Cours d'algèbre

Maths1
LMD Sciences et Techniques

Par M. Mechab

Avant Propos

Ceci est un avant projet d'un manuel de la partie Algèbre du cours de Mathématiques de premières années LMD Sciences et techniques et Mathématiques et informatique. Il peut aussi être utilement utilisé par les étudiants d'autres paliers aussi bien en sciences et sciences et techniques que ceux de Biologie, Sciences économiques ou autre.

Il sera composé de trois partie.

Cette première partie est un peu les mathématiques générales
La deuxième portera sur une introduction à l'algèbre linéaire
La troisième au calcul matriciel, qui est en fait le but ultime de ce cours.

Toutes les remarques et commentaires sont les bienvenus de la part des étudiants ainsi que de la part d'enseignants ou spécialistes en mathématiques ou utilisateurs de mathématiques.
Ces remarques et commentaires nous permettront certainement d'améliorer le contenu ainsi que la présentation de la version finale.

Elles peuvent être envoyées à :

mustapha.mechab@gmail.com

Pr. Mustapha Mechab.

Table des matières

Chapitre 1

ELÉMENTS DE LOGIQUE

Dans ce chapitre on se limitera à l'introduction des premiers éléments de la logique classique.

Définition 1.1 *On appelle proposition logique toute relation $\mathcal{P}$ qui est soit vraie soit fausse.*

- *Quand la proposition est vraie, on lui affecte la valeur* 1
- *Quand la proposition est fausse, on lui affecte la valeur* 0. [1]

Ces valeurs sont appelées "Valeurs de vérité de la proposition"*.*

Ainsi, pour définir une proposition logique, il suffit de donner ses valeurs de vérités. En général, on met ces valeurs dans un tableu qu'on nommera *"Table de vérités"* ou *"Tableau de vérités"*

L'Equivalence $\Longleftrightarrow$: On dit que deux propositions logiques $\mathcal{P}$ et $\mathcal{Q}$ sont logiquement équivalentes, ou équivalentes, si elles ont les mêmes valeurs de vérité. On note : $\mathcal{P} \Longleftrightarrow \mathcal{Q}$. Sa table de vérités est donnée par :

$\mathcal{P}$	0	0	1	1
$\mathcal{Q}$	0	1	0	1
$\mathcal{P} \Longleftrightarrow \mathcal{Q}$	1	0	0	1

Il est clair que Si $\mathcal{O}$, $\mathcal{P}$ et $\mathcal{Q}$ sont trois propositions logiques, alors : si $\mathcal{O}$ est équivalente à $\mathcal{P}$ et $\mathcal{P}$ équivalente à $\mathcal{Q}$, alors $\mathcal{O}$ est équivalente à $\mathcal{Q}$.

1.1 Opérations Logiques

1.1.1 La négation $\neg$:

Etant donnée une proposition logique $\mathcal{P}$, on appelle négation de $\mathcal{P}$ la proposition logique $\overline{\mathcal{P}}$, qu'on note aussi $\neg\mathcal{P}$, qui est fausse quand $\mathcal{P}$ est vraie et qui est vraie quand $\mathcal{P}$ est fausse, donc on peut la représenter comme suit :

[1] Le fait qu'une proposition ne peut prendre que les valeurs 0 ou 1 provient d'un principe fondamental de la logique "classique" qui est : *Le principe du tiers exclu*, à savoir qu'*une proposition logique ne peut pas être vraie et fausse à la fois.*

$\mathcal{P}$	0	1
$\overline{\mathcal{P}}$	1	0

En établissant les tables de vérités des propositions $(\mathcal{P} \Longleftrightarrow \mathcal{Q})$ et $\left(\overline{\mathcal{P}} \Longleftrightarrow \overline{\mathcal{Q}}\right)$, on déduit que :

$$(\mathcal{P} \Longleftrightarrow \mathcal{Q}) \iff \left(\overline{\mathcal{P}} \Longleftrightarrow \overline{\mathcal{Q}}\right) \tag{1.1}$$

De même, la table de vérités de $\overline{\overline{\mathcal{P}}}$ est la suivante :

$\mathcal{P}$	0	1
$\overline{\mathcal{P}}$	1	0
$\overline{\overline{\mathcal{P}}}$	0	1

on voit qu'elle est identique à celle de $\mathcal{P}$, par suite :

Propriété 1.1 *La négation de la négation d'une proposition logique $\mathcal{P}$ est équivalente à $\mathcal{P}$, donc :*

$$\overline{\overline{\mathcal{P}}} \Longleftrightarrow \mathcal{P}$$

Remarque 1.1 *Pour définir une proposition logique $\mathcal{P}$, il suffit de donner les situations où elle est Vraie, dans le reste des situations la proposition $\mathcal{P}$ étant Fausse et inversement si on connaît les situations où $\mathcal{P}$ est Fausse, dans le reste des situations $\mathcal{P}$ est Vraie.*

1.1.2 La Conjonction $\wedge$

: Etant données deux propositions logiques $\mathcal{P}$ et $\mathcal{Q}$, on appelle conjonction de $\mathcal{P}$ et $\mathcal{Q}$, la proposition logique $\mathcal{P} \wedge \mathcal{Q}$ qui est Vraie quand $\mathcal{P}$ et $\mathcal{Q}$ sont vraies à la fois. Sa table de vérités est donnée par :

$\mathcal{Q} \backslash \mathcal{P}$	0	1
0	0	0
1	0	1

ou

$\mathcal{P}$	0	0	1	1
$\mathcal{Q}$	0	1	0	1
$\mathcal{P} \wedge \mathcal{Q}$	0	0	0	1

Propriété 1.2 *Soit $\mathcal{P}$ une proposition logique, alors $\mathcal{P} \wedge \bar{\mathcal{P}}$ est une proposition fausse.*

Preuve : Pour montrer celà, il suffit de remarque que la table de vérités de $\mathcal{P} \wedge \bar{\mathcal{P}}$ est la suivante :

$\mathcal{P}$	0	1
$\bar{\mathcal{P}}$	1	0
$\mathcal{P} \wedge \bar{\mathcal{P}}$	0	0

□

1.1.3 La Disjonction $\vee$:

Etant données deux propositions logiques $\mathcal{P}$ et $\mathcal{Q}$, on appelle disjonction de $\mathcal{P}$ et $\mathcal{Q}$, la proposition logique $\mathcal{P} \vee \mathcal{Q}$ qui est Vraie si l'une des propositions logiques $\mathcal{P}$ ou $\mathcal{Q}$ est vraie. Sa table de vérités est donnée par :

$\mathcal{Q}\backslash\mathcal{P}$	0	1
0	0	1
1	1	1

ou

$\mathcal{P}$	0	0	1	1
$\mathcal{Q}$	0	1	0	1
$\mathcal{P} \vee \mathcal{Q}$	0	1	1	1

Propriété 1.3 *Soit $\mathcal{P}$ une proposition logique, alors $\mathcal{P} \wedge \bar{\mathcal{P}}$ est une proposition fausse et $\mathcal{P} \vee \bar{\mathcal{P}}$ est toujours vraie.*

Preuve : Pour montrer celà, il suffit de remarque que la table de vérités de $\mathcal{P} \vee \bar{\mathcal{P}}$ est la suivante :

$\mathcal{P}$	0	1
$\bar{\mathcal{P}}$	1	0
$\mathcal{P} \vee \mathcal{P}$	1	1

□

1.1.4 Règles de De Morgan

Propriété 1.4 (Règles de De Morgan) [2][3] *Soient $\mathcal{P}$ et $\mathcal{Q}$ deux propositions logiques, alors :*

1. $\overline{\mathcal{P} \wedge \mathcal{Q}} \Longleftrightarrow \overline{\mathcal{P}} \vee \overline{\mathcal{Q}}$.
2. $\overline{\mathcal{P} \vee \mathcal{Q}} \Longleftrightarrow \overline{\mathcal{P}} \wedge \overline{\mathcal{Q}}$.

Preuve : On établit la preuve de ces règles en donnant les valeurs de vérités des propositions logiques correspondantes.

$\mathcal{P}$	0	0	1	1
$\mathcal{Q}$	0	1	0	1
$\overline{\mathcal{P}}$	1	1	0	0
$\overline{\mathcal{Q}}$	1	0	1	0
$\overline{\mathcal{P}} \vee \overline{\mathcal{Q}}$	1	1	1	0
$\overline{\mathcal{P}} \wedge \overline{\mathcal{Q}}$	1	0	0	0
$\mathcal{P} \vee \mathcal{Q}$	0	1	1	1
$\overline{(\mathcal{P} \vee \mathcal{Q})}$	1	0	0	0
$\mathcal{P} \wedge \mathcal{Q}$	0	0	0	1
$\overline{(\mathcal{P} \wedge \mathcal{Q})}$	1	1	1	0

On voit que les propositions logiques $\overline{(\mathcal{P} \vee \mathcal{Q})}$ et $(\overline{\mathcal{P}} \wedge \overline{\mathcal{Q}})$ ont les mêmes valeurs de vérité, donc elles sont équivalentes. De même pour $\overline{(\mathcal{P} \wedge \mathcal{Q})}$ et $\overline{\mathcal{P}} \vee \overline{\mathcal{Q}}$. □

[2] Connues aussi sous l'appellation de : **Loi de dualité** .

[3] **De Morgan Auguste** : Mathématicien britannique (Madurai Tamil Nadu (Inde) 1806 - Londres 1871). Il est le fondateur avec Boole de la logique moderne.

1.1.5 L'Implication $\Longrightarrow$:

Etant données deux propositions logiques $\mathcal{P}$ et $\mathcal{Q}$, on note $(\mathcal{P} \Longrightarrow \mathcal{Q})$, la proposition logique qui est Fausse si $\mathcal{P}$ est Vraie et $\mathcal{Q}$ est Fausse.
Quand la proposition $(\mathcal{P} \Longrightarrow \mathcal{Q})$ est Vraie, on dit que la proposition $\mathcal{P}$ **implique** la proposition $\mathcal{Q}$.

De cette définition, on obtient la table de vérités suivante :

$\mathcal{Q}\backslash\mathcal{P}$	0	1
0	1	0
1	1	1

ou

$\mathcal{P}$	0	0	1	1
$\mathcal{Q}$	0	1	0	1
$\mathcal{P} \Longrightarrow \mathcal{Q}$	1	1	0	1

Etant données deux propositions logiques $\mathcal{P}$ et $\mathcal{Q}$, alors la table de vérités de $\mathcal{Q} \vee \overline{\mathcal{P}}$ est la suivante :

$\mathcal{Q}\backslash\mathcal{P}$	0	1
0	1	0
1	1	1

ou

$\mathcal{P}$	0	0	1	1
$\mathcal{Q}$	0	1	0	1
$\mathcal{Q} \vee \overline{\mathcal{P}}$	1	1	0	1

On voit que cette table est identique à celle de $\Big(\mathcal{P} \Longrightarrow \mathcal{Q}\Big)$, donc :

$$\Big(\mathcal{P} \Longrightarrow \mathcal{Q}\Big) \Longleftrightarrow \Big(\mathcal{Q} \vee \overline{\mathcal{P}}\Big) \tag{1.2}$$

1.1.6 La contraposée.

Le travail des scientifiques consiste à établir à partir de certaines données ou hypothèses d'autres propriétés. Si on note $\mathcal{P}$ les données ou hypothèses qu'on a et $\mathcal{Q}$ les propriétés qu'on veut établir, alors tout revient à démontrer que $\Big(\mathcal{P} \Longrightarrow \mathcal{Q}\Big)$ est vraie. Ce qui nous fait dire que la tâche des mathématiques consiste en la *démonstration d'implications*.
Dans certaines situations, il est difficile de montrer directement l'implication $\Big(\mathcal{P} \Longrightarrow \mathcal{Q}\Big)$ alors on essaye de donner une autre proposition équivalente qui pourrait être plus facile à établir.

Propriété 1.5 *Etant données deux propositions logiques $\mathcal{P}$ et $\mathcal{Q}$, alors les propositions suivantes sont équivalentes :*
- $(\mathcal{P} \Longrightarrow \mathcal{Q})$
- $(\overline{\mathcal{Q}} \Longrightarrow \overline{\mathcal{P}})$

La deuxième implication est appelée Contraposée *de la première implication.*

Preuve : On donnera la preuve de cette équivalence de deux manière différentes.

1. En utilisant l'équivalence (1.2) on obtient

$$\begin{aligned}(\overline{\mathcal{Q}} \Longrightarrow \overline{\mathcal{P}}) &\Longleftrightarrow \Big(\overline{\mathcal{P}} \vee \overline{\overline{\mathcal{Q}}}\Big)\\ &\Longleftrightarrow \Big(\overline{\mathcal{P}} \vee \mathcal{Q}\Big)\\ &\Longleftrightarrow \Big(\mathcal{Q} \vee \overline{\mathcal{P}}\Big)\\ &\Longleftrightarrow (\mathcal{P} \Longrightarrow \mathcal{Q})\end{aligned}$$

donc : $(\overline{\mathcal{Q}} \Longrightarrow \overline{\mathcal{P}}) \Longleftrightarrow (\mathcal{P} \Longrightarrow \mathcal{Q})$.

2. En utilisant les valeurs de vérité des implications $(\mathcal{P} \Longrightarrow \mathcal{Q})$ et $(\overline{\mathcal{Q}} \Longrightarrow \overline{\mathcal{P}})$, on obtient :

$\mathcal{P}$	0	0	1	1
$\mathcal{Q}$	0	1	0	1
$\mathcal{P} \Longrightarrow \mathcal{Q}$	1	1	0	1
$\overline{\mathcal{Q}}$	1	0	1	0
$\overline{\mathcal{P}}$	1	1	0	0
$\overline{\mathcal{Q}} \Longrightarrow \overline{\mathcal{P}}$	1	1	0	1

d'où on déduit que : $(\mathcal{P} \Longrightarrow \mathcal{Q}) \Longleftrightarrow (\overline{\mathcal{Q}} \Longrightarrow \overline{\mathcal{P}})$.

1.1.7 La réciproque

Etant données P et Q deux propositions logiques, on appelle la **Réciroque** de l'implication $\Big(P \Longrightarrow Q\Big)$ la proposition

$$\Big(Q \Longrightarrow P\Big)$$

1.2 Propriétés des opérations logiques

Propriété 1.6 *Soient $\mathcal{O}$, $\mathcal{P}$ et $\mathcal{Q}$ trois propositions logiques, alors*

1. $\Big((\mathcal{O} \vee \mathcal{P}) \vee \mathcal{Q}\Big) \Longleftrightarrow \Big(\mathcal{O} \vee (\mathcal{P} \vee \mathcal{Q})\Big)$ *(*Associativité de $\vee$*)*
2. $\Big((\mathcal{O} \wedge \mathcal{P}) \wedge \mathcal{Q}\Big) \Longleftrightarrow \Big(\mathcal{O} \wedge (\mathcal{P} \wedge \mathcal{Q})\Big)$ *(*Associativité de $\wedge$*)*
3. $((\mathcal{O} \vee \mathcal{P}) \wedge \mathcal{Q}) \Longleftrightarrow \Big((\mathcal{O} \wedge \mathcal{P}) \vee (\mathcal{O} \wedge \mathcal{Q})\Big)$ *(*Distributivité de $\wedge$ par rapport à $\vee$*)*
4. $\Big((\mathcal{O} \wedge \mathcal{P}) \vee \mathcal{Q}\Big) \Longleftrightarrow \Big((\mathcal{O} \vee \mathcal{Q}) \wedge (\mathcal{P} \vee \mathcal{Q})\Big)$ *(*Distributivité de $\vee$ par rapport à $\wedge$*).*
5. $\Big((\mathcal{O} \Longrightarrow \mathcal{P}) \wedge (\mathcal{P} \Longrightarrow \mathcal{Q})\Big) \Longrightarrow (\mathcal{O} \Longrightarrow \mathcal{Q})$. *(*Transitivité de $\Longrightarrow$*).*

Preuve : On se limitera à la preuve des trois dernières propriétés.

3. Dans le tableau suivant, on remarque que les propositions $\Big[(\mathcal{O} \vee \mathcal{P}) \wedge \mathcal{Q}\Big]$ et $\Big[(\mathcal{O} \wedge \mathcal{P}) \vee (\mathcal{O} \wedge \mathcal{Q})\Big]$ ont les mêmes valeurs de vérité.

$\mathcal{O}$	0	0	0	0	1	1	1	1
$\mathcal{P}$	0	0	1	1	0	0	1	1
$\mathcal{Q}$	0	1	0	1	0	1	0	1
$\mathcal{O} \wedge \mathcal{Q}$	0	0	0	0	0	1	0	1
$\mathcal{P} \wedge \mathcal{Q}$	0	0	0	1	0	0	0	1
$(\mathcal{O} \wedge \mathcal{P}) \vee (\mathcal{O} \wedge \mathcal{Q})$	0	0	0	1	0	1	0	1
$\mathcal{O} \vee \mathcal{P}$	0	0	1	1	1	1	1	1
$(\mathcal{O} \vee \mathcal{P}) \wedge \mathcal{Q}$	0	0	0	1	0	1	0	1

donc : $\Big[(\mathcal{O}\vee\mathcal{P})\wedge\mathcal{Q}\Big]\Longleftrightarrow\Big[(\mathcal{O}\wedge\mathcal{P})\vee(\mathcal{O}\wedge\mathcal{Q})\Big]$.

4. De même, dans le tableau suivant on remarque que les propositions $\Big[(\mathcal{O}\wedge\mathcal{P})\vee\mathcal{Q}\Big]$ et $\Big[(\mathcal{O}\vee\mathcal{Q})\wedge(\mathcal{P}\vee\mathcal{Q})\Big]$ ont les mêmes valeurs de vérité.

$\mathcal{O}$	0	0	0	0	1	1	1	1
$\mathcal{P}$	0	0	1	1	0	0	1	1
$\mathcal{Q}$	0	1	0	1	0	1	0	1
$(\mathcal{O}\wedge\mathcal{P})$	0	0	0	0	0	0	1	1
$(\mathcal{O}\wedge\mathcal{P})\vee\mathcal{Q}$	0	1	0	1	0	1	1	1
$(\mathcal{O}\vee\mathcal{Q})$	0	1	0	1	1	1	1	1
$(\mathcal{P}\vee\mathcal{Q})$	0	1	1	1	0	1	1	1
$(\mathcal{O}\vee\mathcal{Q})\wedge(\mathcal{P}\vee\mathcal{Q})$	0	1	0	1	0	1	1	1

donc : $\Big[(\mathcal{O}\wedge\mathcal{P})\vee\mathcal{Q}\Big]\Longleftrightarrow\Big[(\mathcal{O}\vee\mathcal{Q})\wedge(\mathcal{P}\vee\mathcal{Q})\Big]$.

