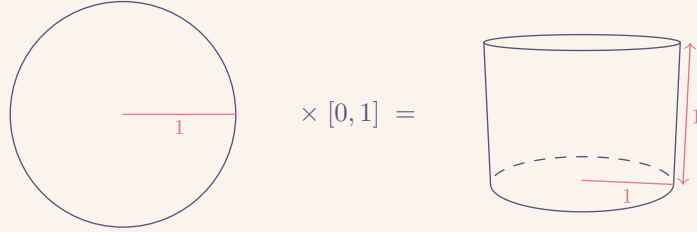
$$\forall x, x' \in E, \forall y, y' \in F, \quad (x, y) = (x', y') \iff \begin{cases} x = x', \\ y = y'. \end{cases}$$

On note $E \times F$ l'ensemble des couples ; c'est le produit cartésien de E et F .

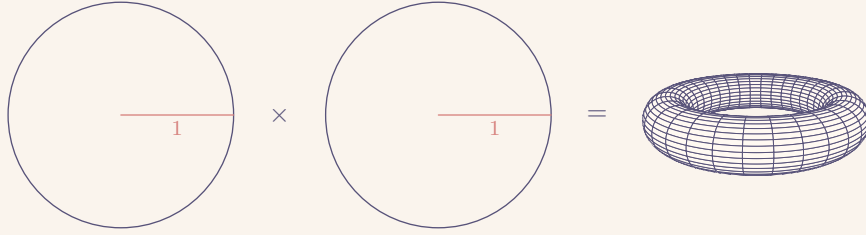
EXEMPLE:

$D \times [0, 1]$ est un cylindre plein où D est le disque unité fermé i.e.

$$D = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}.$$



$C \times C$ où $C = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ est un tore (creu).



Définition: Soient E et F deux ensembles. On dit que E et F sont équipotents s'il existe une bijection de E dans F .

EXEMPLE: 1. \mathbb{N} et \mathbb{N}^* sont équipotents car $f : \begin{matrix} \mathbb{N} & \longrightarrow & \mathbb{N}^* \\ k & \longmapsto & k+1 \end{matrix}$ est bijective.

2. $P = \{n \in \mathbb{N} \mid n \text{ pair}\}$ et $I = \{n \in \mathbb{N} \mid n \text{ impair}\}$ sont équipotents car $f : \begin{matrix} P & \longrightarrow & I \\ x & \longmapsto & x+1 \end{matrix}$ est bijective.

3. \mathbb{N} et P sont équipotents car $f : \begin{matrix} \mathbb{N} & \longrightarrow & P \\ k & \longmapsto & 2k \end{matrix}$ est bijective.

4. $[0, 1]$ et $[0, 1[$ sont équipotents car

$$f : [0, 1] \longrightarrow [0, 1[$$

$$x \longmapsto \begin{cases} \frac{1}{n+1} & \text{si } x = \frac{1}{n} \text{ avec } n \in \mathbb{N}^* \\ x & \text{sinon} \end{cases}$$

est bijective.

5. De même, $]0, 1[$ et $]0, 1]$ sont équipotents.

6. $]0, 1[$ et $[0, 1[$ sont équipotents : $f : \begin{array}{ccc}]0, 1[& \longrightarrow & [0, 1[\\ x & \longmapsto & 1 - x \end{array}$ est bijective.

7. $\forall a < b$, $[a, b]$ et $[0, 1]$ sont équipotents :

$$\begin{array}{ccc} f : [0, 1] & \longrightarrow & [a, b] \\ \alpha & \longmapsto & \alpha b + (1 - \alpha)a \end{array}$$

est bijective (interpolation linéaire).

8. \mathbb{R} et $]0, 1[$ sont équipotents :

$$\begin{array}{ccc} f : \mathbb{R} & \longrightarrow &]0, 1[\\ x & \longmapsto & \frac{1}{2} + \frac{\text{Arctan } x}{\pi} \end{array}$$

est bijective.

9. $[0, 1[$ et \mathbb{N} ne sont pas équipotents (argument de Cantor). Soit $f : \mathbb{N} \rightarrow [0, 1[$ une bijection :

k	$f(k)$
0	0, 0 0 0 0 ...
1	0, $a_1 a_2 a_3 a_4$...
2	0, $b_1 b_2 b_3 b_4$...
\vdots	\vdots

On considère le nombre

$$x = 0, (a_0 + 1)(b_1 + 1)(c_2 + 1) \cdots$$

$f(1) \neq x$ car ils n'ont pas le même chiffre des dizaines.

$f(2) \neq x$ car ils n'ont pas le même chiffre des centaines.

