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
$\mathcal{P}$	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
$\mathcal{P} \vee \bar{\mathcal{P}}$	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 $x \notin E$.

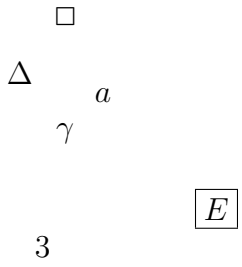
Pour définir un ensemble,
- ou bien on connait la liste de tous ses éléments, on dit alors que l'ensemble est donné "*par Extension*",
- ou bien on connait seulement les relations qui lient les éléments et qui nous permettent de les retrouver tous, on dit alors que l'ensemble est donné par "*Compréhension*".
- 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] *:*

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

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*

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

alors

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

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 :

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

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 :

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

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

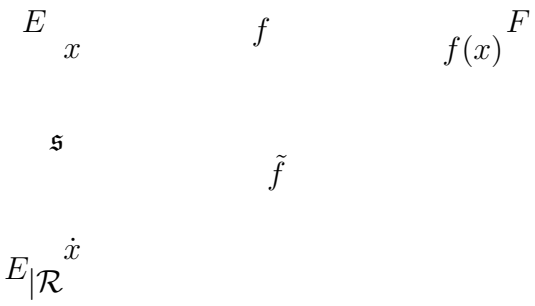
$$\forall x,\ y \in E, \qquad (x\mathcal{R}y) \Longrightarrow (y\mathcal{R}x)$$

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

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

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 " ∩" et " ∪", alors il est très facile de montrer que :*

- *" ∩" et " ∪" sont associatives*
- *" ∩" et " ∪" 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 :

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

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 : $\forall\, \dot{x} \in G_{/G'}$,

$$\begin{aligned} \dot{x} \oplus \dot{e} &= \dot{\overline{x \star e}} = \dot{x} \\ \dot{e} \oplus \dot{x} &= \dot{\overline{e \star x}} = \dot{x} \end{aligned}$$

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

$$\begin{aligned} \dot{x} \oplus \dot{\overline{x^{-1}}} &= \dot{\overline{x \star \dot{x^{-1}}}} = \dot{e} \\ \dot{\overline{x^{-1}}} \oplus \dot{x} &= \dot{\overline{x^{-1} \star x}} = \dot{e} \end{aligned}$$

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

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

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

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

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 :*

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

- *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*
- $\mathbf{K}' \neq \emptyset$
- $\forall\ a,\ b \in \mathbf{K}',\quad a - b \quad et \quad a \bullet b^{-1} \in \mathbf{K}'$.

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.

Chapitre 5

ESPACES VECTORIELS

5.1 Espaces vectoriels

Soient $\mathbb{K}$ un corps commutatif et E un ensemble non vide. On considère

$$\begin{array}{rccc} + : & E \times E & \longrightarrow & E \\ & (x, y) & \longrightarrow & x + y \end{array}$$

une loi de composition interne dans E et

$$\begin{array}{rccc} \cdot \ : & \mathbb{K} \times E & \longrightarrow & E \\ & (\alpha, x) & \longrightarrow & \alpha \cdot x \end{array}$$

une loi de composition externe sur E.

Définition 5.1 [1] On dit que E est un espace vectoriel sur $\mathbb{K}$, ou c'est un $\mathbb{K}$-espace vectoriel, si :

1. $(E, +)$ est un groupe abélien.
2. $\forall \alpha \in \mathbb{K},\ \forall x,\ y \in E, \quad \alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$
3. $\forall \alpha,\ \beta \in \mathbb{K},\ \forall x \in E, \quad (\alpha + \beta) \cdot x = \alpha \cdot x\ +\ \beta \cdot x$
4. $\forall \alpha,\ \beta \in \mathbb{K},\ \forall x \in E, \quad (\alpha.\beta) \cdot x = \alpha \cdot (\beta x)$
5. $\forall x \in E, \quad 1_{\mathbb{K}} \cdot x = x.$

Conventions :

- Les éléments d'un espace vectoriel E sont appelés *vecteurs* et sont représentés en général avec une flèche dessus pour les distinguer des éléments du corps $\mathbb{K}$ qui sont appelés *scalaires*.
- L'élément neutre de la loi $+$ est noté $\overrightarrow{0}$, appelé le vecteur nul et le scalaire nul est noté $0_{\mathbb{K}}$ ou 0.
- $(E, +)$ étant un groupe, le symétrique d'un vecteur $\overrightarrow{x} \in E$ est noté $-\overrightarrow{x}$.
- Quand il n'y a pas de confusion, on écrira $\alpha \overrightarrow{x}$ au lieu de $\alpha \cdot \overrightarrow{x}$.