5. Notons $\mathcal{R}$ la proposition logique :

$$\Big[\Big((\mathcal{O}\Longrightarrow\mathcal{P})\wedge(\mathcal{P}\Longrightarrow\mathcal{Q})\Big)\Longrightarrow(\mathcal{O}\Longrightarrow\mathcal{Q})\Big]$$

En utilisant la définition de l'implication et les propriétés précédentes, on obtient :

$$\begin{array}{rcl}
\mathcal{R} & \Longleftrightarrow & \Big[\Big((\mathcal{O}\Longrightarrow\mathcal{P})\wedge(\mathcal{P}\Longrightarrow\mathcal{Q})\Big)\Longrightarrow(\mathcal{O}\Longrightarrow\mathcal{Q})\Big]\\
& \Longleftrightarrow & \Big[(\mathcal{O}\Longrightarrow\mathcal{Q})\vee\overline{\Big((\mathcal{O}\Longrightarrow\mathcal{P})\wedge(\mathcal{P}\Longrightarrow\mathcal{Q})\Big)}\Big]\\
& \Longleftrightarrow & \Big[(\mathcal{O}\Longrightarrow\mathcal{Q})\vee\Big(\overline{(\mathcal{O}\Longrightarrow\mathcal{P})}\vee\overline{(\mathcal{P}\Longrightarrow\mathcal{Q})}\Big)\Big]\\
& \Longleftrightarrow & \Big[(\mathcal{Q}\vee\overline{\mathcal{O}})\vee\Big(\overline{(\mathcal{P}\vee\overline{\mathcal{O}})}\vee\overline{(\mathcal{Q}\vee\overline{\mathcal{P}})}\Big)\Big]\\
& \Longleftrightarrow & \Big[(\mathcal{Q}\vee\overline{\mathcal{O}})\vee\Big((\overline{\mathcal{P}}\wedge\overline{\overline{\mathcal{O}}})\vee(\overline{\mathcal{Q}}\wedge\overline{\overline{\mathcal{P}}})\Big)\Big]\\
& \Longleftrightarrow & \Big[(\mathcal{Q}\vee\overline{\mathcal{O}})\vee\Big((\overline{\mathcal{P}}\wedge\mathcal{O})\vee(\overline{\mathcal{Q}}\wedge\mathcal{P})\Big)\Big]
\end{array}$$

Ainsi, pour montrer que la proposition $\mathcal{R}$ est vraie, il suffit de montrer que toutes ses valeurs de vérité sont égales à 1. On a :

$\mathcal{O}$	0	0	0	0	1	1	1	1
$\mathcal{P}$	0	0	1	1	0	0	1	1
$\mathcal{Q}$	0	1	0	1	0	1	0	1
$\mathcal{Q}\vee\overline{\mathcal{O}}$	1	1	1	1	0	1	0	1
$\overline{\mathcal{P}}\wedge\mathcal{O}$	0	0	0	0	1	1	0	0
$\overline{Q}\wedge P$	0	0	1	0	0	0	1	0
$\mathcal{R}$	1	1	1	1	1	1	1	1

ce qui montre la véracité de $\mathcal{R}$, donc la transitivité de l'implication.

□

Propriété 1.7 *Etant données deux propositions logiques $\mathcal{P}$ et $\mathcal{Q}$, alors*

$$[\mathcal{P} \Longleftrightarrow \mathcal{Q}] \Longleftrightarrow [(\mathcal{P} \Longrightarrow \mathcal{Q}) \wedge (\mathcal{Q} \Longrightarrow \mathcal{P})]$$

Preuve : Comme :

$$[(\mathcal{P} \Longrightarrow \mathcal{Q}) \wedge (\mathcal{Q} \Longrightarrow \mathcal{P})] \iff (\mathcal{Q} \vee \bar{\mathcal{P}}) \wedge (P \vee \bar{Q})$$

en utilisant la table de vérités suivante :

$\mathcal{P}$	0	0	1	1
$\mathcal{Q}$	0	1	0	1
$\overline{\mathcal{P}}$	1	1	0	0
$\overline{\mathcal{Q}}$	1	0	1	0
$\mathcal{Q} \vee \overline{\mathcal{P}}$	1	1	0	1
$\mathcal{P} \vee \overline{\mathcal{Q}}$	1	0	1	1
$(\mathcal{Q} \vee \overline{\mathcal{P}}) \wedge (\mathcal{P} \vee \overline{\mathcal{Q}})$	1	0	0	1
$\mathcal{P} \wedge \mathcal{Q}$	0	0	0	1
$\overline{\mathcal{P}} \wedge \overline{\mathcal{Q}}$	1	0	0	0
$(\mathcal{Q} \wedge \mathcal{P}) \vee (\bar{\mathcal{P}} \wedge \bar{\mathcal{Q}})$	1	0	0	1
$\mathcal{P} \Longleftrightarrow \mathcal{Q}$	1	0	0	1

on déduit que

$$[\mathcal{P} \Longleftrightarrow \mathcal{Q}] \Longleftrightarrow [(\mathcal{P} \Longrightarrow \mathcal{Q}) \wedge (\mathcal{Q} \Longrightarrow \mathcal{P})]$$

□

Chapitre 2

ELÉMENTS DE LA THÉORIE DES ENSEMBLES

2.1 Les Ensembles

Définition 2.1 *On appelle ensemble E toute collection d'objets, appelés éléments de l'ensemble E. Si le nombre de ces objets est fini, on l'appelle cardinal de E et on le note* $\text{card}(E)$*, si E possède une infinité d'éléments, on dit qu'il est de cardinal infini et on note $CardE = \infty$.*
Si un objet x est un élément de E, on dit que x appartient à E et on note $x \in E$. Si x n'est pas un élément de E, on note $x \notin E$.

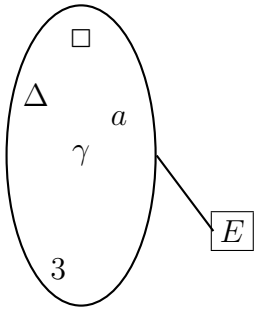
Pour définir un ensemble,
- ou bien on connait la liste de tous ses éléments, on dit alors que l'ensemble est donné "*par Extension*",
- ou bien on connait seulement les relations qui lient les éléments et qui nous permettent de les retrouver tous, on dit alors que l'ensemble est donné par "*Compréhension*".
- Pour représenter un ensemble E, on met les objets qui forment l'enlemble entre deux accolades.

Exemple 2.1
- *Soit A l'ensemble des étudiants de première année SETI (Sciences Exactes, Technologie et Informatique). On ne connait pas tous ces étudiants mais on peut bien les retrouver, donc A est un ensemble donné par compréhension.*

- *Soit $B = \{1, 3, a, y, \gamma, \square\}$. B est défini par extension, car on connait tous ses éléments. Le cardinal de B est égal à 6 ($card(B) = 6$).*

- *Il arrive de représenter un ensemble par un diagramme de Venn*[1].

[1] **Venn John** : mathématicien et logicien britannique, (Hull 1834 - Cambridge 1923). Célèbre pour avoir conçu ses diagrammes qu'il présenta en 1881, lesquels sont employés dans beaucoup de domaines, en théorie des ensembles, en probabilité, en logique, en statistique et en informatique. Elu membre de la Royal Society en 1883.



L'ensemble $E = \{a, \square, \gamma, \Delta, 3\}$.

L'un des axiomes de la téorie des ensembles, est que :

Il existe un ensemble, appelé l'*ensemble vide* et noté $\emptyset$, qui ne contient aucun élément.

On a alors $Card(\emptyset) = 0$.

Un ensemble contenant un seul élément est appelé "*Singleton*", donc de cardinal égal à 1.

2.1.1 Les quantificateurs

On utilise les symboles suivants :

1. $\exists$ le quantificateur existentiel. On écrit $\exists x$ pour lire "*Il existe* x".
2. $\forall$ le quantificateur universel. On écrit $\forall\ x$ pour lire "*Pour tout* x".
3. On écrit $\exists! x$ pour lire "*Il existe un unique* x".

En utilisant ces quantificateurs, pour A un ensemble on a :

– $A = \emptyset \Longleftrightarrow \forall x\,(x \notin A)$

– $$\begin{array}{lll} A \text{ est un singleton} & \Longleftrightarrow & \exists!\, x\,(x \in A) \\ & \Longleftrightarrow & \exists x\,\Big((x \in A) \wedge \Big(\forall y\,(y \in A \Longrightarrow y = x)\Big)\Big) \end{array}$$

2.1.2 Parties d'un ensemble

Définition 2.2 *On dit qu'un ensemble A est inclus dans un ensemble B, ou que A est une partie de l'ensemble B, ou que A est un sous ensemble de B si tout élément de A est un élément de B. On note $A \subset B$ et on a formellement :*

$$A \subset B \Longleftrightarrow \forall\ x(x \in A \Longrightarrow x \in B)$$

Quand A n'est pas une partie de B, on note $A \not\subset B$ et on a formellement :

$$A \not\subset B \Longleftrightarrow \exists x\,((x \in A) \wedge (x \notin B))$$

L'ensemble de toutes les parties d' un ensemble A est noté $\mathcal{P}(A)$. [2]

Exemple : Soit $A = \{a, \alpha, \square\}$, alors

$$\mathcal{P}(A) = \Big\{\emptyset, \{a\}, \{\alpha\}, \{\square\}, \{a, \alpha\}, \{a, \square\}, \{\alpha, \square\}, A\Big\}$$

Propriété 2.1 *Soit A un ensemble, alors $\emptyset \in \mathcal{P}(A)$ et $A \in \mathcal{P}(A)$.*

Définition 2.3 *Soient A et B deux ensembles, on dit que A est égal à B, on note $A = B$, s'ils ont les mêmes éléments.*

Formellement on a :

$$\begin{aligned} A = B &\iff \Big(\forall x(x \in A \iff x \in B)\Big) \\ &\iff \Big((A \subset B) \wedge (B \subset A)\Big) \end{aligned}$$

2.1.3 Opérations sur les ensembles

Définition 2.4 *Soient A et B deux ensembles.*
- *On appelle intersection de A et B, l'ensemble, noté $A \cap B$, des éléments de A appartenant aussi à B.*
- *On appelle réunion de A et B, l'ensemble, noté $A \cup B$, des éléments de A et de ceux de B.*

Formellement, on a :
$A \cap B = \{x;\ (x \in A) \wedge (x \in B)\}$.
$A \cup B = \{x;\ (x \in A) \vee (x \in B)\}$.

Exemple 2.2 *Soient $A = \{a, c, 1, 5, \alpha, \gamma, \square\}$ et $B = \{\zeta, \eta, \gamma, a, x, z\}$, alors :*

$$A \cap B = \{a, \gamma\} \quad et \quad A \cup B = \{a, c, 1, 5, \alpha, \gamma, \square, \zeta, \eta, x, z\}.$$

Propriété 2.2 *Soient A et B deux ensembles, alors*
- $(A \cap B \subset A) \wedge (A \cap B \subset B)$
- $(A \subset A \cup B) \wedge (B \subset A \cup B)$

Si $Z \in \mathcal{P}(A)$, on note :
- $\bigcap\limits_{Y \in Z} Y = \{x;\ (\forall\, Y \in Z,\ x \in Y)\}$.
- $\bigcup\limits_{Y \in Z} Y = \{x;\ (\exists\, Y \in Z,\ x \in Y)\}$.

[2] L'ensemble de tous les ensembles n'existe pas.

Définition 2.5 *Si $A \cap B = \emptyset$, on dit que A et B sont deux ensembles disjoints, et si de plus $E = A \cup B$, on dit que A est le complémentaire de B dans E, ou que A et B sont deux ensembles complémentaires dans E, et on note :*

$$A = \complement_E B \quad ou \quad B = \complement_E A$$

On note aussi :

$$A = E \backslash B$$

En d'autres termes,

Propriété 2.3 *Soit E un ensemble et A une partie de E. On appelle complémentaire de A dans E l'ensemble $\complement_E A$ des éléments de E qui ne sont pas dans A.*

Formellement on a :

$$\boxed{\complement_E A = \Big\{ x \in E;\ x \notin A \Big\}}$$

Avant de donner un exemple, on remarque que si E est un ensemble alors $\emptyset \subset E$ et $(\forall\, x \in E,\ x \notin \emptyset)$, donc : $\complement_E \emptyset = E$.

Exemple 2.3 *Soient $E = \Big\{1, a, \alpha, 3, l, \gamma, \square, \ell, \clubsuit, \spadesuit\Big\}$ et $A = \Big\{1, a, \alpha, \spadesuit\Big\}$, alors :*

$$\complement_E A = \Big\{3, l, \gamma, \square, \ell, \clubsuit\Big\}$$

Propriété 2.4 *Soient E un ensemble et A et B deux parties de E, alors :*

1. $A \subset B \Longleftrightarrow \complement_E B \subset \complement_E A$.
2. $\complement_E \left(\complement_E A\right) = A$.
3. $\complement_E (A \cap B) = \complement_E A \bigcup \complement_E B$
4. $\complement_E (A \cup B) = \complement_E A \bigcap \complement_E B$

Preuve :

1. On a

$$\begin{array}{rcll} A \subset B & \Longleftrightarrow & \forall\, x \in E \Big((x \in A) \Longrightarrow (x \in B) \Big) & \\ & \Longleftrightarrow & \forall\, x \in E \Big((x \notin B) \Longrightarrow (x \notin A) \Big) & \text{Contrapposée de l'implication} \\ & \Longleftrightarrow & \forall\, x \in E \Big((x \in \complement_E B) \Longrightarrow (x \in \complement_E A) \Big) & \\ & \Longleftrightarrow & \complement_E B \subset \complement_E A & \end{array}$$

donc

$$A \subset B \Longleftrightarrow \complement_E B \subset \complement_E A\ .$$

2. Soit $x \in E$, alors

$$\begin{array}{rcl} x \in \complement_E\left(\complement_E A\right) & \Longleftrightarrow & x \notin \complement_E A \\ & \Longleftrightarrow & \overline{\left(x \in \complement_E A\right)} \\ & \Longleftrightarrow & \overline{(x \notin A)} \\ & \Longleftrightarrow & (x \in A) \end{array}$$

donc

$$\complement_E\left(\complement_E A\right) = A \ .$$

3. Soit $x \in E$, alors

$$\begin{array}{rcl} x \in \complement_E(A \cap B) & \Longleftrightarrow & x \notin A \cap B \\ & \Longleftrightarrow & (x \notin A) \vee (x \notin B) \\ & \Longleftrightarrow & (x \in \complement_E A) \vee (x \in \complement_E B) \\ & \Longleftrightarrow & x \in (\complement_E A \cup \complement_E B) \end{array}$$

donc

$$\complement_E(A \cap B) = (\complement_E A \cup \complement_E B) \ .$$

4. Soit $x \in E$, alors

$$\begin{array}{rcl} x \in \complement_E(A \cup B) & \Longleftrightarrow & x \notin A \cup B \\ & \Longleftrightarrow & (x \notin A) \wedge (x \notin B) \\ & \Longleftrightarrow & (x \in \complement_E A) \wedge (x \in \complement_E B) \\ & \Longleftrightarrow & x \in (\complement_E A \cap \complement_E B) \end{array}$$

donc

$$\complement_E(A \cup B) = (\complement_E A \cap \complement_E B) \ .$$

□

De la première propriété on déduit que : $\complement_E E = \emptyset$.

Définition 2.6 *On appelle partition d'un ensemble E, toute famille $\mathcal{F} \subset \mathcal{P}(E)$ telle que :*

1. *Les éléments de la famille $\mathcal{F}$ sont disjoints deux à deux, c'est à dire*

$$\forall\ A,\ B \in \mathcal{F}, \quad A \cap B = \emptyset$$

2. *La famille $\mathcal{F}$ recouvre l'ensemble E ou que $\mathcal{F}$ est un recouvrement de E, c'est à dire*

$$\bigcup_{A \in \mathcal{F}} A = E$$

Propriété 2.5 *Soit E un ensemble, alors pour toute partie A de E, $\mathcal{F} = \left\{\complement_E A, \mathcal{A}\right\}$ est une partition de E.*

Exemple 2.4 *Soit $E = \{1, a, \ell, 3, b, c, d, \alpha, \beta, \gamma\}$, alors :*
$\mathcal{F} = \Big\{\{a, \gamma\},\ \{d, \alpha, \beta\},\ \{c, 1\},\ \{3, \ell\},\ \{b\}\Big\}$ *est une partition de l'ensemble E.* □

Définition 2.7 *Soient A et B deux ensembles non vides, on note $A\times B$ l'ensemble des couples ordonnés (x,y) tels que $x\in A$ et $y\in B$. Il est appelé produit cartésien*[3] *des ensembles A et B. On convient que*

$$\forall\ (x,y),\ (x',y')\in A\times B,\quad (x,y)=(x',y')\Longleftrightarrow\Big((x=x')\wedge(y=y')\Big).$$

Exemple 2.5 *Soient* $A=\Big\{1,5,\square\Big\}$ *et* $B=\Big\{a,\alpha,\clubsuit,\heartsuit,\spadesuit\Big\}$, *alors*

$$\begin{aligned}A\times B &= \Big\{(1,a),(5,a),(\square,a),(1,\alpha),(5,\alpha),(\square,\alpha),(1,\clubsuit),(5,\clubsuit),(\square,\clubsuit),\\ &\qquad (1,\heartsuit),(5,\heartsuit),(\square,\heartsuit),(1,\spadesuit),(5,\spadesuit),(\square,\spadesuit)\Big\}\\ B\times A &= \Big\{(a,1),(a,5),(a,\square),(\alpha,1),(\alpha,5),(\alpha,\square),(\clubsuit,1),(\clubsuit,5),(\clubsuit,\square),\\ &\qquad (\heartsuit,1),(\heartsuit,5),(\heartsuit,\square),(\spadesuit,1),(\spadesuit,5),(\spadesuit,\square)\Big\}\end{aligned}$$

Remarque 2.1 *$A\times B=B\times A$ si et seulement si $A=B$.*

2.2 Applications et Fonctions

Définition 2.8 *On appelle application d'un ensemble E dans un ensemble F, toute correspondance f entre les éléments de E et ceux de F qui à tout élément $x\in E$ fait correspondre un unique élément $y\in F$ noté $f(x)$.*

- *$y=f(x)$ est appelé image de x et x est un antécédant de y.*
- *On représente l'application f de E dans F par $f:E\longrightarrow F$. E est appelé ensemble de départ et F l'ensemble d'arrivée de l'application f.*

Une correspondance entre E et F est représentée par : $\quad f:E\rightsquigarrow F$

Une application f entre E et F est aussi représentée par :

$$\begin{array}{rccc} f: & E & \longrightarrow & F\\ & x & \longrightarrow & f(x)\end{array}$$

Formellement, une correspondance f entre deux ensembles non vides est une application si et seulement si :

$$\boxed{\forall x,\ x'\in E\ \Big((x=x')\Longrightarrow(f(x)=f(x')\ )\Big).}$$

Exemple 2.6 *L'application $Id_E:E\longrightarrow E$ telle que*

$$\forall\, x\in E,\qquad Id_E(x)=x$$

est appelée **application identité sur** *E.*

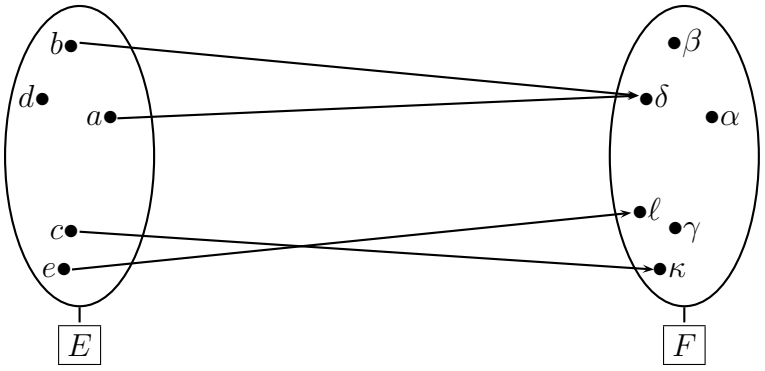
[3] **DESCARTES René** : Philosophe, physicien et mathématicien français (La Haye 1596-Stockholm 1650). Il créa l'algèbre des polynômes , avec Fermat il fonda la géométrie analytique. Ennonça les propriétés fondamentales des équations algébriques et simplifia les notations algébriques en adoptant les premières lettres de l'alphabet pour désigner les constantes et les dernières lettres pour désigner les variables. Publia "Le Discours de la méthode", qui est une référence pour le raisonnement logique. Découvrit aussi les principes (régles) de l'optique géométrique.