Par le même raisonnement, on en déduit que

$$\forall n \in \mathbb{N}, f(n) \neq x$$

donc x n'a pas d'antécédant : une contradiction.

10. On verra en exercice que E et $\mathcal{P}(E)$ ne sont pas équipotents. \mathbb{R} et $\mathcal{P}(\mathbb{R})$ ne sont pas équipotents mais \mathbb{R} et $\mathcal{P}(\mathbb{N})$ le sont (développement dyadique).
11. \mathbb{R}^2 et \mathbb{R} sont équipotents ; \mathbb{C} et \mathbb{R} sont équipotents.

EXERCICE:

Soit E un ensemble. L'application

$$\begin{array}{ccc} f : \mathcal{P}(E) & \longrightarrow & 0, 1^E \\ A & \longmapsto & \mathbb{1}_A \end{array}$$

est bijective.

Soit $g : E \rightarrow \{0, 1\}$.

ANALYSE Soit $A \in \mathcal{P}(E)$ tel que $f(A) = g$. Alors $g = \mathbb{1}_A$. donc

$$\forall x \in E, g(x) = \mathbb{1}_A(x)$$

et donc

$$\begin{cases} \forall x \in A, g(x) = 1 \\ \forall x \in E \setminus A, g(x) = 0 \end{cases}$$

On en déduit que

$$A = \{x \in E \mid g(x) = 1\} = g^{-1}(\{1\}).$$

SYNTHÈSE On pose $A = g^{-1}(\{1\})$. Montrons que $f(A) = g$.

$$\forall x \in E, g(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases} = \mathbb{1}_A$$

donc $g = \mathbb{1}_A$.

On aurait aussi pu rédiger de la façon suivante : on pose

$$\begin{aligned} u : \{0, 1\}^E &\longrightarrow \mathcal{P}(E) \\ g &\longmapsto g^{-1}(\{1\}). \end{aligned}$$

On montre que u est la réciproque de f :

$$\begin{cases} f \circ u = \text{id}_{\{0,1\}^E}, \\ u \circ f = \text{id}_{\mathcal{P}(E)}. \end{cases}$$

Définition: Soit $f : E \rightarrow F$. L'image de f est

$$\text{Im}(f) = f(E) = \{f(x) \mid x \in E\}.$$

Proposition: Soit $f : E \rightarrow F$.

$$f \text{ est surjective} \iff f(E) = F.$$

Définition: Une suite de E est une application de \mathbb{N} dans E .

REMARQUE (Notation):

Soit $u \in E^{\mathbb{N}}$. Pour $n \in \mathbb{N}$, on écrit u_n à la place de $u(n)$.

Définition: Soient E et I deux ensembles. Une famille de E indexée par I est une application de I dans E .

À la place de $u(i)$ (avec $i \in I$), on écrit u_i .

Définition: Soit E un ensemble et $(A_i)_{i \in I}$ une famille de parties de E . On suppose $I \neq \emptyset$. On pose

$$\bigcup_{i \in I} A_i = \{x \in E \mid \exists i \in I, x \in A_i\}$$

et

$$\bigcap_{i \in I} A_i = \{x \in E \mid \forall i \in I, x \in A_i\}.$$

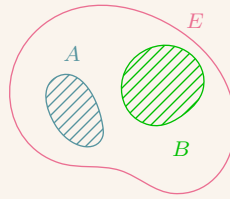
On pose aussi $\bigcup_{i \in \emptyset} A_i = \emptyset$ et $\bigcap_{i \in \emptyset} A_i = E$.

REMARQUE:

De même que pour les sommes et produits de complexes, on peut intervertir des réunions doubles.

Proposition: Soit E un ensemble, $(A, B) \in \mathcal{P}(E)^2$.

$$A \subset (E \setminus B) \iff A \cap B = \emptyset.$$



Preuve: “ \implies ” Soit $x \in A \cap B$. Alors $x \in A$ et $x \in B$. Comme $x \in A \subset (E \setminus B)$, alors $x \in E \setminus B$ i.e. $x \notin B$: une contradiction. Donc $A \cap B = \emptyset$.
 “ \impliedby ” On suppose $A \cap B = \emptyset$. Soit $x \in A$. Si $x \in B$, alors $x \in A \cap B = \emptyset$: faux. Donc $x \notin B$ et donc $x \in E \setminus B$.

□

Proposition: Si $f : E \rightarrow F$ et $g : F \rightarrow G$ sont bijectives, alors $g \circ f$ est bijective et

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

□

REMARQUE (\triangle Attention):

$g \circ f$ peut-être bijective alors que f et g ne le sont pas.