Exemples : Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, alors :

1. $\mathbb{K}$ est un $\mathbb{K}$-espace verctoriel.

[1] Si $\mathbb{K}$ est seulement un anneau commutatif unitaire, on dit que E est un module sur $\mathbb{K}$

2. $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel.

Soit $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$ l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. On définit sur E les opérations suivantes :

1. $\forall\, f,\ g \in \mathcal{F}(\mathbb{R}, \mathbb{R}),\ \ f \oplus g$ est définie par :

$$\forall\, x \in \mathbb{R}, \quad (f \oplus g)(x) = f(x) + g(x)$$

2. $\forall\, f \in \mathcal{F}(\mathbb{R}, \mathbb{R}), \forall\, \alpha \in \mathbb{R},\ \ \alpha \cdot f$ est définie par

$$\forall\, x \in \mathbb{R}, \quad (\alpha \cdot f)(x) = \alpha f(x)$$

Propriété 5.1 *$(\mathcal{F}(\mathbb{R}, \mathbb{R}), \oplus, \odot)$ est un $\mathbb{R}$-espace vectoriel.*

Preuve :

5.1.1 Regles de calcul dans un espace vectoriel

Soit $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel, alors on a les règles de calcul suivantes :

1. $\forall\ \overrightarrow{x} \in E, \quad 0_{\mathbb{K}} \cdot \overrightarrow{x} = \overrightarrow{0}$
2. $\forall\ \alpha \in \mathbb{K}, \quad \alpha \cdot \overrightarrow{0} = \overrightarrow{0}$
3. $\forall\ \overrightarrow{x} \in E, \forall\ \alpha \in \mathbb{K}, \quad \alpha \cdot (-\overrightarrow{x}) = (-\alpha) \cdot \overrightarrow{x} = -(\alpha \cdot \overrightarrow{x})$
4. $\forall\ \overrightarrow{x},\ \overrightarrow{y} \in E,\ \forall\ \alpha \in \mathbb{K}, \quad \alpha \cdot (\overrightarrow{x} - \overrightarrow{y}) = \alpha \cdot \overrightarrow{x} - (\alpha \cdot \overrightarrow{y})$
5. $\forall\ \alpha,\ \beta \in \mathbb{K}, \forall\ x \in E \quad (\alpha - \beta) \cdot \overrightarrow{x} = \alpha \cdot \overrightarrow{x} - (\beta \cdot \overrightarrow{x})$

Preuve :

1. Soit $\overrightarrow{x} \in E$, alors

$$\begin{array}{rcl} 0_{\mathbb{K}} \cdot \overrightarrow{x} & = & (0_{\mathbb{K}} + 0_{\mathbb{K}}) \cdot \overrightarrow{x} \\ & = & (0_{\mathbb{K}} \cdot \overrightarrow{x}) + (0_{\mathbb{K}} \cdot \overrightarrow{x}) \quad \text{(on utilise l'axiome } \mathbf{3} \text{ de la définition 5.1)} \end{array}$$

comme $(E, +)$ est un groupe, en rajoutant le symétrique de $0_{\mathbb{K}} \cdot \overrightarrow{x}$ dans les deux membres de cette identité on trouve

$$\overrightarrow{0} = 0_{\mathbb{K}} \cdot \overrightarrow{x}.$$

2. Soit $\alpha \in \mathbb{K}$, alors

$$\begin{array}{rcl} \alpha \cdot \overrightarrow{0} & = & \alpha \cdot (\overrightarrow{0} + \overrightarrow{0}) \\ & = & \alpha \cdot \overrightarrow{0} + \alpha \cdot \overrightarrow{0} \quad \text{(on utilise l'axiome } \mathbf{2} \text{ de la définition 5.1)} \end{array}$$