Exemple 2.7 *Soient E et F deux ensembles non vides et a un élément de F, alors la correspondance f de E dans F définie par :*

$$\forall x \in E, \qquad x \rightsquigarrow a$$

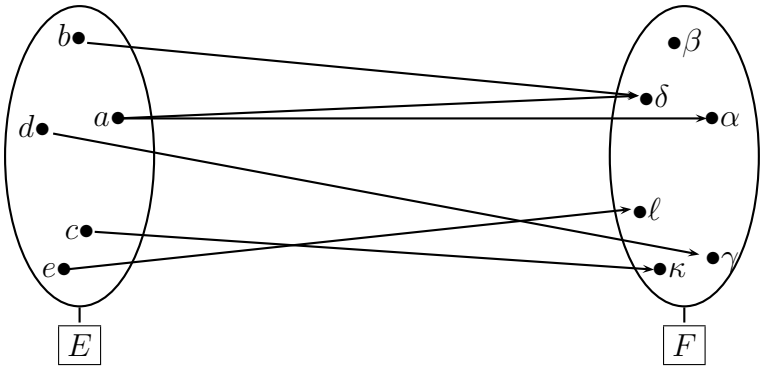
est une application dite **application constante**.

Exemple 2.8



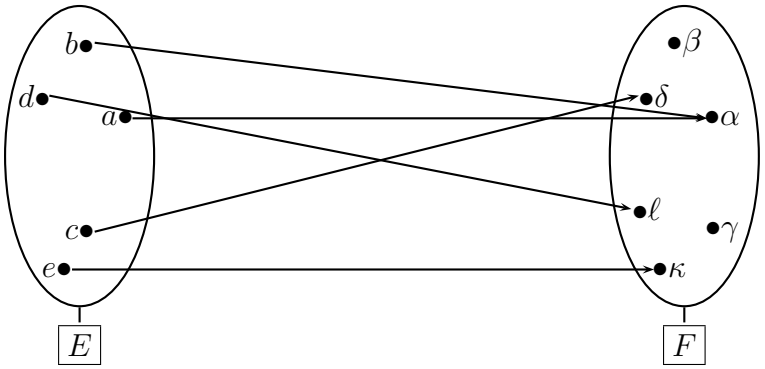
Cette correspondance n'est pas une application car il existe un élément $d \in E$ qui n'a pas d'image dans F.

Exemple 2.9



Cette correspondance n'est pas une application car il existe un élément $a \in E$ qui a deux images α et δ dans F.

Exemple 2.10



Cette correspondance est une application malgré qu'il existe des éléments de F qui n'ont pas d'antécedents dans E et plusieurs éléments de E qui ont une même image dans F.

Définition 2.9 *On dit que deux applications f et g sont égales si :*

1. *Elles ont un même ensemble de départ E et un même ensemble d'arrivée F.*
2. $\forall x \in E, \quad f(x) = g(x)$.

Exemple 2.11 *On considère les applications suivantes*[4] *:*

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longrightarrow & x^2 \end{array} \qquad \begin{array}{rccc} g: & \mathbb{R} & \longrightarrow & \mathbb{R}_+ \\ & x & \longrightarrow & x^2 \end{array} \qquad \begin{array}{rccc} h: & \mathbb{R}_+ & \longrightarrow & \mathbb{R} \\ & x & \longrightarrow & x^2 \end{array} \qquad \begin{array}{rccc} k: & \mathbb{R}_+ & \longrightarrow & \mathbb{R}_+ \\ & x & \longrightarrow & x^2 \end{array}$$

alors :

$f \neq g$, *car elles n'ont pas le même ensemble d'arrivée.*
$f \neq h$, *car elles n'ont pas le même ensemble de départ.*
$f \neq k$, *car elles n'ont pas ni le même ensemble de départ ni le même ensemble d'arrivée.*

Définition 2.10 *On appelle graphe d'une application $f : E \longrightarrow F$, l'ensemble*

$$\Gamma_f = \{(x, f(x)),\ x \in E\}$$

En fait, la définition d'une application f revient à la donnée d'un sous ensemble Γ_f de $E \times F$ tel que

$$\forall (x, y),\ (x', y') \in \Gamma_f, \qquad \Big((x, y) = (x', y') \Longleftrightarrow x = x'\Big)$$

2.2.1 Composition d'applications

Définition 2.11 *Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$, on note $g \circ f$ l'application de E dans G définie par :*

$$\forall x \in E, \quad gof(x) = g(f(x))$$

Cette application[5] *est appelée composée des applications f et g.*

Exemple 2.12 *Etant données les applications*

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R}_+ \\ & x & \longrightarrow & x^2 \end{array} \quad et \quad \begin{array}{rccc} g: & \mathbb{R}_+ & \longrightarrow & \mathbb{R}_+ \\ & x & \longrightarrow & x^3 \end{array}$$

alors

$$\begin{array}{rccc} g \circ f: & \mathbb{R} & \longrightarrow & \mathbb{R}_+ \\ & x & \longrightarrow & (x^2)^3 = x^6 \end{array} \quad et \quad \begin{array}{rccc} f \circ g: & \mathbb{R}_+ & \longrightarrow & \mathbb{R}_+ \\ & x & \longrightarrow & (x^3)^2 = x^6 \end{array}$$

Il est claire que $\boxed{f \circ g \neq g \circ f}$.

[4] $\mathbb{R}$ est l'ensemble des nombres réels.

[5] $g \circ f$ est une application car pour $x,\ x' \in E$, si $x = x'$ alors $f(x) = f(x')$ car f est une application et comme g est une application alors $g(f(x)) = g(f(x'))$, donc $g \circ f(x) = g \circ f(x')$.

2.2.2 Restriction et prolongement d'une application

Définition 2.12 *Etant donnée une application $f : E \longrightarrow F$.*

1. *On appelle restriction de f à un sous ensemble non vide X de E, l'application $g : X \longrightarrow F$ telle que*
$$\forall x \in X, \quad g(x) = f(x)$$
On note $g = f_{/X}$.
2. *Etant donné un ensemble G tel que $E \subset G$, on appelle prolongement de l'application f à l'ensemble G, toute application h de G dans F telle que f est la restriction de h à E.*

D'après cette définition, f est un prolongement de $f_{/X}$ à E.

Remarque 2.2 *Si F n'est pas un singleton, alors le prolongement de f n'est pas unique.*

Exemple 2.13 *Etant donnée l'application*
$$\begin{array}{rccc} f: & \mathbb{R}_+ & \longrightarrow & \mathbb{R} \\ & x & \longrightarrow & \log x \end{array}$$
alors
$$\begin{array}{rccc} g: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longrightarrow & \log|x| \end{array} \quad et \quad \begin{array}{rccc} h: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longrightarrow & \log(2|x| - x) \end{array}$$
sont deux prolongements différents de f à $\mathbb{R}$.

2.2.3 Images et images réciproques

Définition 2.13 *Soient $A \subset E$ et $M \subset F$.*

1. *On appelle image de A par f, l'ensemble des images des éléments de A noté :*
$$f(A) = \{f(x), \quad x \in A\} \subset F$$
2. *On appelle image réciproque de M par f, l'ensemble des antécédents des éléments de M, noté*
$$f^{-1}(M) = \{x \in E, \quad f(x) \in M\} \subset E$$

Formellement on a :
$$\forall\, y \in F,\ \Big(y \in f(A) \iff \exists x \in A,\ y = f(x)\Big)$$
$$\forall\, x \in E,\ \Big(x \in f^{-1}(M) \iff f(x) \in M\Big)$$

Remarque 2.3 *Etant données deux applications $f : E \longrightarrow F$ et $g : F' \longrightarrow G$, alors on peut définir l'application composée $g \circ f : E \longrightarrow G$, si $f(E) \subset F'$.*

Exemple 2.14 *Soient*

$$f:\begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R}\\ x & \longrightarrow & x^2\end{array} \quad et \quad h:\begin{array}{ccc}\mathbb{R}_+ & \longrightarrow & \mathbb{R}\\ x & \longrightarrow & \log x\end{array}$$

alors $h\circ f$ est définie par :

$$h\circ f:\begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R}\\ x & \longrightarrow & \log x^2\end{array}$$

Proposition 2.1 *Soient $f : E \longrightarrow F$, $A,\ B \subset E$ et $M,\ N \subset F$, alors*

1. $f(A\cup B) = f(A)\cup f(B)$
2. $f(A\cap B) \subset f(A)\cap f(B)$
3. $f^{-1}(M\cup N) = f^{-1}(M)\cup f^{-1}(N)$
4. $f^{-1}(M\cap N) = f^{-1}(M)\cap f^{-1}(N)$
5. $f^{-1}\left(\complement_F M\right) = \complement_E f^{-1}(M)$

Preuve :

1. Soit $y\in F$, alors

$$\begin{array}{rcl} y\in f(A\cup B) & \Longleftrightarrow & \exists x\in A\cup B;\ y=f(x)\\ & \Longleftrightarrow & \exists x\left[\Big((x\in A)\vee(x\in B)\Big)\wedge\Big(y=f(x)\Big)\right]\\ & \Longleftrightarrow & \exists x\left[\ \Big((x\in A)\wedge(y=f(x))\Big)\vee\Big((x\in B)\wedge(y=f(x))\Big)\ \right]\\ & \Longleftrightarrow & \Big[\exists x\Big((x\in A)\wedge(y=f(x))\Big)\Big]\vee\Big[\exists x\Big((x\in B)\wedge(y=f(x))\Big)\Big]\\ & \Longleftrightarrow & (y\in f(A))\vee(y\in f(B))\\ & \Longleftrightarrow & y\in f(A)\cup f(B)\end{array}$$

ce qui montre que $f(A\cup B) = f(A)\cup f(B)$.

2. Soit $y\in F$, alors

$$\begin{array}{rcl} y\in f(A\cap B) & \Longleftrightarrow & \exists x\in A\cap B;\ y=f(x)\\ & \Longleftrightarrow & \exists x\Big((x\in A)\wedge(x\in B)\wedge(y=f(x))\Big)\\ & \Longleftrightarrow & \exists x\left[\Big((x\in A)\wedge(y=f(x))\Big)\wedge\Big((x\in B)\wedge(y=f(x))\Big)\right]\\ & \Longrightarrow & \Big[\exists x\Big((x\in A)\wedge(y=f(x))\Big)\Big]\wedge\Big[\exists x\Big((x\in B)\wedge(y=f(x))\Big)\Big]\\ & \Longrightarrow & (y\in f(A))\wedge(y\in f(B)\\ & \Longrightarrow & y\in f(A)\cap f(B)\end{array}$$

ce qui montre que $f(A\cap B)\subset f(A)\cap f(B)$.

3. Soit $x\in E$, alors

$$\begin{array}{rcl} x\in f^{-1}(M\cup N) & \Longleftrightarrow & f(x)\in M\cup N\\ & \Longleftrightarrow & \Big(f(x)\in M\Big)\vee\Big(f(x)\in N\Big)\\ & \Longleftrightarrow & \Big(x\in f^{-1}(M)\Big)\vee\Big(x\in f^{-1}(N)\Big)\\ & \Longleftrightarrow & x\in f^{-1}(M)\cup f^{-1}(N)\end{array}$$

ce qui montre que $f^{-1}(M \cup N) = f^{-1}(M) \cup f^{-1}(N)$.

4. Soit $x \in E$, alors

$$\begin{array}{rcl} x \in f^{-1}(M \cap N) & \Longleftrightarrow & f(x) \in M \cap N \\ & \Longleftrightarrow & \Big(f(x) \in M\Big) \wedge \Big(f(x) \in N\Big) \\ & \Longleftrightarrow & \Big(x \in f^{-1}(M)\Big) \wedge \Big(x \in f^{-1}(N)\Big) \\ & \Longleftrightarrow & x \in f^{-1}(M) \cap f^{-1}(N) \end{array}$$

ce qui montre que $f^{-1}(M \cap N) = f^{-1}(M) \cap f^{-1}(N)$.

5. Soit $x \in E$, alors

$$\begin{array}{rcl} x \in f^{-1}\left(\complement_F M\right) & \Longleftrightarrow & f(x) \in \complement_F M \\ & \Longleftrightarrow & \Big(f(x) \in F\Big) \wedge \Big(f(x) \notin M\Big) \\ & \Longleftrightarrow & \Big(x \in E\Big) \wedge \Big(x \notin f^{-1}(M)\Big) \\ & \Longleftrightarrow & x \in \complement_E f^{-1}(M) \end{array}$$

ce qui montre que $f^{-1}\left(\complement_F\right) = \complement_E f^{-1}(M)$.

Remarque 2.4 *Les ensembles $\complement_F f(A)$ et $f\left(\complement_E A\right)$ ne sont pas toujours comparables.*

Exemple 2.15 *Soient $E = \Big\{a, \beta, \gamma, \spadesuit\Big\}$, $F = \Big\{\ell, \zeta, \heartsuit, \Big\}$ et l'application $f : E \longrightarrow F$ définie par :*

$$f(a) = f(\beta) = \ell \qquad et \qquad f(\gamma) = f(\spadesuit) = \zeta$$

On considère l'ensemble $A = \Big\{a, \gamma\Big\}$, alors

- $f(A) = \Big\{\ell, \zeta\Big\}$ *et* $\complement_F f(A) = \{\heartsuit\}$
- $\complement_E A = \Big\{\beta, \spadesuit\Big\}$ *et* $f(\complement_E A) = \Big\{\ell, \zeta\Big\}$

donc $\complement_F f(A) \not\subset f(\complement_E A)$ et $f(\complement_E A) \not\subset \complement_F f(A)$, c'est à dire que $\complement_F f(A)$ et $f(\complement_E A)$ ne sont pas comparables dans cet exemple.

□

On peut prendre le deuxième exemple suivant.

Exemple 2.16 *Etant donnés $E = \{-3, -2, -1, 0, 1, 2, 3, 4\}$, $F = \{-1, 0, 1, 2, 4, 5, 9, 10, 16\}$ et l'application $f : E \longrightarrow F$ définie par :*

$$\forall\, x \in E, \quad f(x) = x^2$$

On considère l'ensemble $A = \{0, 1, 2, 4\}$, alors $\complement_E A = \{-3, -2, -1, 3\}$, $f(A) = \{0, 1, 4, 16\}$, $f\left(\complement_E A\right) = \{1, 4, 9\}$ et $\complement_F f(A) = \{-1, 2, 5, 9, 10\}$, donc

$$\complement_F f(A) \not\subset f(\complement_E A) \qquad et \qquad f(\complement_E A) \not\subset \complement_F f(A),$$

c'est à dire que $\complement_F f(A)$ *et* $f(\complement_E A)$ *ne sont pas comparables.*

Mais si on prend $B = \{-2, -1, 0, 1, 2\}$*, alors :*
$\complement_E B = \{-3, 4\}$*,* $f(B) = \{0, 1, 4\}$*,* $f\left(\complement_E B\right) = \{9, 16\}$ *et* $\complement_F f(B) = \{-1, 2, 5, 9, 10, 16\}$
donc

$$f\left(\complement_E B\right) \subset \complement_F f(B)\ .$$

□

2.2.4 Applications injectives, surjectives, bijectives

Définition 2.14 *On dit que :*

1. *f est injective si tout élément de F possède au plus un antécédant.*
2. *f est surjective si tout élément de F possède au moins un antécédant.*
3. *f est bijective si elle est injective et surjective*

La première propriété est équivalente à dire que deux éléments distincts de E ne peuvent pas être des antécédents d'un même élément de F, ce qui revient formellement a :

$$\boxed{f \text{ injective } \Longleftrightarrow \forall\ x,\ x' \in E,\ (x \neq x' \Longrightarrow f(x) \neq f(x')\ )}$$

En prenant la contrapposée de l'implication, dans la deuxième proposition de cette équivalence, on obtient

$$\boxed{f \text{ injective } \Longleftrightarrow \forall\ x,\ x' \in E,\ (f(x) = f(x') \Longrightarrow x = x')}$$

De même

$$\boxed{f \text{ surjective } \Longleftrightarrow \forall\ y \in F,\ \exists x \in E,\ f(x) = y}$$

d'où on déduit :

$$\boxed{f \text{ bijective } \Longleftrightarrow \forall\ y \in F,\ \exists!\ x \in F;\ f(x) = y.}$$

L'application réciproque

Proposition 2.2 *Une application $f : E \longrightarrow F$ est bijective si et seulement si il existe une unique application $g : F \longrightarrow E$ telle que*

$$fog = Id_F \quad et \quad gof = Id_E.$$

On dit que f est inversible et g, notée f^{-1}, est appelée "l'application réciproque" ou "l'application inverse" de f.

Preuve :

I.) Supposons qu'il existe une application $g : F \longrightarrow E$ telle que

$$fog = Id_F \quad \text{et} \quad gof = Id_E.$$

Montrons que f est bijective.

1. Soit $y \in F$, comme $fog = Id_F$ alors $fog(y) = y$, par suite il existe $x = g(y) \in E$ tel que $f(x) = y$, ce qui montre que f est surjective.
2. Soient $x,\ x' \in E$, comme $gof = Id_E$ alors $gof(x) = x$ et $gof(x') = x'$, par suite :

$$\begin{array}{rcll} f(x) = f(x') & \Longrightarrow & g(f(x)) = g(f(x')) & \text{car } g \text{ application} \\ & \Longrightarrow & gof(x) = gof(x') & \\ & \Longrightarrow & x = x' & \end{array}$$

ce qui montre que f est injective.
De 1. et 2. on déduit que f est bijective.

II.) Supposons que f est bijective.
Construisons l'unique application $g : F \longrightarrow E$ telle que

$$fog = Id_F \quad \text{et} \quad gof = Id_E.$$

f étant bijective, alors : $\forall y \in F,\ \exists! x \in E; \quad y = f(x)$.
Ainsi, à tout élément $y \in F$, on fait associer un unique élément $x \in E$, qu'on notera $g(x)$, tel que $f(x) = y$. On définit ainsi une application

$$\begin{array}{rccc} g : & F & \longrightarrow & E \\ & y & \longrightarrow & g(y) = x \end{array}$$

Montrons que $fog = Id_F \quad \text{et} \quad gof = Id_E$..

1. Soit $y \in F$, alors $g(y) = x$, avec $f(x) = y$, donc

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

ce qui montre que : $f \circ g = Id_F$.

2. Soit $x \in E$, alors pour $y = f(x)$ on a $g(y) = x$, par suite

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

ce qui montre que : $g \circ f = Id_E$.

3. Montrons l'unicité de g. Soit $g_1 : F \longrightarrow E$ vérifiant les deux propriétés précédentes, alors pour tout $y \in F$, il existe $x \in E$ tel que $y = f(x)$, donc

$$g_1(y) = g_1(f(x)) = g_1 \circ f(x) = Id_E(x) = g \circ f(x) = g(f(x)) = g(y)$$

ce qui montre que $g_1 = g$.

□

Exemple 2.17 *On considère l'application*

$$\begin{array}{rccc} f: & \mathbb{R}\backslash\{2\} & \longrightarrow & F \\ & x & \longrightarrow & \dfrac{x+5}{x-2} \end{array}$$

avec F un sous ensemble de $\mathbb{R}$.
Déterminer F pour que l'application f soit bijective et donner l'application inverse de f.

Montrer que f est bijective revient à examiner l'existence de solution de l'équation $y = f(x)$, pour tout $y \in F$.

Soit $y \in F$, alors

$$\begin{array}{rcl} y = f(x) & \Longleftrightarrow & y = \dfrac{x+5}{x-2} \\ & \Longleftrightarrow & y(x-2) = x+5 \\ & \Longleftrightarrow & yx - x = 5 + 2y \\ & \Longleftrightarrow & x(y-1) = 5+2y \\ & \Longleftrightarrow & x = \dfrac{5+2y}{y-1} \quad \text{si } y \neq 1 \end{array}$$

ce qui montre que :

$$\forall\, y \in \mathbb{R}\backslash\{1\},\ \exists!\, x = \frac{5+2y}{y-1}; \qquad y = f(x)$$

pour montrer que f est bijective, il reste à voir si $x = \dfrac{5+2y}{y-1} \in \mathbb{R}\backslash\{2\}$?.
On a :

$$\begin{array}{rcl} \dfrac{5+2y}{y-1} = 2 & \Longleftrightarrow & 5+2y = 2(y-1) \\ & \Longleftrightarrow & 5 = -2 \quad \text{ce qui est impossible} \end{array}$$

ce qui montre que $\dfrac{5+2y}{y-1} \in \mathbb{R}\backslash\{2\}$, par suite :

$$\forall\, y \in \mathbb{R}\backslash\{1\},\ \exists!\, x = \frac{5+2y}{y-1} \in \mathbb{R}\backslash\{2\}; \qquad y = f(x)$$

donc f est bijective si $F = \mathbb{R}\backslash\{1\}$ et l'inverse de f est :

$$\begin{array}{rccc} f^{-1}: & \mathbb{R}\backslash\{1\} & \longrightarrow & \mathbb{R}\backslash\{2\} \\ & y & \longrightarrow & \dfrac{5+2y}{y-1} \end{array}$$

□

Remarque 2.5 *Il est clair que si f est bijective, il en est de même de f^{-1} et on a $(f^{-1})^{-1} = f$. On dit que f est une bijection entre E et F et que E et F sont deux ensembles équipotents.*

Proposition 2.3 *Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$, alors*

1. *(f injective) $\wedge$ (g injective) $\Longrightarrow$ ($g \circ f$ injective).*

2. $(f$ *surjective* $) \wedge (g$ *surjective* $) \Longrightarrow (g \circ f$ *surjective* $)$.
3. $(f$ *bijective* $) \wedge (g$ *bijective* $) \Longrightarrow (g \circ f$ *bijective et* $(g \circ f)^{-1} = f^{-1} \circ g^{-1})$.

Preuve : On a $g \circ f : E \longrightarrow G$.

1. Supposons f et g injectives et montrons que $g \circ f$ est injective.
Soient $x,\ x' \in E$, alors :

$$\begin{array}{rcl} x \neq x' & \Longrightarrow & f(x) \neq f(x') \quad \text{car } f \text{ injective} \\ & \Longrightarrow & g\left(f(x)\right) \neq g\left(f(x')\right) \quad \text{car } g \text{ injective} \\ & \Longrightarrow & g \circ f(x) \neq g \circ f(x') \end{array}$$

ce qui montre que $g \circ f$ est injective.

2. Supposons f et g surjectives et montrons que $g \circ f$ est surjective.
Soit $z \in G$, g étant surjective, il existe $y \in F$ tel que $z = g(y)$, comme $y \in F$ et f est surjective alors il existe $x \in E$ tel que $y = f(x)$, donc $z = g(f(x))$ et on déduit que :

$$\forall\, z \in G,\ \exists x \in E; \quad z = g \circ f(x)$$

ce qui montre que $g \circ f$ est surjective.

3. De **1.** et **2.** on déduit que si f et g sont bijectives alors $g \circ f$ est bijective.
Montrons que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
D'après **2.** , pour $z \in G$, $z = g(y)$, $y = f(x)$ et $z = g \circ f(x)$, comme f, g et $g \circ f$ sont bijectives, alors $y = g^{-1}(z)$, $x = f^{-1}(y)$ et $x = (g \circ f)^{-1}(z)$, par suite

$$\forall z \in G, \qquad (g \circ f)^{-1}(z) = x = f^{-1}(y) = f^{-1}\left(g^{-1}(z)\right) = f^{-1} \circ g^{-1}(z)$$

donc : $\quad (g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

Remarque 2.6 *Les réciproques de ces implications ne sont pas vraies, pour s'en convaincre il suffit de prendre l'exemple suivant.*
Etant données les applications suivantes :

$$f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longrightarrow & \exp x \end{array} \quad et \quad g : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longrightarrow & \ln(|x|) \end{array}$$

alors

$$g \circ f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longrightarrow & x \end{array}$$

est injective malgré que g ne le soit pas et $g \circ f$ est surjective malgré que f ne le soit pas.

En remplacement des réciproques des implications antérieures, on a :

Proposition 2.4 *Etant données deux applications $f : E \longrightarrow F$ et $g : F' \longrightarrow G$, telles que $F \subset F'$, alors :*

1. $\Big(g \circ f$ *injective*$\Big) \Longrightarrow f$ *injective.*

2. $\Big(g \circ f \quad \textit{surjective}\Big) \Longrightarrow g \quad \textit{surjective.}$

3. Si $f(E) = F'$, *alors* $\Big(g \circ f \quad \textit{injective}\Big) \Longrightarrow g \quad \textit{injective.}$

Preuve : Comme $F \subset F'$, alors $g \circ f : E \longrightarrow G$ est bien définie.

1. Supposons que $g \circ f$ est injective et montrons que f est injective. Soient $x,\ x' \in E$, alors

$$\begin{array}{rcll} f(x) = f(x') & \Longrightarrow & g\Big(f(x)\Big) = g\Big(f(x')\Big) & \text{car } g \text{ est une application} \\ & \Longrightarrow & g \circ f(x) = g \circ f(x') & \\ & \Longrightarrow & x = x' & \text{car } g \circ f \text{ est injective} \end{array}$$

donc :

$$\forall\, x,\ x' \in E, \qquad \Big(f(x) = f(x')\Big) \Longrightarrow \Big(x = x'\Big)$$

ce qui montre que f est injective.

2. Supposons que $g \circ f$ est surjective et montrons que g est surjective. Soit $z \in G$, alors

$$\begin{array}{rcl} g \circ f \text{ surjective} & \Longrightarrow & \exists x \in E; \quad g \circ f(x) = z \\ & \Longrightarrow & \exists x \in E; \quad g\Big(f(x)\Big) = z \\ & \Longrightarrow & \exists y = f(x) \in F; \qquad g(y) = z \end{array}$$

donc

$$\forall\, z \in G,\ \exists y \in F; \quad g(y) = z$$

ce qui montre que g est surjective.

3. Soient $f : E \longrightarrow F$ et $g : F' \longrightarrow G$, avec $F' = f(E)$. Supposons que $g \circ f$ est injective et montrons que g est injective. Soient $y,\ y' \in F' = f(E)$, alors il existe $x,\ x' \in E$ tels que $y = f(x)$ et $y' = f(x')$, donc :

$$\begin{array}{rcll} g(y) = g(y') & \Longrightarrow & g\Big(f(x)\Big) = g\Big(f(x')\Big) & \\ & \Longrightarrow & g \circ f(x) = g \circ f(x') & \\ & \Longrightarrow & x = x' & \text{car } g \circ f \text{ est injective} \\ & \Longrightarrow & f(x) = f(x') & \text{car } f \text{ application} \\ & \Longrightarrow & y = y' & \end{array}$$

ce qui montre que g est injective.

□

2.2.5 Fonctions

Définition 2.15 *On appelle fonction de E dans F, toute application f d'un sous ensemble $\mathcal{D}_f \subset E$ dans F. $\mathcal{D}_f$ est appelé "Ensemble de définition de f".*

Remarque 2.7 *Toutes les notions données pour les applications peuvent être adaptées pour les fonctions.*

Chapitre 3

Relations binaires

Définition 3.1 *On appelle relation binaire, toute assertion entre deux objets, pouvant être vérifiée ou non. On note $x\mathcal{R}y$ et on lit "x est en relation avec y".*

Définition 3.2 *Etant donnée une relation binaire $\mathcal{R}$ entre les éléments d'un ensemble non vide E, on dit que :*

1. *$\mathcal{R}$ est Reflexive $\Longleftrightarrow \forall\ x \in E\ (x\mathcal{R}x)$,*
2. *$\mathcal{R}$ est Transitive $\Longleftrightarrow \forall\ x,\ y,\ z \in E\ \Big(\ \Big((x\mathcal{R}y) \wedge (y\mathcal{R}z)\Big) \Longrightarrow (x\mathcal{R}z)\Big)$*
3. *$\mathcal{R}$ est Symétrique $\Longleftrightarrow \forall\ x,\ y \in E\ \Big(\ (x\mathcal{R}y) \Longrightarrow (y\mathcal{R}x)\ \Big)$*
4. *$\mathcal{R}$ est Anti-Symétrique $\Longleftrightarrow \forall\ x,\ y \in E\ \Big(\ \Big((x\mathcal{R}y) \wedge (y\mathcal{R}x)\Big) \Longrightarrow x = y\ \Big)$*

3.1 Relations d'équivalence

Définition 3.3 *On dit qu'une relation binaire $\mathcal{R}$ sur un ensemble E est une relation d'équivalence si elle est* **R***éflexive,* **S***ymétrique et* **T***ransitive.*

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E.

Définition 3.4

- *On dit que deux éléments x et $y \in E$ sont équivalents si $x\mathcal{R}y$.*
- *On appelle classe d'équivalence d'un élément $x \in E$, l'ensemble : $\dot{x} = \{y \in E;\ \ x\mathcal{R}y\}$.*
- *x est dit un représentant de la calsse d'équivalence $\dot{x}$.*
- *On appelle ensemble quotient de E par la relation d'équivalence $\mathcal{R}$, l'ensemble des classes d'équivalence de tous les éléments de E. Cet ensemble est noté $E_{/\mathcal{R}}$.*
- *L'application s de E dans $E_{/\mathcal{R}}$ telle que pour tout $x \in E$, $\mathsf{s}(x) = \dot{x}$, est appelée "surjection canonique" de E sur $E_{/\mathcal{R}}$.*

Exemple 3.1 *Etant donné E un ensemble non vide, alors*

L'egalité est une relation d'équivalence dans E

Exemple 3.2 *Dans* $\mathbb{R}$ *on définit la relation* $\mathfrak{R}$ *par :*

$$\forall\, x,\ y \in \mathbb{R}, \qquad x\mathfrak{R}y \Longleftrightarrow x^2 - 1 = y^2 - 1$$

Montrer que $\mathfrak{R}$ *est une relation d'équivalence et donner l'ensemble quotient* $\mathbb{R}_{/\mathfrak{R}}$.

1. $\mathfrak{R}$ *est une relation d'équivalence.*

I) $\mathfrak{R}$ *est une relation Reflexive, car d'après la Réflexivité de l'égalité on a :*

$$\forall\, x,\ y \in \mathbb{R},\ x^2 - 1 = x^2 - 1,$$

donc

$$\forall\, x,\ y \in \mathbb{R}, \qquad x\mathfrak{R}x$$

ce qui montre que $\mathfrak{R}$ *est une relation Réflexive.*

II) $\mathfrak{R}$ *est une relation Symétrique, car d'après la Symétrie de l'égalité on a :*

$$\begin{array}{lll} \forall\, x,\ y \in \mathbb{R}, \quad x\mathfrak{R}y & \Longleftrightarrow & x^2 - 1 = y^2 - 1 \\ & \Longleftrightarrow & y^2 - 1 = x^2 - 1 \quad \textit{car l'égalité est symétrique} \\ & \Longleftrightarrow & y\mathfrak{R}x \end{array}$$

donc

$$\forall\, x,\ y \in \mathbb{R}, \qquad x\mathfrak{R}x \Longleftrightarrow y\mathfrak{R}x$$

ce qui montre que $\mathfrak{R}$ *est une relation Symétrique.*

III) $\mathfrak{R}$ *est une relation Transitive, car d'après la Transitivité de l'égalité on a :*

$$\begin{array}{lll} \forall\, x,\ y,\ z \in \mathbb{R}, \quad (x\mathfrak{R}y) \wedge (y\mathfrak{R}z) & \Longrightarrow & (x^2 - 1 = y^2 - 1) \wedge (y^2 - 1 = z^2 - 1) \\ & \Longrightarrow & (x^2 - 1 = z^2 - 1) \quad \textit{car l'égalité est Transitive.} \\ & \Longrightarrow & (x\mathfrak{R}y)\,(x\mathfrak{R}y) \end{array}$$

donc

$$\forall\, x,\ y,\ z \in \mathbb{R}, \qquad (x\mathfrak{R}y) \wedge (y\mathfrak{R}z) \Longrightarrow (x\mathfrak{R}y)$$

ce qui montre que $\mathfrak{R}$ *est une relation Transitive.*
De I) , II) *et* III) *, on déduit que* $\mathfrak{R}$ *est une relation déquivalence.*

2. *Déterminer l'ensemble quotient* $\mathbb{R}_{/\mathfrak{R}}$.
Soit $x \in \mathbb{R}$*, alors :*

$$\begin{array}{lll} \forall\, y \in \mathbb{R}, \qquad x\mathfrak{R}y & \Longleftrightarrow & x^2 - 1 = y^2 - 1 \\ & \Longleftrightarrow & x^2 - y^2 = 0 \\ & \Longleftrightarrow & (x - y)(x + y) = 0 \\ & \Longleftrightarrow & (y = x) \vee (y = -x) \end{array}$$

donc : $\dot{x} = \{x,\ -x\}$*, par suite*

$$\mathbb{R}_{/\mathfrak{R}} = \Big\{\{x,\ -x\},\ x \in \mathbb{R}\Big\}$$

□

Propriété 3.1 *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble non vide E, alors*

$$\forall\ x,\ y \in E,\ (\dot{y} \cap \dot{x} = \emptyset) \vee (\dot{y} = \dot{x})$$

Preuve : Soient $x,\ y \in E$, supposons que $\dot{y} \cap \dot{x} \neq \emptyset$ alors il existe $z \in \dot{y} \cap \dot{x}$, donc $z\mathcal{R}y$ et $z\mathcal{R}x$.
Montrons alors que $\dot{y} = \dot{x}$.
Soit $u \in \dot{x}$, alors

$$\Big((u\mathcal{R}x) \wedge (z\mathcal{R}x)\Big) \wedge (z\mathcal{R}y)$$

comme $\mathcal{R}$ est symétrique et transitive, on déduit que

$$(u\mathcal{R}z) \wedge (z\mathcal{R}y)$$

et de la transitivité de $\mathcal{R}$ on déduit que $u\mathcal{R}y$, par suite $u \in \dot{y}$, ce qui montre que $\dot{x} \subset \dot{y}$.
De la même manière, on montre que $\dot{y} \subset \dot{x}$, ce qui termine la preuve de la propriété.

□

De cette propriété on déduit que :

$$E_{/\mathcal{R}} \textbf{ est une partition de l'ensemble } E.$$

Exemple 3.3 *Soient E et F deux ensembles non vides et $f : E \longrightarrow F$, on définit la relation binaire $\mathcal{R}$ sur E par :*

$$\forall x,\ y \in E, \qquad x\mathcal{R}y \Longleftrightarrow f(x) = f(y)$$

alors $\mathcal{R}$ est une relation d'équivalence sur E.