en aditionnant le symétrique de $\alpha \cdot \overrightarrow{0}$ dans les deux membres de cette identité on trouve

$$\overrightarrow{0} = \alpha \cdot \overrightarrow{0}.$$

3. Soient $\overrightarrow{x} \in E$ et $\alpha \in \mathbb{K}$, en utilisant l'axiome **2** de la définition 5.1 on obtient

$$\alpha \cdot (-\overrightarrow{x}) + \alpha \cdot (\overrightarrow{x}) = \alpha \cdot (-\overrightarrow{x} + \overrightarrow{x}) = \alpha \cdot \overrightarrow{0})$$

et de la deuxième règle de calcul dans les espaces vectoriels on déduit que

$$\alpha \cdot (-\overrightarrow{x}) + \alpha \cdot (\overrightarrow{x}) = \overrightarrow{0}$$

ce qui montre que

$$\alpha \cdot (-\overrightarrow{x}) = -(\alpha \cdot (\overrightarrow{x}))$$

De la même manière, en utilisant le troisième axiome de la définition d'un espace vectoriel on trouve

$$\alpha \cdot (\overrightarrow{x}) + (-\alpha) \cdot (\overrightarrow{x}) = (\alpha - \alpha) \cdot \overrightarrow{x} = 0 \cdot \overrightarrow{x}$$

et d'après la première règle de calcul on déduit que

$$\alpha \cdot (\overrightarrow{x}) + (-\alpha) \cdot (\overrightarrow{x}) = \overrightarrow{0}$$

ce qui montre que

$$(-\alpha) \cdot (\overrightarrow{x}) = -\alpha \cdot (\overrightarrow{x})$$

4. et **5.** sont des conséquences de la troisième règle de calcul et des axiomes **2** et **3** de la définition 5.1. □

Proposition 5.1 *Soit $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel, alors :*

$$\forall\, \alpha \in \mathbb{K},\ \forall\, \overrightarrow{x} \in E, \qquad \alpha \cdot \overrightarrow{x} = \overrightarrow{0} \Longleftrightarrow \Big[(\alpha = 0_K) \vee (\overrightarrow{x} = \overrightarrow{0})\Big]$$

Démonstration : La réciproque de cette équivalence traduit la première et la deuxième régle de calcul dans un espace vectoriel, montrons l'implication directe.

Soient $\alpha \in \mathbb{K}$ et $\overrightarrow{x} \in E$. Supposons que $\alpha \neq 0$ et montrons que $\overrightarrow{x} = \overrightarrow{0}$.
Comme $\mathbb{K}$ est un corp et $\alpha \neq 0$, alors α est inversible et en utilisant le cinquième et le quatrième axiome de la définition d'un espace vectoriel on obtient :

$$\overrightarrow{x} = 1_{\mathbb{K}} \cdot \overrightarrow{x} = (\alpha^{-1}.\alpha)\overrightarrow{x} = \alpha^{-1}(\alpha \cdot \overrightarrow{x}) = \alpha^{-1}\overrightarrow{0} = \overrightarrow{0}$$

ce qui termine notre démonstration. □

5.1.2 Espaces vectoriels produits

Soient $(E_1, , \cdot)$, $(E_2, , \cdot)$, $\ldots$, $(E_n, , \cdot)$ des $\mathbb{K}$-espaces vectoriels[2].
On définit sur l'ensemble produit $E = E_1 \times E_2 \ \ldots \ \times E_n$ la loi de composition interne $\oplus$ et la loi de composition externe $\odot$ par :
$\forall\ (\overrightarrow{x}_1, \ldots,\ \overrightarrow{x}_n),\ \ (\overrightarrow{y}_1, \ldots,\ \overrightarrow{y}_n) \in E,\ \ \forall \alpha \in \mathbb{K},$

$$(\overrightarrow{x}_1, \ldots,\ \overrightarrow{x}_n) \oplus (\overrightarrow{y}_1, \ldots,\ \overrightarrow{y}_n) = (\overrightarrow{x}_1 + \overrightarrow{y}_1, \ldots,\ \overrightarrow{x}_n + \overrightarrow{y}_n)$$

$$\alpha \odot (\overrightarrow{x}_1, \ldots, \overrightarrow{x}_n) = (\alpha \cdot \overrightarrow{x}_1, \ldots,\ \alpha \cdot \overrightarrow{x}_n)$$

Proposition 5.2 *$(E, \oplus, \odot)$ est un espace vectoriel sur $\mathbb{K}$, appelé espace vectoriel produit des E_j, $j = 1, \ldots, n$.*

La preuve de cette proposition est immédiate et on a :
- Le vecteur nul dans E est $\overrightarrow{0} = (\overrightarrow{0}_{E_1},\ \ldots,\ \overrightarrow{0}_{E_n})$.
- Pour $\overrightarrow{X} = (\overrightarrow{x}_1,\ \ldots,\ \overrightarrow{x}_n) \in E$, $-\overrightarrow{X} = (-\overrightarrow{x}_1,\ \ldots,\ -\overrightarrow{x}_n)$

Remarque 5.1 *Dans la pratique on utilise très souvent les espaces produits $\mathbb{R}^n$, avec $n \in \mathbb{N}^*$, qui sont des $\mathbb{R}$-espaces vectoriels.*

5.2 Sous-espaces vectoriels

Soient $(E, +, \bullet)$ un espace vectoriel sur $\mathbb{K}$ et F un sous ensemble non vide de E.

Définition 5.2 On dit que F est un sous espace vectoriel de E si les restrictions, à F, des lois de composition $+$ et $\bullet$ lui confèrent une structure d'espace vectoriel.

On a la caractéristation suivante des sous espaces vectoriels.

5.2.1 Caractérisations des sous espaces vectoriels

Proposition 5.3 *F est un sous espace vectoriel de E si et seulement si :*
sv1. $\overrightarrow{0} \in F$,
sv2. $\forall \overrightarrow{x},\ \overrightarrow{y} \in F,\ \ \overrightarrow{x} + \overrightarrow{y} \in F$
sv3. $\forall \overrightarrow{x} \in F,\ \forall \alpha \in \mathbb{K},\ \ \alpha \bullet \overrightarrow{x} \in F$

Démonstration :

I) Il est clair que si F avec les restrictions des lois $+$ et $\bullet$ est un espace vectoriel, alors :
1) F est un sous groupe de $(E, +)$, donc **sv1.** et **sv2.** sont vérifiées.
2) $\bullet$ est une application de $\mathbb{K} \times F$ dans F, donc **sv3.** est vérifiée.

II) Inversement, si **sv1.**, **sv2.** et **sv3.** sont vérifiées, alors

[2] Les lois définies sur les E_j ne sont pas nécessairement les mêmes

a) Pour $\overrightarrow{x}$ et $\overrightarrow{y}$ dans F, en choisissant $\alpha = 1_{\mathbb{K}}$, d'après la troisième règle de calcul dans un espace vectoriel et de **sv3.** on déduit que

$$-\overrightarrow{y} = (-1_{\mathbb{K}}) \bullet \overrightarrow{y} \in F$$

et de **sv2.** on déduit que

$$\overrightarrow{x} - \overrightarrow{y} \in F$$

et comme $\overrightarrow{0} \in F$, d'après **sv1.** on déduit que F est un sous groupe de $(E, +)$.

b) **sv3.** exprime le fait que la restriction de $\bullet$ à F est une loi de composition externe

c) Comme les quatres derniers axiomes de la définition d'un espace vectoriel sont vrais pour E, alors ils seront aussi vrais pour $F \subset E$.

De **a)**, **b)** et **c)** on déduit que F est un sous espace vectoriel de E.

□

Exemples : Parmi les ensembles suivants, donner ceux qui sont des sous espaces vectoriels de $\mathbb{R}^3$. $E = \{(x, y, z) \in \mathbb{R}^3;\quad 2x - y = 1\}$, $F = \big\{(x, y, z) \in \mathbb{R}^3; xy = 0\big\}$, $H = \{(x, y, z) \in \mathbf{Z}^3; x + y = 0\}$, $L = \big\{(x, y, z) \in \mathbb{R}^3;\quad 2x - y + z = 0\big\}$.