Preuve :

1. $\mathcal{R}$ est réflexive, car f étant une application alors : $\forall x \in E,\ f(x) = f(x)$, donc

$$\forall x \in E, \qquad x\mathcal{R}x.$$

2. $\mathcal{R}$ est transitive, car pour tous $x,\ y,\ z \in E$ on a :

$$\left.\begin{array}{l} f(x) = f(y) \\ f(y) = f(z) \end{array}\right\} \Longrightarrow f(x) = f(z)$$

ce qui montre que :

$$\forall x,\ y,\ z \in E, \quad \Big((x\mathcal{R}y) \wedge (y\mathcal{R}z)\Big) \Longrightarrow (x\mathcal{R}z).$$

3. $\mathcal{R}$ est symétrique, car pour tous $x,\ y \in E$,

$$f(x) = f(y) \Longrightarrow f(y) = f(x)$$

donc

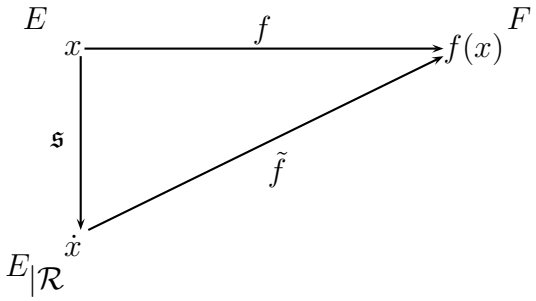
$$\forall x,\ y \in E, \qquad (x\mathcal{R}y) \Longrightarrow (y\mathcal{R}x)$$

ce qui montre que la relation binaire $\mathcal{R}$ est une relation déquivalence. □

3.1.1 Décomposition d'une application

Etant donnée une application $f : E \longrightarrow F$, on note $E_{/\mathcal{R}}$ le quotient de E par la relation $\mathcal{R}$ et pour toute classe $\dot{x}$ on pose $\widetilde{f}(\dot{x}) = f(x)$, alors :

$\widetilde{f}$ est une application de $E_{/\mathcal{R}}$ dans F injective et le diagramme suivant est commutatif.



Décomposition de l'application f.

En effet :

1. Montrer que $\widetilde{f}$ est une application revient à montrer que $\widetilde{f}(\dot{x})$ ne dépend pas du représentant de la classe $\dot{x}$.
Soient $x,\ y \in E$ tels que $\dot{x} = \dot{y}$, alors $x\mathcal{R}y$, donc $f(x) = f(y)$, par suite :

$$\widetilde{f}(\dot{x}) = f(x) = f(y) = \widetilde{f}(\dot{y})$$

donc :

$$\forall\, \dot{x},\ \dot{y} \in E_{/\mathcal{R}}, \qquad (\dot{x} = \dot{y}) \Longrightarrow \left(\widetilde{f}(\dot{x}) = \widetilde{f}(\dot{y})\right)$$

ce qui montre que $\widetilde{f}$ est une application de $E_{/\mathcal{R}}$ dans F.

2. Montrons que $\widetilde{f} : E_{/\mathcal{R}} \longrightarrow F$ est injective.
Soient $\dot{x},\ \dot{y} \in E_{/\mathcal{R}}$, alors

$$\begin{array}{lll} \left(\widetilde{f}(\dot{x}) = \widetilde{f}(\dot{y})\right) & \Longleftrightarrow & f(x) = f(y) \\ & \Longleftrightarrow & x\mathcal{R}y \\ & \Longleftrightarrow & \dot{x} = \dot{y} \qquad \text{d'après la propriété 3.1} \end{array}$$

ce qui montre que $\widetilde{f}$ est injective.

3. Le diagramme est commutatif car :

$$\forall\, x \in E, \qquad f(x) = \widetilde{f}(\dot{x}) = \widetilde{f}(\mathsf{s}(x)) = \widetilde{f} \circ \mathsf{s}(x)$$

donc

$$f = \widetilde{f} \circ \mathsf{s}$$

□

3.2 Relations d'ordre

Définition 3.5 *On dit qu'une relation binaire $\mathcal{R}$ sur E est une relation d'ordre si elle est* **R***éflexive,* **T***ransitive et* **A***nti-Symétrique.*

Dans la littérature, les relations d'ordre sont souvent notées $\preceq$.

Si $x \preceq y$, on dit que x est inférieur ou égal à y ou que y est supérieur ou égal à x. On dit aussi que x est plus petit (ou égal) que y et y est plus grand (ou égal) que x.

Définition 3.6 *Soit $\preceq$ une relation d'ordre sur un ensemble E.*

1. *On dit que deux éléments x et y de E sont comparables si :*

$$x \preceq y \quad ou \quad y \preceq x$$

2. *On dit que $\preceq$ est une relation d'ordre total, ou que E est totalement ordonné par $\preceq$, si tous les éléments de E sont deux à deux comparables. Si non, on dit que la relation $\preceq$ est une relation d'ordre partiel ou que E est partiellement ordonné par $\preceq$.*

Exemple 3.4 *Etant donné E un ensemble non vide, alors*

L'egalité est une relation d'ordre dans E

Il est évident que

Si E n'est pas un singleton, L'egalité est une relation d'ordre partiel dans E

Exemple 3.5 *Soit F un ensemble et $E = \mathcal{P}(F)$. On considère, sur $E = \mathcal{P}(F)$, la relation binaire "$\subset$", alors :*

I) *"$\subset$" est une relation d'ordre sur E.*

1. *"$\subset$" est Réflexive, car pour tout ensemble $A \in \mathcal{P}(A)$, on a $A \subset A$.*
2. *"$\subset$" est Transitive, car pour tous $A,\ B,\ C \in \mathcal{P}(A)$,*

$$\begin{aligned}(A \subset B) \wedge (B \subset C) &\implies \forall x \Big(\big((x \in A) \Longrightarrow (x \in B)\big) \wedge \big((x \in B) \Longrightarrow (x \in C)\big)\Big)\\ &\implies \forall x \Big((x \in A) \Longrightarrow (x \in C)\Big) \quad car \Longrightarrow \text{ est transitive}\\ &\implies (A \subset C).\end{aligned}$$

3. *"$\subset$" est Anti-symétrique, car pour tous $A,\ B \in \mathcal{P}(A)$,*

$$(A \subset B) \wedge (B \subset A) \Longleftrightarrow A = B$$

De 1), 2) et 3) on déduit que "$\subset$" est une relation d'ordre sur E.

II) *L'ordre est-il total ?*

i) *Si $F = \emptyset$, alors $E = \{\emptyset\}$ et on a : $\forall A,\ B \in E,\ A = B = \emptyset$, donc*

$$\forall A,\ B \in E, \qquad A \subset B$$

ce qui montre que l'ordre est Total.

ii) *Si F est un signgleton, alors il existe a tel que $F = \{a\}$ et $E = \Big\{\emptyset, \{a\}\Big\}$, donc pour tous A et B dans E on a*

$$\Big((A = \emptyset) \vee (A = \{a\})\Big) \wedge \Big((B = \emptyset) \vee (B = \{a\})\Big)$$

donc

$$\forall A,\ B \in E, \quad \Big((A \subset B) \vee (B \subset A)\Big)$$

ce qui montre que l'ordre est Total.

iii) *Si F contient au moins deux éléments distincts a et b, alors*

$$\exists A = \{a\},\ B = \{b\} \in E; \qquad (A \not\subset B) \wedge (B \not\subset A)$$

donc A et B ne sont pas comparables, par suite "$\subset$" est une relation d'ordre partiel dans E.

□

3.2.1 Plus petit, Plus grand élément

Définition 3.7 *Soit $(E, \preceq)$ un ensemble ordonné et $A \in \mathcal{P}(E)$.*

1. *On dit que $m \in A$ est le plus petit élément de A si*

$$\forall\ y \in A\ (m \preceq y)$$

2. *On dit que $M \in A$ est le plus grand élément de A si*

$$\forall\ y \in A\ (y \preceq M)$$

Exemple 3.6 *Dans $\mathbb{Z}^*$ on définit la relation $\preceq$ par :*[1]

$$\forall\, n,\ m \in \mathbb{Z}^*, \qquad n \preceq m \Longleftrightarrow \Big(\exists k \in \mathbb{Z};\ m = k.n\Big)$$

I. *Montrer que $\preceq$ est une relation d'ordre.*

I) *$\preceq$ est une relation Reflexive, car :*

$$\forall\, n \in \mathbb{Z}^*,\ \exists k = 1 \in \mathbb{Z}; \quad n = k.n$$

donc

$$\forall\, n \in \mathbb{Z}, \quad n \preceq n$$

ce qui montre que $\preceq$ est une relation Reflexive.

[1] $n \preceq m$ si n divise m.

II) $\preceq$ *est une relation Anti-Symétrique, car :* $\forall\, n,\ m \in \mathbb{Z}^*$,

$$\begin{aligned} & \Big(n \preceq m\Big) \wedge \Big(m \preceq n\Big) \Longleftrightarrow \Big(\exists k_1 \in \mathbb{Z};\ m = k_1.n\Big) \wedge \Big(\exists k_2 \in \mathbb{Z};\ n = k_2.m\Big) \\ \Longrightarrow\ & \Big(\exists k_1 \in \mathbb{Z};\ m = k_1.n\Big) \wedge \Big(\exists k_2 \in \mathbb{Z};\ n = k_2.m\Big) \wedge \Big(m = k_1k_2.m\Big) \\ \Longrightarrow\ & \Big(\exists k_1 \in \mathbb{Z};\ m = k_1.n\Big) \wedge \Big(\exists k_2 \in \mathbb{Z};\ n = k_2.m\Big) \wedge \Big(k_1k_2 = 1, \quad car\ m \neq 0\Big) \\ \Longrightarrow\ & m = n, \quad car\ \ \forall\, k_1,\ k_2 \in \mathbb{Z},\ \ \Big(k_1k_2 = 1 \Longrightarrow k_1 = k_2 = 1\Big) \end{aligned}$$

donc

$$\forall\, n,\ m \in \mathbb{Z}^*, \quad \Big(n \preceq m\Big) \wedge \Big(m \preceq n\Big) \Longrightarrow m = n$$

ce qui montre que $\preceq$ *est Anti-symétrique.*

III) $\preceq$ *est une relation Transitive, car :* $\forall\, n,\ m,\ p \in \mathbb{Z}^*$,

$$\begin{aligned} \Big(n \preceq m\Big) \wedge \Big(m \preceq p\Big) \ &\Longleftrightarrow\ \Big(\exists k_1 \in \mathbb{Z};\ m = k_1.n\Big) \wedge \Big(\exists k_2 \in \mathbb{Z};\ p = k_2.m\Big) \\ &\Longrightarrow\ \Big(\exists k = k_1k_2 \in \mathbb{Z};\ p = k.n\Big) \\ &\Longrightarrow\ n \preceq p \end{aligned}$$

ce qui montre que $\preceq$ *est Transitive.*
De I) , II) *et* III) *, on déduit que* $\preceq$ *est une relation d'ordre.*

II. *L'ordre est-il Total ?*
L'ordre est partiel, car si on considére $n = 2$ *et* $m = 3$*, alors* n *et* m *ne sont pas comparables.*

III. *Pour cette relation d'ordre,* $\mathbb{Z}^*$ *a-t-il un plus petit élément ou un plus grand élément ?*

I) *Il est clair que* 1 *est le plus petit élément de* $\mathbb{Z}*$*, car*

$$\forall\, n \in \mathbb{Z}^*,\ \exists k = n \in \mathbb{Z}; \quad n = k.1$$

donc

$$\forall\, n \in \mathbb{Z}^*, \quad 1 \preceq n$$

II) $\mathbb{Z}^*$ *n'a pas de plus grand élément, car :*

$$\forall\, n \in \mathbb{Z}^*,\ \exists m = 2.n \in \mathbb{Z}^*; \quad n \preceq m$$

V. *Soient* $A = \Big\{-20,\ -18,\ -14,\ -10,\ -6,\ 2\Big\}$ *et* $B = \Big\{-42,\ 2,\ 3,\ 6,\ 7\Big\}$*, donner le plus petit et le plus grand élément respectivement de* A *et de* B *s'ils existent.*

a) 2 *est le plus petit élément de* A*, car il divise tous les autres éléments de* A*, donc :*

$$\forall\, n \in A, \quad 2 \preceq n$$

b) A *n'a pas de plus grand élément, car il n'y a pas dans* A *un élément qui est divisible par tous les autres éléments de* A*.*

c) *B n'a pas de plus petit élément, car il n'y a pas dans A un élément qui divise tous les autres éléments de A.*

d) *-42 est le plus grand élément de B, car tous les éléments de B divisent -42, donc*

$$\forall\, n \in B, \quad n \preceq -42.$$

V. *Pour cette relation d'ordre, $\mathbb{Z}^*\backslash\{1\}$ a-t-il un plus petit élément ?*

$\mathbb{Z}^*\backslash\{1\}$ n'a pas de plus petit élément, car pour tout $n \in \mathbb{Z}^*\backslash\{1\}$:

- Si n est pair alors il n'est pas divisible par les nombres impairs différents de 1, donc il n'est pas plus petit que ces nombres, par suite n n'est pas le plus petit élément de $\mathbb{Z}^*\backslash\{1\}$.
- Si n est impair alors il n'est pas divisible par les nombres pairs, donc il n'est pas plus petit que ces nombres, par suite n n'est pas le plus petit élément de $\mathbb{Z}^*\backslash\{1\}$,

ce qui montre que $\mathbb{Z}^*\backslash\{1\}$ n'admet pas de plus petit élément par rapport à cette relation d'ordre $\preceq$.

□

Propriété 3.2 *Soit $(E, \preceq)$ un ensemble ordonné et $A \in \mathcal{P}(A)$ alors si A possède un plus petit ou un plus grand élément, il est unique.*

Preuve : Soient m et m' deux éléments de A, alors :

$$\left.\begin{array}{l} \wedge \quad (m \text{ plus petit élément de } A) \\ \qquad\quad (m' \text{ plus petit élément de } A) \end{array}\right\} \Longrightarrow \left\{\begin{array}{ll} & m \preceq m' \\ \wedge & \\ & m \preceq m' \end{array}\right. \overset{\text{"Anti-symetrie"}}{\Longrightarrow} m = m'$$

d'où l'unicité du plus petit élément de A, s'il existe.

Le même type de raisonnement nous montre l'unicité du plus grand élément de A, s'il existe.

□

3.2.2 Eléments Minimaux et éléments maximaux

Définition 3.8 *Soit $(E, \preceq)$ un ensemble ordonné et $A \in \mathcal{P}(E)$.*

1. *On dit qu'un élément $m \in A$ est un élément minimal dans A s'il n'y a pas dans A un élément plus petit que lui. Ceci est formellement équivalent à :*

$$\forall\ y \in A\ (y \preceq m \Longrightarrow y = m)$$

2. *On dit qu'un élément $M \in A$ est un élément maximal dans A s'il n'y a pas dans A un élément plus grand que lui. Ceci est formellement équivalent à :*

$$\forall\ y \in A\ (M \preceq y \Longrightarrow y = M)$$

Exemple 3.7 *On reprend la relation inclusion et*

$$A = \{\{1,2,3\},\{0,4\},\{1,3,5\},\{1,5\},\{1,3\},\{5,3\},\{0,5,6,7\}\},$$

alors

1. *Les éléments minimaux de A sont :* $\{0,4\}$, $\{1,5\}$, $\{1,3\}$, $\{5,3\}$ *et* $\{0,5,6,7\}$
2. *Les éléments maximaux de A sont :* $\{0,4\}$, $\{1,2,3\}$, $\{1,3,5\}$ *et* $\{0,5,6,7\}$.
3. *A n'a pas de plus petit élément.*
4. *A n'a pas de plus grand élément.*

□

Propriété 3.3 *Soit* $(E,\preceq)$ *un ensemble ordonné et* $m,\ M \in E$, *alors*

1. *m plus petit élément de* $A \Longrightarrow$ *m est le seul élément minimal dans A.*

2. *M plus grand élément de* $A \Longrightarrow$ *M est le seul élément maximal dans A.*

Preuve : Immédiate.

PROBLEME : A-t-on les réciproques de ces propriétés ?

3.2.3 Borne Inférieure, Borne Supérieure

Définition 3.9 *Soit* $(E,\preceq)$ *un ensemble ordonné, A une partie de E.*

- *On appelle minorant de l'ensemble A, tout élément* $m \in E$ *tel que*

$$\forall\ x \in A, \quad m \preceq x$$

- *On appelle majorant de l'ensemble A, tout élément* $M \in E$ *tel que*

$$\forall\ x \in A, \quad x \preceq M$$

- *Le plus grand des minorants, s'il existe, est appelé Borne inférieure de A et noté* $\inf A$.
- *Le plus petit des majorants, s'il existe, est appelé Borne supérieure de A et noté* $\sup A$.
- *Si A possède un minorant, on dit que A est Minoré,*
- *Si A possède un majorrant, on dit que A est Majoré,*
- *Si A possède un minorant et un majorrant, on dit que A est Borné.*

Remarque 3.1

1. *Le plus petit (respectivement le plus grand) élément de A, s'il existe, est un minorant (respectivement un majorant) de A. Par contre, un minorant (respectivement un majorant) de A peut ne pas être le plus petit (respectivement le plus grand) élément de A, car il n'est pas nécessairement dans A.*
2. *Si la borne inférieure ou la borne supérieure d'un ensemble A existe, alors elle est unique.*

3. *Si E est totalement ordonné par $\preceq$, alors tout sous ensemble fini A de E admet un plus petit éléments et un plus grand élément.*

Exemple 3.8 *Soient $F = \{1, a, 2, 5, \gamma\}$, l'ensemble $E = \mathcal{P}(F)$ ordonné par la relation $\subset$ et une partie $A = \Big\{\{a, 2\}, \{2, 5, \gamma\}, \{1, 2, \gamma\}, \{a, 2, 5\}, \Big\}$, alors :*

1. *Les mimorants de A sont : $\emptyset$ et $\{a\}$.*
2. $\mathrm{Inf}A = \{a\}$.
3. *A n'a pas de plus petit élément, car* $\mathrm{Inf}A \notin A$.
4. *Le seul majorant de A est : $F = \{1, a, 2, 5, \gamma\}$.*
5. $\mathrm{Sup}A = F$.
6. *A n'a pas de plus grand élément, car* $\mathrm{Sup}A \notin A$.