On va utiliser la caractérisation précédente pour répondre à cette question.

1.

a. Soit $\overrightarrow{0} = (x, y, z) = (0, 0, 0) \in \mathbb{R}^3$, alors

$$2x - y = 2.0 + 0 = 0 \neq 0$$

ce qui montre que $\overrightarrow{0} \notin E$, par suite E n'est pas un sous espace vectoriel de $\mathbb{R}^3$.

2.

a. Soit $\overrightarrow{0} = (x, y, z) = (0, 0, 0) \in \mathbb{R}^3$, alors

$$xy = 0.0 = 0$$

donc $\overrightarrow{0} \in F$.

b. Soient $\overrightarrow{X} = (x, y, z),\ \overrightarrow{Y} = (x', y', z') \in F$, alors

$$\overrightarrow{X} + \overrightarrow{Y} = (x + x', y + y', z + z') = (u, v, w)$$

et

$$u.v = x.y + x.y' + x'.y + x'.y' = 0 + x.y' + x'.y + 0 = x.y' + x'.y$$

or, si on choisit $\overrightarrow{X} = (0, y, z),\ \overrightarrow{Y} = (x', 0, z')$, avec $y \neq 0$ et $x' \neq 0$, alors $\overrightarrow{X},\ \overrightarrow{Y} \in F$ et $u.v = x'.y \neq 0$, donc :

$$\exists \overrightarrow{X},\ \overrightarrow{Y} \in F;\quad \overrightarrow{X} + \overrightarrow{Y} \notin F$$

ce qui montre que F n'est pas un sous espace vectoriel de $\mathbb{R}^3$.

3.

a. Soit $\overrightarrow{0} = (x, y, z) = (0, 0, 0) \in \mathbb{R}^3$, alors

$$\overrightarrow{0} \in \mathbf{Z}^3 \qquad et \qquad x + y = 0$$

donc $\overrightarrow{0} \in H$.

b. Soient $\overrightarrow{X} = (x, y, z),\ \overrightarrow{Y} = (x', y', z') \in H$, alors

$$\overrightarrow{X} + \overrightarrow{Y} = (x + x', y + y', z + z') = (u, v, w) \in \mathbf{Z}^3$$

et

$$u + v = x + x' + y + y' = (x + y) + (x' + y') = 0 + 0 = 0$$

donc $\overrightarrow{X} + \overrightarrow{Y}$.

c. Soient $\overrightarrow{X} = (x, y, z) \in H$ et $\alpha \in \mathbb{R}$, on remarque que si on choisit $\overrightarrow{X} = (1, -1, 3)$, alors $\overrightarrow{X} \in H$ et pour $\alpha \in \mathbb{R}\backslash\mathbf{Z}\ \alpha\overrightarrow{X} \notin \mathbf{Z}^3$, donc

$$\exists \overrightarrow{X} \in H,\ \exists \alpha \in \mathbb{R}; \qquad \alpha\overrightarrow{X} \notin H$$

ce qui montre que H n'est pas un sous espace vectoriel de $\mathbb{R}^3$.

4.

a. Soit $\overrightarrow{0} = (x, y, z) = (0, 0, 0) \in \mathbb{R}^3$, alors

$$2x - y + z = 2.0 - 0 + 0 = 0$$

donc $\overrightarrow{0} \in L$.

b. Soient $\overrightarrow{X} = (x, y, z),\ \overrightarrow{Y} = (x', y', z') \in L$, alors

$$\overrightarrow{X} + \overrightarrow{Y} = (x + x', y + y', z + z') = (u, v, w)$$

et

$$2u - v + w = 2(x + x') - (y + y') + (z + z') = (2x - y + z) + (2x' - y' + z') = 0 + 0 = 0$$

donc $\overrightarrow{X} + \overrightarrow{Y} \in L$.

c. Soient $\overrightarrow{X} = (x, y, z) \in L$ et $\alpha \in \mathbb{R}$, alors

$$\alpha\overrightarrow{X} = (\alpha x, \alpha y, \alpha z) = (u, v, w)$$

et

$$2u - v + w = 2\alpha x - \alpha y + \alpha z = \alpha(2x - y + z) + \alpha.0 = 0$$

donc $\alpha\overrightarrow{X} \in L$.