Proposition 3.1 *Soient $(E, \preceq)$ un ensemble totalement ordonné[2] et A et B deux sous ensembles de E dont les bornes inférieures et supérieures existent, alors :*

- $\sup(A \cup B) = \max\{\sup A, \sup B\}$
- $\inf(A \cup B) = \min\{\inf A, \inf B\}$
- $\sup(A \cap B) \preceq \min\{\sup A, \sup B\}$
- $\max\{\inf A, \inf B\} \preceq \inf(A \cap B)$

Preuve : Soient $M = \max\{\sup A, \sup B\}$ et $m = \min\{\inf A, \inf B\}$, alors :

$$\begin{array}{rcl} \forall x(x \in A \cup B & \Longrightarrow & (x \in A) \vee (x \in B)) \\ & \Longrightarrow & (x \preceq \sup A) \vee (x \preceq \sup B) \\ & \Longrightarrow & (x \preceq M) \vee (x \preceq M) \\ & \Longrightarrow & (x \preceq M) \end{array}$$

ce qui montre que M est un majorant de $A \cup B$.
Montrons que M est le plus petit des majorants de $A \cup B$. Soit M' un majorant de $A \cup B$, il est évident que M' est alors un majorant de A et de B, donc

$$(\sup A \preceq M') \wedge (\sup B \preceq M')$$

par suite

$$\max\{\sup A, \sup B\} \preceq M'$$

d'où on déduit que : $M = \sup(A \cup B)$.

La preuve des autres propriétés est similaire.

□

Remarque 3.2 *La seule relation d'ordre et d'équivalence, à la fois, est la relation égalité.*

[2]On a supposé que l'ordre est total pour assurer l'existence de $\max\{\sup A, \sup B\}$, $\min\{\sup A, \sup B\}$, $\max\{\inf A, \inf B\}$ et de $\min\{\inf A, \inf B\}$.

Chapitre 4

STRUCTURES ALGEBRIQUES

4.1 Lois de Compositions Internes

Définition 4.1 *On appelle loi de composition interne (l.c.i) sur un ensemble E, toute application $\star : E \times E \longrightarrow E$.*
Un sous ensemble F de E est dit stable par rapport à la loi $\star$ si :

$$\forall\ a,\ b \in F, \quad a \star b \in F$$

Exemple 4.1 *Soit A un ensemble et $E = \mathcal{P}(A)$, alors l'intersection et la réunion d'ensembles sont deux lois de compositions internes dans E car : $\forall\, X,\ Y \in \mathcal{P}(A)$,*

1. $X \cap Y \subset X \subset A$
et on a

$$\forall\, x, \quad x \in X \cup Y \Longrightarrow \Big(x \in X\Big) \vee \Big(x \in Y\Big) \Longrightarrow \Big(x \in A\Big) \vee \Big(x \in A\Big) \Longrightarrow \Big(x \in A\Big)$$

donc
2. $X \cup Y \subset A$,
ce qui montre que "$\bigcap$" et "$\bigcup$" sont des lois de compositions internes dans $\mathcal{P}(A)$.

□

Exemple 4.2 *Soit $F = \Big\{\{a,b\},\ \{a,c\},\{b,c\}\Big\} \subset \mathcal{P}\Big(\{a,b,c\}\Big)$, alors F n'est pas stable par rapport à l'intersection et la réunion, car :*

$$\begin{array}{ll} \exists X = \{a,b\},\ Y = \{a,c\} \in F; & X \cap Y = \{a\} \notin F \\ \exists X = \{a,b\},\ Y = \{a,c\} \in F; & X \cup Y = \{a,b,c\} \notin F \end{array}$$

□

Définition 4.2 *Soient $\star$ et $\bullet$ deux lois de composition internes sur E, on dit que :*

1. *$\star$ est commutative si : $\forall\ a,\ b \in E,\ a \star b = b \star a$*

2. *$\star$ est associative si : $\forall\ a,\ b,\ c \in E,\ (a \star b) \star c = a \star (b \star c)$,*

3. $\star$ *est distributive par rapport à* $\bullet$ *si :* $\quad \forall\ a,\ b,\ c \in E,$

$$a \star (b \bullet c) = (a \star b) \bullet (a \star c) \text{ et } (b \bullet c) \star a = (b \star a) \bullet (c \star a)$$

4. $e \in E$ *est un élément neutre à gauche (respectivement à droite) de la loi* $\star$ *si*

$$\forall\ a \in E, \quad e \star a = a \quad (\text{respectivement } a \star e = a\ )$$

Si e *est un élément neutre à droite et à gauche de* $\star$ *on dit que* e *est un élément neutre de* $\star$.

Exemple 4.3 *Soit* F *un ensemble et* $E = \mathcal{P}(F)$. *On considère sur* E *les lois de composition internes " $\cap$" et " $\cup$", alors il est très facile de montrer que :*

- *" $\cap$" et " $\cup$" sont associatives*
- *" $\cap$" et " $\cup$" sont commutatives*
- $\emptyset$ *est l'élément neutre de* $\cup$
- F *est l'élément neutre de* $\cap$

□

et on a :

Propriété 4.1 $\cap$ *est distributive par rapport à* $\cup$ *et* $\cup$ *est distributive par rapport à* $\cap$

Preuve. Soient $A,\ B, C$ trois éléments de $E = \mathcal{P}(F)$, alors pour tout x, on a :

$$\begin{array}{rcl} x \in A \cap (B \cup C) & \iff & (x \in A) \wedge (x \in B \cup C) \\ & \iff & (x \in A) \wedge \Big((x \in B) \vee (x \in C)\Big) \\ & \iff & \Big((x \in A) \wedge (x \in B)\Big) \vee \Big((x \in A) \wedge (x \in C)\Big) \\ & \iff & (x \in A \cap B) \vee (x \in A \cap C) \\ & \iff & x \in (A \cap B) \cup (A \cap C) \end{array}$$

ce qui montre que :

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

et comme $\cap$ est commutative, on déduit que $\cap$ est distributive par rapport à $\cup$.

De la même manière on montre la distributivité de $\cup$ par rapport à $\cap$.

□

Propriété 4.2 *Si une loi de composition interne* $\star$ *possède un élément neutre à droite* e' *et un élément neutre à gauche* e'', *alors* $e' = e''$ *et c'est un élément neutre de* $\star$.

Preuve. Soit e', respectivement e'', un élément neutre à droite, respectivement à gauche, de $\star$, alors

$$\begin{array}{ll} e' = e'' \star e' & \text{car } e'' \text{ élément neutre à gauche de } \star \\ e'' = e'' \star e' & \text{car } e' \text{ élément neutre à droite de } \star \end{array}$$

ce qui montre que $e' = e''$.

□

Remarque 4.1 *D'après cette dernière propriété, si $\star$ possède un élément neutre, alors il est unique.*

Définition 4.3 *Soit $\star$ une loi de composition interne sur un ensemble E admettant un élément neutre e. On dit qu'un élément $a \in E$ est inversible, ou symetrisable, à droite (respectivement à gauche) de $\star$ si*

$$\exists\ a' \in E, \quad a \star a' = e \quad (respectivement \quad a' \star a = e)$$

et a' est dit un inverse (ou un symétrique) à droite (respectivement à gauche) de a.
S'il existe $a' \in E$ tel que

$$a' \star a = a \star a' = e$$

on dit que a est inversible (ou symetrisable) et a' est dit un inverse (ou un symétrique) de a par rapport à $\star$.

Remarque 4.2
- *a est inversible (ou symetrisable) s'il est inversible à droite et à gauche de $\star$.*
- *Le symétrique d'un élément n'est pas toujours unique*

Exemple 4.4 *Soit $E = \{a, b, \gamma\}$, on définit une l.c.i dans E par :*

$\star$	a	b	γ
a	a	b	γ
b	b	γ	a
γ	γ	a	a

c'est à dire

$$\begin{cases} \textbf{1.} & a \star a = a, & a \star b = b, & a \star \gamma = \gamma \\ \textbf{2.} & b \star a = b, & b \star b = \gamma, & b \star \gamma = a \\ \textbf{3.} & \gamma \star a = \gamma, & \gamma \star b = a, & \gamma \star \gamma = a \end{cases}$$

On remarque que :

I. *a est l'élément neutre de $\star$.*

II. *Tous les éléments de E sont inversibles avec :*
- I) *a est l'inverse de a,*
- II) *γ est l'inverse de b*
- III) *b et γ sont des inverses de γ.*

Propriété 4.3 *Soit $\star$ une loi de composition interne dans un ensemble E admettant un élément neutre* e*, alors :*

1. *e est inversible (ou symétrisable) et son unique inverse (ou symétrique) est e.*

2. *Soit a un élément de E inversible (ou symétrisable) par rapport à la loi $\star$ et a' un inverse (ou un symétrique) de a, alors a' est inversible (ou symétrisable) et a est un inverse (ou un symétrique) de a'.*

Preuve.

1. Soit $x' \in E$, alors

$$\Big(x' \text{ est un inverse (ou un symétrique) de } e\Big) \Longleftrightarrow \Big(e \star x' = x' \star e = e\Big) \Longleftrightarrow \Big(x' = e\Big)$$

ce qui montre que le seul inverse (ou symétrique) de e est e lui même.

2. Soit $a \in E$ un élément inversible (ou symétrisable) par rapport à la loi $\star$ et soit $a' \in E$ un unverse (ou un symétrique) de a, alors

$$a \star a' = a' \star a = e$$

d'où on déduit que a' est inversible (ou sysmétrisable) par rapport à la loi $\star$ et que a est un inverse (ou un symétrique) de a'.

□

4.1.1 Unicité de l'inverse (du symétrique)

Propriété 4.4 *Soit $\star$ une loi de composition interne dans E, associative et admettant un élément neutre e. Si un élément $x \in E$ admet x_1 un inverse (ou symétrique) à droite et x_2 un inverse (ou symétrique) à gauche, alors x_1 et x_2 sont identiques.*

Preuve. Soient x_1 un inverse (ou un symétrique) à droite de x et x_2 un inverse (ou un symétrique) à gauche de x, alors

$$x \star x_1 = e \quad et \quad x_2 \star x = e$$

donc

$$\begin{array}{rcll} x_1 & = & e \star x_1 & \\ & = & (x_2 \star x) \star x_1 & \\ & = & x_2 \star (x \star x_1) & \text{car } \star \text{ est associative} \\ & = & x_2 \star e & \\ & = & x_2 & \end{array}$$

□

Remarque 4.3

- *De cette propriété on déduit que l'associativité de la loi assure l'unicité du symétrique d'un élément s'il existe*
- *D'après cette propriété on déduit que la loi définie dans l'exemple 4.4 n'est pas associative. Pour s'en convaincre, on remarque que :*

$$(b \star b) \star \gamma = \gamma \star \gamma = a \quad et \quad b \star (b \star \gamma) = b \star a = b$$

donc

$$(b \star b) \star \gamma \neq b \star (b \star \gamma)$$

ce qui montre que la loi $\star$ n'est pas associative.

Conventions : Etant donnée une loi de composition interne associative dans un ensemble E,
- Si la loi est notée $+$, son élément neutre est noté 0_E ou 0, et on parle du symétrique de a qu'on note $a' = -a$.
- Si la loi est notée multiplicativement, son élément neutre est noté 1_E ou 1, et on parle de l'inverse de a qu'on note $a' = a^{-1}$.

Avec ces conventions, si e est l'élément neutre d'une loi de composition interne $\star$ dans un ensemble E, alors

$$\boxed{e^{-1} = e \qquad (\text{ou } -e = e)}$$

et on a : $\forall\, a,\ a' \in E$,

$$\boxed{\Big(a' = a^{-1} \Longleftrightarrow a' \star a = a \star a' = e\Big) \quad ou \quad \Big(a' = -a \Longleftrightarrow a' + a = a + a' = e\Big)}$$

Propriété 4.5 *Soit $\star$ une loi de composition interne dans un ensemble E, associative et admettant un élément neutre* e*, alors si a et b sont deux éléments inversibles (symétrisables) il en sera de même de $(a \star b)$ et on a :*

$$\boxed{(a \star b)^{-1} = b^{-1} \star a^{-1}}$$

Preuves : Soient $a,\ b \in E$ deux éléments inversibles, alors

$$\begin{array}{rcll} (a \star b) \star (b^{-1} \star a^{-1}) & = & (a \star (b \star b^{-1})) \star a^{-1} & (\text{car } \star \text{ est associative.}) \\ & = & (a \star e) \star a^{-1} & \\ & = & a \star a^{-1} & \\ & = & e & \end{array}$$

De la même manière on montre que

$$(b^{-1} \star a^{-1}) \star (a \star b) = e$$

d'où on déduit que $(a \star b)$ est inversible et que

$$(a \star b)^{-1} = b^{-1} \star a^{-1}$$

□

Définition 4.4 *Soit $\star$ une loi de composition interne dans un nesemble E. On dit qu'un élément $r \in E$ est régulier à droite (respectivement à gauche) de $\star$ si*

$$\forall b,\ c \in E, \quad b \star r = c \star r \Longrightarrow b = c$$

$$\Big(respectivement\ \ \forall b,\ c \in E, \quad r \star b = r \star c \Longrightarrow b = c\Big)$$

Si r est un élement régulier à droite et à gauche de $\star$, on dit que r est un élément régulier de $\star$ dans E.

Exemple 4.5 *Soient F un ensemble et $E = \mathcal{P}(F)$, alors $\emptyset$ est une élément régulier pour la réunion dans E et F est un élément régulier pour l'intersection dans E.*

Propriété 4.6 *Soit $\star$ une loi de composition interne associative admettant un élément neutre e dans E, alors tout élément symétrisable dans $(E, \star)$ est régulier.*

Preuve. Soit $x \in E$ un élément symétrisable dans E, alors x^{-1} existe et pour tous a et b dans E, on a :

$$\begin{array}{rcl} a \star x = b \star x & \Longrightarrow & (a \star x) \star x^{-1} = (b \star x) \star x^{-1} \\ & \Longrightarrow & a \star (x \star x^{-1}) = b \star (x \star x^{-1}) \quad \text{car } \star \text{ est associative} \\ & \Longrightarrow & a \star e = b \star e \\ & \Longrightarrow & a = b \end{array}$$

Ce qui montre que x est régulier à droite de $\star$.
De la même manière on montre que x est régulier à gauche de $\star$.

□

Remarque 4.4 *Si x est symétrisable à droite, respectivement à gauche, alors x est régulier à droite, respectivement à gauche de $\star$.*

4.2 Structure de Groupe

Définition 4.5 *On appelle groupe, tout ensemble non vide G muni d'un loi de composition interne $\star$ tel que :*

1. *$\star$ est associative ;*
2. *$\star$ possède un élément neutre e ;*
3. *Tout élément de E est symetrisable.*

Si de plus $\star$ est commutative, on dit que $(G, \star)$ est un groupe commutatif, ou groupe Abélien[1]

Exemple 4.6 *Un exemple illustratif de groupe abélien est $(\mathbb{Z}, +)$.*

Exemple 4.7 *On définit l'opération $\star$ par :*

$$\forall\, x,\ y \in]-1, 1[, \quad x \star y = \frac{x + y}{1 + xy}$$

Montrer que $\Big(]-1, 1[, \star\Big)$ est un groupe abélien.

1) *$\star$ est une loi de composition interne dans $]-1, 1[$.*
Soient $x,\ y \in]-1, 1[$, alors

$$\Big(|x| < 1\Big) \wedge \Big(|y| < 1\Big)$$

[1] **ABEL Niels Henrik** : Mathématicien norvégien (île de Finnøy 1802-Arendal 1829). Algébriste, il créa la théorie des fonctions elliptiques. Il est mort de tuberculose.

donc

$$\Big(|xy| = |x|\,|y| < 1\Big)$$

par suite

$$1 + xy > 1 - |xy| > 0$$

Ainsi

$$\begin{array}{rcl}
\forall\, x,\ y \in]-1,1[, \quad \left|\dfrac{x+y}{1+xy}\right| < 1 & \Longleftrightarrow & \dfrac{|x+y|}{|1+xy|} < 1 \\
& \Longleftrightarrow & |x+y| < |1+xy| \\
& \Longleftrightarrow & |x+y| < 1+xy \quad car \ \ 1+xy > 0 \\
& \Longleftrightarrow & -(1+xy) < x+y < 1+xy \\
& \Longleftrightarrow & \begin{cases} x+y-1-xy < 0 \\ x+y+1+xy > 0 \end{cases} \\
& \Longleftrightarrow & \begin{cases} x(1-y)+y-1 < 0 \\ x(1+y)+y+1 > 0 \end{cases} \\
& \Longleftrightarrow & (*) \begin{cases} (1-y)(x-1) < 0 \\ (1+y)(x+1) > 0 \end{cases}
\end{array}$$

comme $-1 < x,\ y < 1$, *alors*

$$\Big(1-y>0\Big) \wedge \Big(x-1<0\Big) \qquad et \qquad \Big(1+y>0\Big) \wedge \Big(x+1>0\Big)$$

donc

$$\Big(\,(1-y)(x-1)<0\,\Big) \wedge \Big(\,(1+y)(x+1)>0\Big),$$

d'où on déduit que $(*)$ *est vraie pour tous* $x,\ y \in]-1,1[$, *par suite :*

$$\forall\, x,\ y \in]-1,1[, \qquad |x \star y| = \left|\frac{x+y}{1+xy}\right| < 1$$

ce qui montre que $\star$ *est une loi de composition interne dans* $]-1,1[$.

2) $\star$ *est commutative.*
D'après la commutativité de l'addition et de la multiplication dans $\mathbb{R}$ *on a :*

$$\forall\, x,\ y \in]-1,1[, \qquad x \star y = \frac{x+y}{1+xy} = \frac{y+x}{1+yx} = y \star x$$

ce qui montre que $\star$ *est commutative.*

3) $\star$ *est associative.*

Soient $x,\ y,\ z \in]-1,1[$, *alors*

$$\begin{aligned}(x\star y)\star z &= \frac{(x\star y)+z}{1+(x\star y)z} = \frac{\dfrac{x+y}{1+xy}+z}{1+x\dfrac{x+y}{1+xy}z}\\ &= \frac{\dfrac{(x+y)+z(1+xy)}{1+xy}}{\dfrac{(1+xy)+(x+y)z}{1+xy}} = \frac{(x+y)+z(1+xy)}{(1+xy)+(x+y)z}\\ &= \frac{x+y+z+xyz}{1+xy+xz+yz}\end{aligned}$$

et on a :

$$\begin{aligned}x\star(y\star z) &= \frac{x+(y\star z)}{1+x(y\star z)} = \frac{x+\dfrac{y+z}{1+yz}}{1+x\dfrac{y+z}{1+yz}}\\ &= \frac{\dfrac{x(1+yz)+(y+z)}{1+yz}}{\dfrac{(1+yz)+x(y+z)}{1+yz}} = \frac{x(1+yz)+(y+z)}{(1+yz)+x(y+z)}\\ &= \frac{(x+xyz)+(y+z)}{(1+yz)+(xy+xz)} = \frac{x+y+z+xyz}{1+xy+xz+yz}\end{aligned}$$

en comparant les deux expressions on obtient :

$$\forall\, x,\ y,\ z \in]-1,1[, \qquad (x\star y)\star z = x\star(y\star z)$$

d'où on déduit que $\star$ *est associative.*

4) $\star$ *admet un élément neutre.*
Soit $e \in \mathbb{R}$, *alors*

$$\Big(e \text{ élément neutre de } \star\Big) \Longleftrightarrow \Big(\forall\, x \in]-1,1[, \quad e\star x = x\star e = x\Big)$$

comme $\star$ *est commutative et*

$$\begin{aligned}x\star e = x &\Longleftrightarrow \frac{x+e}{1+xe} = x\\ &\Longleftrightarrow x+e = x+x^2e\\ &\Longleftrightarrow e = x^2e\\ &\Longleftrightarrow e(1-x^2) = 0\\ &\Longleftrightarrow \Big(e=0\Big)\vee(x=\mp 1)\end{aligned}$$

on déduit que $e = 0 \in]-1,1[$ *est l'élément neutre de* $\star$.

5) *Tout élément de* $]-1,1[$ *est symétrisable.*
Soient $x \in]-1,1[$ *et* $x \in \mathbb{R}$*, alors*

$$\begin{array}{rcl} x \star x' = e & \Longleftrightarrow & \dfrac{x+x'}{1+xx'} = 0 \\ & \Longleftrightarrow & x + x' = 0 \\ & \Longleftrightarrow & x' = -x \end{array}$$

comme $\star$ *est commutative on déduit que tout élément* $x \in]-1,1[$ *est symétrisable et son symétrique est* $x' = -x \in]-1,1[$.

De **1)**, **2)**, **3)**, **4)** *et* **5)** *on déduit que* $\Big(]-1,1[, \star\Big)$ *est un groupe abélien.*

□

4.2.1 Groupes à deux éléments

Soit $G = \{a, b\}$ un ensemble à deux éléments, définir toutes les lois de composition internes dans G qui lui confèrent une structure de groupe.

Soit $\star$ une loi de composition sur G, alors pour que $(G, \star)$ soit un groupe il faut que $\star$ soit interne dans G et admette un élément neutre qui peut être a ou b, donc $\star$ doit être définie de la sorte :

1. Si a est l'élément neutre de $\star$, alors
- $a \star a = a$
- $a \star b = b$
- $b \star a = b$

reste à définir $b \star b$, or pour que $(G, \star)$ soit un groupe il faut que tout élément soit inversible, en particulier il faut trouver b^{-1}. Si on pose $b \star b = b$, alors on remarque que

$$\forall x \in G, \qquad b \star x \neq a$$

donc b ne sera pas inversible, ce qui nous amène à poser
- $b \star b = a$

Ainsi, on a défini une l.c.i. dans G avec un élément neutre a, reste à voir si la loi ainsi définie est associative. On a :
- $(a \star a) \star a = a \star a = a \star (a \star a)$
- $(a \star a) \star b = a \star b = a \star (a \star b)$
- $(a \star b) \star a = b \star a = a \star b = a \star (b \star a)$
- $(a \star b) \star b = b \star b = a = a \star a = a \star (b \star b)$

En remarquant que la loi est commutative on déduit que
- $(b \star a) \star a = b \star (a \star a)$
- $(b \star a) \star b = b \star (a \star b)$

ce qui montre que

$$\forall\, x,\ y,\ z \in G, \quad x \star (y \star z) = (x \star y) \star z$$

donc $\star$ est associative dans G, et par suite $(G, \star)$ est un groupe.

2. Si b est l'élément neutre de $\star$, alors de la même manière on construit la loi $\star$ comme suit :

- $b \star b = b$
- $b \star a = a$
- $a \star b = a$
- $a \star a = b$

D'après ce qui précède : Il existe deux groupes à deux éléments et formellement on les définit ainsi :

$\star$	a	b
a	a	b
b	b	a

et

$\star$	a	b
a	b	a
b	a	b

□

4.2.2 Sous groupes

Définition 4.6 *Soit $(G, \star)$ un groupe, on appelle sous groupe de $(G, \star)$ tout sous ensemble non vide G' de G tel que la restriction de $\star$ à G' en fait un groupe.*

Comme $\star$ est associative dans G alors sa restriction à G' est aussi associative, par suite $G' \neq \emptyset$ est un sous groupe de $(G, \star)$ s'il est stable par rapport à $\star$ et à l'opération inversion, c'est à dire :

$$\begin{cases} (i) & G' \neq \emptyset \\ (ii) & \forall\, a,\ b \in G', \quad a \star b \in G' \\ (iii) & \forall\, a \in G', \quad a^{-1} \in G' \end{cases}$$

Il est claire que si $(G, \star)$ est un groupe, alors G est un sous groupe de G.

Propriété 4.7 *Soient $(G, \star)$ un groupe et $G' \subset G$, alors*

$$G' \text{ est un sous groupe de } G' \Longleftrightarrow \begin{cases} G' \neq \emptyset, \\ \forall\ a,\ b \in G', \quad a \star b^{-1} \in G' \end{cases}$$

Preuve :

1. Soit G' un sous groupe de $(G, \star)$, alors :

i) $\star$ a un élément neutre dans G', donc $G' \neq \emptyset$.

ii) Soient $a,\ b \in G'$, comme G' muni de la restriction de $\star$ est un groupe alors b^{-1} existe dans G' et comme G' est stable par rapport à $\star$ on déduit que $a \star b^{-1} \in G'$.

2. Inversement, soit G' un sous ensemble de G tel que $\begin{cases} G' \neq \emptyset, \\ \forall\ a,\ b \in G', \quad a \star b^{-1} \in G' \end{cases}$

Montrons que G' muni de la restriction de $\star$ est un groupe.

i) Comme $G' \neq \emptyset$ alors il existe $a \in G'$ et d'après la deuxième hypothèse

$$e = a \star a^{-1} \in G',$$

ce qui montre que *la restriction de $\star$ admet un élément neutre e dans G'.*

ii) Soit $x \in G'$, comme $e \in G'$ alors d'après la deuxième hypothèse on aura

$$x^{-1} = e \star x^{-1} \in G'$$

ce qui montre que tout élément x de G' est inversible dans G' par rapport à la restriction de $\star$ à G'.

iii) La restriction de $\star$ à G' est une loi de composition interne, car pour tous x et y dans G', d'après ii) on a

$$y^{-1} \in G'$$

et en utilisant la deuxième hypothèse on déduit que

$$x \star y = x \star (y^{-1})^{-1} \in G'$$

iv) La restriction de $\star$ à G' est associative, car $\star$ est associative dans G.

□

Remarque 4.5 *D'après* i) *de la preuve de la proposition précédente, on voit que : Si e est l'élément neutre d'un groupe $(G, \star)$, alors tout sous groupe de G contient e et on déduit la propriété suivante.*

Propriété 4.8 *Soient $(G, \star)$ un groupe, e l'élément neutre de $\star$ et G' un sous ensemble de G, alors G' est un sous groupe de G si et seulement si :* $\begin{cases} e \in G' \\ \forall\, x,\ y \in G', \quad x \star y^{-1} \in G'. \end{cases}$

Exemple 4.8 *Soit $(G, \star)$ un groupe et $G' = \{x \in G; \quad (\forall y \in G,\ x \star y = y \star x)\}$, alors G' est un sous groupe de G.*

En effet,

i) Si e est l'élément neutre de $\star$, alors $e \in G'$ car :

$$\forall y \in G, \qquad e \star y = y \star e = y$$

ii) Soient $x,\ y \in G'$, alors

$$\begin{array}{lrcll} \forall z \in G, & (x \star y^{-1}) \star z & = & (x \star y^{-1}) \star (z^{-1})^{-1} & \\ & & = & x \star (y^{-1} \star (z^{-1})^{-1}) & car \star \text{ est associative} \\ & & = & x \star (z^{-1} \star y)^{-1} & \\ & & = & x \star (y \star z^{-1})^{-1} & car\ y \in G' \\ & & = & x \star ((z^{-1})^{-1} \star y^{-1}) & \\ & & = & x \star (z \star y^{-1}) & \\ & & = & (x \star z) \star y^{-1} & car \star \text{ est associative} \\ & & = & (z \star x) \star y^{-1} & car\ x \in G' \\ & & = & z \star (x \star y^{-1}) & car \star \text{ est associative} \end{array}$$

ce qui montre que $x \star y^{-1} \in G'$.

De i) et ii) on déduit que G' est un sous groupe de G.

□

Remarque 4.6 *Sachant que si e est l'élément neutre d'un groupe $(G,\star)$, alors il commute avec tous les éléments de G, de l'exemple précédent on déduit que si e est l'élément neutre d'un groupe $(G,\star)$, alors :*

$$\{e\} \text{ est un sous groupe de } G.$$

Définition 4.7 *Soit $(G,\star)$ un groupe, on dit que G' est un sous groupe propre de G si $G' \neq \{e\}$ et $G' \neq G$.*

Exemple 4.9 *Soit $n \in \mathbb{N}$, alors $n\mathbb{Z} = \{n.p\,;\quad p \in \mathbb{Z}\}$ est un sous groupe de $\mathbb{Z}$.*
En effet :

i) $0 \in n\mathbb{Z}$, *car :* $\exists p = 0 \in \mathbb{Z}$; $\quad 0 = n.p$.

ii) Soient $x,\ y \in n\mathbb{Z}$, alors il existe $p_1,\ p_2 \in \mathbb{Z}$ tels que $x = n.p_1$ et $y = n.p_2$, donc

$$x - y = n.p_1 - n.p_2 = n.(p_1 - p_2) = n.p \in n\mathbb{Z}$$

par suite

$$\forall\, x,\ y \in n\mathbb{Z}, \qquad x - y \in n\mathbb{Z}$$

De i) et ii) on déduit que $n\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$.

Pour $n \in \mathbb{N}\backslash\{0,1\}$, $n\mathbb{Z}$ est un sous groupe propre de $\mathbb{Z}$.

□

4.2.3 Goupes Quotients

Soient $(G,\star)$ un groupe et G' un sous groupe de G. On définit une relation binaire $\mathcal{R}$ sur G par :

$$\forall\ a,\ b \in G, \quad a\mathcal{R}b \Longleftrightarrow a \star b^{-1} \in G'$$

Propriété 4.9 *$\mathcal{R}$ est une relation d'équivalence sur G.*

Preuve :
i) $\mathcal{R}$ est Reflexive, car : $\forall x \in G$, comme G' est un sous groupe de G, alors $x\star x^{-1} = e \in G'$, donc

$$\forall\, x \in G, \quad x\mathcal{R}x$$

ii) $\mathcal{R}$ est Symétrique, car : $\forall\, x,\ y \in G$,

$$\begin{array}{rcl} x\mathcal{R}y & \Longleftrightarrow & x \star y^{-1} \in G' \\ & \Longrightarrow & (x \star y^{-1})^{-1} \in G' \\ & \Longrightarrow & y \star x^{-1} \in G' \\ & \Longrightarrow & y\mathcal{R}x \end{array}$$

iii) $\mathcal{R}$ est Transitive, car : $\forall\, x,\ y\ z \in G$,

$$\begin{array}{rcll}(x\mathcal{R}y)\wedge(y\mathcal{R}z) & \Longleftrightarrow & [(x\star y^{-1})\in G']\wedge[(y\star z^{-1})\in G'] & \\ & \Longrightarrow & (x\star y^{-1})\star(y\star z^{-1})\in G', & \text{car } G' \text{ est un sous groupe}\\ & \Longrightarrow & (x\star(y^{-1}\star y)\star z^{-1})\in G', & \text{car } \star \text{ est associative}\\ & \Longrightarrow & (x\star z^{-1})\in G' & \\ & \Longrightarrow & x\mathcal{R}z & \end{array}$$

De i), ii) et iii) on déduit que $\mathcal{R}$ est une relation d'équivalence.

□

On note $G_{/G'}$ l'ensemble quotient $G_{/\mathcal{R}}$. On définit sur $G_{/G'}\times G_{/G'}$ l'opération $\oplus$ par :

$$\forall\ (\dot{a},\ \dot{b})\in G_{/G'}\times G_{/G'},\quad \dot{a}\oplus\dot{b}=\dot{\overline{a\star b}}$$

Propriété 4.10 *Si $\star$ est commutative, alors $\oplus$ est une loi de composition interne dans $G_{/G'}$.*

Preuve : Ceci revient à montrer que $\oplus$ est une application de $G_{/G'}\times G_{/G'}$ dans $G_{/G'}\times G_{/G'}$.
Soient $(\dot{a},\dot{b})$ et $(\dot{c},\dot{d})\in G_{/G'}$, alors

$$\begin{array}{rcl}(\dot{a},\dot{b})=(\dot{c},\dot{d}) & \Longrightarrow & (\dot{a}=\dot{c})\wedge(\dot{b}=\dot{d})\\ & \Longrightarrow & \Big(a\mathcal{R}c\Big)\wedge\Big(b\mathcal{R}d\Big)\\ & \Longrightarrow & \Big(a\star c^{-1}\in G'\Big)\wedge\Big(b\star d^{-1}\in G'\Big)\end{array}$$

Montrons que

$$(\dot{a},\dot{b})=(\dot{c},\dot{d})\Longrightarrow \dot{a}\oplus\dot{b}=\dot{c}\oplus\dot{d}\ .$$

Supposons que $(\dot{a},\dot{b})=(\dot{c},\dot{d})$, alors : $\forall x\in G$,

$$\begin{array}{rcll}x\in\dot{a}\oplus\dot{b} & \Longleftrightarrow & x\in\dot{\overline{a\star b}} & \\ & \Longleftrightarrow & x\mathcal{R}(a\star b) & \\ & \Longleftrightarrow & x\star(a\star b)^{-1}\in G' & \\ & \Longleftrightarrow & x\star(b^{-1}\star a^{-1})\in G' & \\ & \Longrightarrow & (x\star(b^{-1}\star a^{-1}))\star(a\star c^{-1})\in G', & \text{Car } G' \text{ sous-groupe}\\ & \Longrightarrow & ((x\star b^{-1})\star(a^{-1}\star a)\star c^{-1})\in G', & \text{Car } \star \text{ associative}\\ & \Longrightarrow & ((x\star b^{-1})\star c^{-1})\in G' & \\ & \Longrightarrow & ((x\star b^{-1})\star c^{-1})\star(b\star d^{-1})\in G', & \text{Car } G' \text{ sous-groupe}\\ & \Longrightarrow & (x\star(b^{-1}\star b)\star(c^{-1}\star d^{-1}))\in G', & \text{Car } \star \text{ est commutative et associative}\\ & \Longrightarrow & (x\star(c^{-1}\star d^{-1}))\in G' & \\ & \Longrightarrow & (x\star(d\star c)^{-1})\in G' & \\ & \Longrightarrow & x\mathcal{R}(d\star c) & \\ & \Longrightarrow & x\mathcal{R}(c\star d), & \text{car } \star \text{ commutative}\\ & \Longrightarrow & x\in\dot{c}\oplus\dot{d} & \end{array}$$

donc

$$\dot{a} \oplus \dot{b} \subset \dot{c} \oplus \dot{d}$$

et de la même manière on montre que

$$\dot{c} \oplus \dot{d} \subset \dot{a} \oplus \dot{b}$$

par suite :

$$(\dot{a}, \dot{b}) = (\dot{c}, \dot{d}) \Longrightarrow \dot{a} \oplus \dot{b} = \dot{c} \oplus \dot{d}$$

ce qui montre que la loi $\oplus$ est interne dans $G_{/G'}$.

□

Propriété 4.11 *Si $(G, \star)$ est un groupe abélien, alors $(G_{/G'}, \oplus)$ est un groupe abélien, appelé groupe quotient de G par G'.*

Preuve :

i) $\oplus$ est associative car : $\forall\, \dot{x},\ \dot{y}\ \dot{z} \in G_{/G'}$,

$$\begin{aligned} \dot{x} \oplus (\dot{y} \oplus \dot{z}) &= \dot{x} \oplus \dot{\overline{x + y}} \\ &= \dot{\overline{x \star (\dot{y} \star z)}} \\ &= \dot{\overline{(x \star \dot{y}) \star z}} \text{Car } \star \text{ est associative} \\ &= \dot{\overline{(x \star y)}} \oplus \dot{z} \end{aligned}$$

donc :

$$\forall\, x,\ y\ z \in G_{/G'}, \quad \dot{x} \oplus (\dot{y} \oplus \dot{z}) = \dot{\overline{(x \star y)}} \oplus \dot{z}$$

ii) Si e est l'élément neutre de $\star$, alors $\dot{e}$ est l'élément neutre de $\oplus$, car : $\forall\, \dot{x} \in G_{/G'}$,

$$\dot{x} \oplus \dot{e} = \dot{\overline{x \star e}} = \dot{x}$$
$$\dot{e} \oplus \dot{x} = \dot{\overline{e \star x}} = \dot{x}$$

iii) Soit $\dot{x} \in G_{/G'}$ alors $(\dot{x})^{-1} = \dot{\overline{x^{-1}}}$, car

$$\dot{x} \oplus \dot{\overline{x^{-1}}} = \dot{\overline{x \star \dot{x^{-1}}}} = \dot{e}$$
$$\dot{\overline{x^{-1}}} \oplus \dot{x} = \dot{\overline{x^{-1} \star x}} = \dot{e}$$

iv) $\oplus$ est commutative car $\star$ est commutative.

De i), ii), iii) et iv), on déduit que $\left(G_{/G'}, \oplus\right)$ est un groupe abélien

□

Exemple 4.10 *On sait que dans le groupe commutatif $(\mathbb{Z}, +)$; pour tout $n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous sous groupe de $\mathbb{Z}$, donc on peut parler du groupe quotient $\mathbb{Z}_n = \mathbb{Z}\Big|_{n\mathbb{Z}}$.*

4.2.4 Homomorphismes de Groupes

Dans ce paragraphe, on considère $(G, \bullet)$ et $(H, \star)$ deux groupes, avec e et h leurs éléments neutres respectifs.

Définition 4.8 *Une application $f : G \longrightarrow H$ est appelée homomorphisme de groupes de G dans H si :*

$$\forall\ a,\ b \in G, \quad f(a \bullet b) = f(a) \star f(b).$$

- Si f est bijective, on dit que f est un isomorphisme (de groupes) de G sur H. On dit alors que G est isomorphe à H, ou que G et H sont isomorphes.

- Si $G = H$, on dit que f est un endomorphisme de G, et si de plus f est bijective, on dit que f est un automorphisme (de groupe) de G.

Exemple 4.11 *Etant donnés les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \cdot)$, alors les applications*

$$\begin{array}{rccc} f: & (\mathbb{R},+) & \longrightarrow & (\mathbb{R}^*,\cdot) \\ & x & \longrightarrow & \exp x \end{array} \qquad et \qquad \begin{array}{rccc} g: & (\mathbb{R}^*,\cdot) & \longrightarrow & (\mathbb{R},+) \\ & x & \longrightarrow & \ln|x| \end{array}$$

Définition 4.9 *Soit $f : G \longrightarrow H$ un homomorphisme de groupes. On appelle noyau de f l'ensemble*

$$\mathrm{Ker}\, f = f^{-1}(\{h\}) = \{a \in G;\ f(a) = h\}$$

et l'image de f l'ensemble

$$\Im m f = f(G) = \{f(a),\ a \in G\ \}.$$

Propriété 4.12 *Soit $f : G \longrightarrow H$ un homomorphisme de groupes, alors*

1. $f(e) = h$
2. $\forall\ a \in G,\ (f(a))^{-1} = f(a^{-1})$

Preuve :

1. h étant l'élément neutre de $\star$ et e celui de $\bullet$, alors

$$f(e + e) = f(e) = h \star f(e)$$

et comme f est un homomorphisme on déduit que

$$h \star f(e) = f(e) \star f(e)$$

et comme tous les éléments du groupe $(H, \star)$ sont réguliers, on déduit que $h = f(e)$.

2. Soit $a \in G$ et montrons que $f(a^{-1})$ est l'inverse de $f(a)$ dans le groupe $(H, \star)$.
f étant un homomorphisme de groupe alors

$$f(a) \star f(a^{-1}) = f(a \bullet a^{-1}) = f(e) \quad et \quad f(a^{-1}) \star f(a) = f(a^{-1} \bullet a) = f(e)$$

sachant que $f(e) = h$, d'après la première propriété, on déduit que $(f(a))^{-1} = f(a^{-1})$.

□

Remarque 4.7 *De la première propriété on déduit que $e \in \ker f$.*

Propriété 4.13 *Soit $f : G \longrightarrow H$ un homomorphisme de groupes, alors*

1. *L'image d'un sous groupe de G est un sous groupe de H.*
2. *L'image réciproque d'un sous groupe de H est un sous groupe de G.*

Preuve :

1. Soit G' un sous groupe de G et montrons que $f(G')$ vérifie les deux conditions de la caractérisation des sous groupes.

i) Comme G' est un sous groupe de G, alors $e \in G'$ donc $f(e) \in f(G')$, par suite $f(G') \neq \emptyset$.

ii) Soient $a,\ b \in f(G')$, alors il existe $x,\ y \in G'$ tels que $a = f(x)$ et $b = f(y)$, donc d'après la deuxième propriété on aura

$$a \star b^{-1} = f(x) \star (f(y))^{-1} = f(x) \star f(y^{-1}) = f(x \bullet y^{-1})$$

et comme G' est un sous groupe de G alors $(x \bullet y^{-1}) \in G'$, par suite

$$a \star b^{-1} = f(x \bullet y^{-1}) \in f(G')$$

de i) et ii) on déduit que $f(G')$ est un sous groupe de H.

2. Soit H' un sous groupe de H, alors

i) D'après la première propriété $f(e) = h$ et comme H' est un sous groupe de H alors $h \in H'$ donc $e \in f^{-1}(H')$.

ii) Soient $x,\ y \in f^{-1}(H')$, alors $f(x),\ f(y) \in H'$ et comme H' est un sous groupe de G alors $f(x) \star (f(y))^{-1} \in H'$ et de la deuxième propriété on déduit que

$$f(x \bullet y^{-1}) = f(x) \star f(y^{-1}) = f(x) \star (f(y))^{-1} \in H'$$

ce qui montre que $(x \bullet y^{-1}) \in f^{-1}(H')$.
De i) et ii) on déduit que $f^{-1}(H')$ est un sous groupe de G.

□

Remarque 4.8 *Comme cas particuliers des propriétés,*

$\Im m f$ *est un sous groupe de* $(H, \star)$ *et*

$\mathrm{Ker}\, f$ *est un sous groupe de* $(G, \bullet)$.

Propriété 4.14 *Soit $f : G \longrightarrow H$ un homomorphisme de groupe, alors*

1. *f est injective si et seulement si* $\mathrm{Ker}\, f = \{e\}$.
2. *f est surjective si et seulement si* $\Im m f = H$.
3. *f est un isomorphisme si et seulement si f^{-1} existe et est un homomorphisme de groupe de H dans G.*

Preuve. Soit $f : G \longrightarrow H$ un homomorphisme de groupe, alors

1a. Si f est injectif, sachant que $e \in \ker f$ on va montrer que $\ker f \subset \{e\}$.
Soit $x \in \ker f$, alors $f(x) = h$ et comme $f(e) = h$ on déduit que $f(x) = f(e)$ et comme f est injectif on déduit que $x = e$, donc $x \in \{e\}$ ce qui montre que $\ker f = \{e\}$.

1b. Inversement, supposons que $\ker f = \{e\}$ et montrons que f est injectif.
Soient $x,\ y \in G$, alors

$$\begin{array}{rcll} f(x) = f(y) & \Longrightarrow & f(x) \star (f(y))^{-1} = h & \\ & \Longrightarrow & f(x) \star f(y^{-1}) = h & \\ & \Longrightarrow & f(x \bullet y^{-1}) = h & \\ & \Longrightarrow & (x \bullet y^{-1}) \in \ker f & \\ & \Longrightarrow & x \bullet y^{-1} = e \quad \text{car } \ker f = \{e\} & \\ & \Longrightarrow & x = y & \end{array}$$

ce qui montre que f est injectif.

2. La preuve de cette propriété est immédiate, sachant que $\Im m f = f(G)$.

3. On se limitera à démontrer que si f est un isomorphisme, alors $f^{-1} : H \longrightarrow G$ est aussi un homomorphisme. Soient $x,\ y \in H$, alors il existe $a,\ b \in G$ tels que

$$x = f(a) \qquad et \qquad y = f(b)$$

donc

$$a = f^{-1}(x) \qquad et \qquad b = f^{-1}(y),$$

par suite

$$\begin{array}{rcll} f^{-1}(x \star y) & = & f^{-1}(f(a) \star f(b)) & \\ & = & f^{-1}(f(a \bullet b)) \qquad \text{car } f \text{ homomorphisme} & \\ & = & a \bullet b & \\ & = & f^{-1}(x) \bullet f^{-1}(y) & \end{array}$$

ce qui montre que f^{-1} est un homomorphisme de groupe de H dans G.

□

4.3 Structure d'Anneaux

Définition 4.10 *On appelle anneau, tout ensemble A muni de deux lois de composition internes $+$ et $\bullet$ telles que :*

1. *$(A, +)$ est un groupe abélien (on notera 0 ou 0_A l'élément neutre de $+$),*

2. *$\bullet$ est associative et distributive par rapport à $+$.*

Si de plus $\bullet$ est commutative, on dit que $(A, +, \bullet)$ est un anneau commutatif.

Conventions :

$(A,+)$ étant un groupe, alors tous les éléments de A sont symétrisables et on convient de noter $-x$ le symétrique d'un élément $x \in A$.

Si $\bullet$ possède un élément neutre, on le note 1 ou 1_A et on dit que l'anneau $(A,+,\bullet)$ est unitaire ou unifère.
Dans un tel anneau, on dit qu'un élément est inversible s'il l'est par rapport à la deuxième loi $\bullet$. L'inverse d'un élément $x \in A$ est noté x^{-1}.

Régles de Calcul dans un Anneau

Soit $(A,+,\bullet)$ un anneau, alors on a les règles de calculs suivantes :

Propriété 4.15 *Pour tous x, y et $z \in A$,*

1. $0_A \bullet x = x \bullet 0_A = 0_A$

2. $x \bullet (-y) = (-x) \bullet y = -(x \bullet y)$

3. $x \bullet (y - z) = (x \bullet y) - (x \bullet z)$

4. $(y - z) \bullet x = (y \bullet x) - (z \bullet x)$

Preuve :
1. Soit $x \in A$, alors

$$0_A \bullet x = (0_A + 0_A) \bullet x = (0_A \bullet x) + (0_A \bullet x) \qquad \text{car } \bullet \text{ est distributive par rapport à } +$$

comme tous les éléments de A sont symétrisables, on déduit que $0_A \bullet x = 0_A$.
De la même manière on montre que $x \bullet 0_A = 0_A$.

2. Soient $x,\ y \in A$ et montrons que $x \bullet (-y)$ est le symétrique de $(x \bullet y)$. On a :

$$(x \bullet (-y)) + (x \bullet y) = x \bullet (-y + y) = x \bullet 0_A = 0_A$$

comme $+$ est commutative on déduit que $(x \bullet (-y)) = -(x \bullet y)$.
De la même manière on montre que $(-x) \bullet y = -(x \bullet y)$.

La preuve des propriétés **3.** et **4.** utilise essentiellement la distributivité de la loi $\bullet$ par rapport à $+$.

□

On note $A^* = A \backslash \{0\}$, et pour tout $x \in A^*$ et $n \in \mathbb{N}^*$,

$$n.x = nx = \underbrace{x + x + \ldots + x}_{n \text{ fois}} \qquad et \qquad x^n = \underbrace{x \bullet x \bullet \ldots \bullet x}_{n \text{ fois}}$$

Définition 4.11 *Soit $(A,+,\bullet)$ un anneau commutatif. On dit que $y \in A^*$ divise $x \in A$, ou que y est un diviseur de x ou que x est divisible par y, si*

$$\exists\ z \in A^*, \quad x = y \bullet z.$$

Si 0_A ne possède pas de diviseur dans A, on dit que $(A,+,\bullet)$ est un anneau intègre ou un anneau d'intégrité.

4.3.1 Sous Anneaux

Définition 4.12 *On appelle sous anneau de $(A,+,\bullet)$, tout sous ensemble A' de A tel que muni des restrictions des lois $+$ et $\bullet$ est anneau.*
Si A est un anneau unitaire et $1_A \in A'$, on dit que A' est sous anneau unitaire.

On a la cartérisation suivante des sous anneaux.

Propriété 4.16 *Un sous ensemble A' de A est un sous anneau si et seulement si :*
1. $A' \neq \emptyset$,
2. $\forall\ x,\ y \in A',\ (x-y) \in A'$
3. $\forall\ x,\ y \in A',\ (x \bullet y) \in A'$.

Preuve : On sait que A' est est un sous groupe de $(A,+)$ si et seulement si

$$(A' \neq \emptyset) \wedge (\forall\ x,\ y \in A',\ (x-y) \in A'),$$

donc pour que A' soit un sous anneau de A, il suffit de voir si la restriction de la deuxième loi $\bullet$ est interne dans A', ce qui revient à dire que $(\forall\ x,\ y \in A',\ x \bullet y \in A')$, ce qui termine la preuve de notre proposition.

□

4.3.2 Homomorphismes d'Anneaux

Soient $(A,+,\bullet)$ et $(B,\oplus,\otimes)$ deux anneaux et $f : A \longrightarrow B$.

Définition 4.13 *On dit que f est un homomorphisme d'anneaux si :*

$$\forall\ x,\ y \in A, \quad f(x+y) = f(x) \oplus f(y) \ \ et \ \ f(x \bullet y) = f(x) \otimes f(y)$$

- *Si $A = B$ on dit que f est un endomorphisme d'anneau de A.*
- *Si f est bijective, on dit que f est un isomorphisme d'anneaux*
- *Si f est bijective et $A = B$, on dit que f est un automorphisme d'anneaux.*

On sait que l'image de l'élément neutre du groupe de départ d'un homomorphisme de groupe est l'élément neutre du groupe d'arrivée. Par contre, l'image de l'élément unité de l'anneau de départ par un homomorphisme d'anneau n'est pas toujours l'élément unité de l'anneau d'arrivée. Pour s'en convaincre, il suffit de prendre dans un anneau unitaire $(A,+,\cdot)$,

où $0_A \neq 1_A$[2], l'application $f : A \longrightarrow A$ définie par $f(x) = 0_A$ pour tout $x \in A$.

Ce contre exemple nous amène à poser la définition suivante.

Définition 4.14 *Soient A et B deux anneaux unitaires, on dit qu'un homomorphisme d'anneaux f de A dans B est unitaire si $f(1_A) = 1_B$.*

Proposition 4.1 *Soit $f : A \longrightarrow B$ un homomorphisme d'anneaux, alors*
- *f est injectif si et seulement si $kerf$=$\{0_A\}$*
- *Si A et B sont deux anneaux unitaires et f un homomorphisme d'anneaux surjectif, alors f est unitaire.*

Preuve : La première propriété provient de la caractérisation des homomorphismes injectifs entre les groupes $(A, +)$ et $(B, +)$.

Montrons la deuxième propriété.

Soit $y \in B$, f étant injectif, il existe alors $x \in A$ tel que $y = f(x)$, et comme f est un homomorphisme d'anneau on déduit

$$y = f(x) = f(1_A \cdot x) = f(1_A) \cdot f(x) = f(1_A) \cdot y$$

et de la même manière on montre que $y = y \cdot f(1_A)$, ce qui montre que $f(1_A) = 1_B$.

□

Proposition 4.2 *L'image (respectivement l'image réciproque) d'un sous anneau de A (respectivement de B) par f est un sous anneau de B (respectivement de A).*

4.3.3 Idéaux

Soit $(A, +, \bullet)$ un anneau.

Définition 4.15 *On appelle idéal à droite (respectivement à gauche) de l'anneau A, tout ensemble $I \subset A$ tel que*

1. *I est un sous groupe de $(A, +)$,*
2. *$\forall\ x \in A$, $(\forall\ y \in I, \quad x \bullet y \in I \quad (respectivement\ y \bullet x \in I))$.*

Si I est idéal à droite et à gauche de A, on dit que I est un idéal bilatère de A.

Si l'anneau A est commutatif, tout idéal de A est bilatère, et dans ce cas on parle seulement d'Idéal sans préciser s'il l'est à droite, à gauche ou bilatère.

Exemple 4.12 *Soit $(A, +, \bullet)$ un anneau, alors $I = \{O_A\}$ est un idéal bilatère de A.*

[2]Ceci revient à dire que A n'est pas un singleton.

Exemple 4.13 *Dans l'anneau commutatif $(\mathbb{Z}, +, \cdot)$, $n\mathbb{Z}$ est un idéal.*

Proposition 4.3 *Soit I un idéal à gauche (ou à droite) d'un anneau unitaire $(A, +, \bullet)$, alors*

$$1_A \in I \Longleftrightarrow I = A \Longleftrightarrow \exists\ x \in I; \quad x \quad \textit{est inversible.}$$

Définition 4.16 *On appelle idéal principal d'un anneau commutatif $(A, +, \bullet)$, tout idéal I de A tel que*

$$\exists x \in A; \quad I = x \bullet A$$

L'anneau A est dit principal si tous ses idéaux sont principaux.

4.3.4 Anneaux Quotients

Soient $(A, +, \bullet)$ un anneau commutatif et I un idéal de A. On considère le groupe quotient $(A_{/I}, \oplus)$, et on définit l'application $\otimes$ de $A_{/I} \times A_{/I}$ dans $A_{/I}$ par

$$\forall\ \dot{a},\ \dot{b} \in A_{/I}, \quad \dot{a} \otimes \dot{b} = \overline{a \bullet b}^{\cdot}$$

Propriété 4.17 *$(A_{/I}, \oplus, \otimes)$ est anneau commutatif. Si de plus A est un anneau unitaire, alors $(A_{/I}, \oplus, \otimes)$ est un anneau unitaire et $\overline{1_A}^{\cdot}$ est son élément unité.*

4.4 Corps

Définition 4.17 *On dit qu'un anneau unitaire $(\mathbb{K}, +, \bullet)$ est un corps si tout élément non nul de $\mathbb{K}$ est inversible. Si de plus $\bullet$ est commutative, on dit que $\mathbb{K}$ est un corps commutatif.*

Il est à remarquer que dans la pratique, tous les corps utilisés sont commutatifs.

Propriété 4.18 *Tout corps est un anneau intègre.*

Définition 4.18 *On appelle sous corps, d'un corps $(\mathbb{K}, +, \bullet)$, tout sous ensemble* **K'** *de $\mathbb{K}$ tel que, muni des restrictions des lois $+$ et $\bullet$ est un corps.*

Proposition 4.4 *$\mathbf{K}' \subset \mathbb{K}$ est un sous corps de $(\mathbb{K}, +, \bullet)$ si et seulement si*
- *$\mathbf{K}' \neq \emptyset$*
- *$\forall\ a, b \in \mathbf{K}', \quad a - b$ et $a \bullet b^{-1} \in \mathbf{K}'$.*

On a aussi la caractérisation suivante des corps.

Proposition 4.5 *Soit $(\mathbb{K}, +, \bullet)$ un anneau commutatif unitaire, alors $\mathbb{K}$ est un corps si et seulement si les seuls idéaux de $\mathbb{K}$ sont $\{\mathbf{0}_K\}$ et lui même.*

4.4.1 Caractéristique d'un corps

Etant donné $n \in \mathbb{N}$, alors $\mathbf{Z}_{/n\mathbf{Z}}$ est un corps si n est premier, et on a

$$n\dot{1} = \dot{1} + \cdots + \dot{1} = \dot{0}.$$

D'une façon générale on a :

Définition 4.19 *Le plus petit entier naturel non nul n tel que $n1_{\mathbb{K}} = 0_{\mathbb{K}}$, s'il existe, est appelé caractéristique du corps commutatif* $\mathbf{K}$. *Si pour tout $n \in \mathbb{N}$, $n1_{\mathbb{K}} \neq 0_{\mathbb{K}}$, on dit que* $\mathbf{K}$ *est de caractéristique nulle.*

Propriété 4.19 *La caractéristique d'un corps est un nombre premier.*

Exemple : Pour $n \in \mathbb{N}$ premier, la caractéristique du corps $\mathbf{Z}_{/n\mathbf{Z}}$ est égale à n.