De **a.**, **b.** et **c.** on déduit que L est un sous espace vectoriel de $\mathbb{R}^3$.

□

En combinant **sv2.** et **sv3.** on obtient la caractérisation suivante :

Proposition 5.4 *F est un sous espace vectoriel de E si et seulement si :*
SV1. $\overrightarrow{0} \in F$,
SV2. $\forall \overrightarrow{x},\ \overrightarrow{y} \in F, \quad \forall \alpha,\ \beta \in \mathbb{K}, \qquad \alpha\,\overrightarrow{x} + \beta\,\overrightarrow{y} \in F.$

Exemples :

1. $\{\overrightarrow{0}\}$ est un sous espace vectoriel de E.

2. Soit $n \in \mathbb{N}$. L'ensemble $\mathbb{K}_n[X]$, des polynômes sur $\mathbb{K}$ de degré inférieur ou égal à n, est un sous espace vectoriel de $\mathbb{K}[X]$.

3. Si E est un $\mathbb{K}$-espace vectoriel, l'intersection de deux sous espaces vectoriels de E est un sous espace vectoriel de E.

Définition 5.3 *On dit que F est sous espace vectoriel propre de E si $E \neq \{\overrightarrow{0}\}$ et $F \neq E$.*

Proposition 5.5 *Soient E_1 et E_2 deux sous espaces vectoriels de $(E, , \bullet)$, alors :*
- *$E_1 \cap E_2$ est un sous espace vectoriel de E.*
- *$E_1 \cup E_2$ est un sous espace vectoriel de E si et seulement si $E_1 \subset E_2$ ou $E_2 \subset E_1$.*

Démonstration :
1) Montrons que $E_1 \cap E_2$ est un sous espace vectoriel de E.

a) Comme E_1 et E_2 sont des sous espaces vectoriels de E, alors $\overrightarrow{0}$ appartient à E_1 et à E_2, donc $\overrightarrow{0} \in E_1 \cap E_2$.

b) Soient $\overrightarrow{x},\ \overrightarrow{y} \in E_1 \cap E_2$ et $\alpha,\ \beta \in \mathbb{K}$, comme E_1 et E_2 sont des sous espaces vectoriels de E, alors

$$(\alpha\,\overrightarrow{x} + \beta\,\overrightarrow{y} \in E_1) \quad et \quad (\alpha\,\overrightarrow{x} + \beta\,\overrightarrow{y} \in E_2)$$

donc

$$\alpha\,\overrightarrow{x} + \beta\,\overrightarrow{y} \in E_1 \cap E_2$$

De **a)** et **b)** on déduit que $E_1 \cap E_2$ est un sous espace vectoriel de E.

2) D'apès la caractérisation des sous espaces vectoriels, pour que $E_1 \cup E_2$ soit un sous espace vectoriel de E il faut qu'il soit un sous groupe de $(E, +)$ ce qui n'est vrai que si $E_1 \subset E_2$ ou $E_2 \subset E_1$, ce qui justifie la deuxième propriété de notre proposition. □

5.2.2 Combinaisons linéaires

Proposition 5.6 *Soient $(E, +, \bullet)$ un $\mathbb{K}$-espace vectoriel, E_1, E_2 deux sous espaces vectoriels de E et $\alpha \in \mathbb{K}$, alors $E_1 + E_2$ et αE_1 sont des sous espaces vectoriels de E, avec*

$$\begin{aligned} E_1 + E_2 &= \{\overrightarrow{x} \in E,\ \exists \overrightarrow{x}_1 \in E_1,\ \exists \overrightarrow{x}_2 \in E_2;\ \overrightarrow{x} = \overrightarrow{x}_1 + \overrightarrow{x}_2\} \\ \alpha E_1 &= \{\overrightarrow{x} \in E,\ \exists \overrightarrow{x}_1 \in E_1;\quad \overrightarrow{x} = \alpha\,\overrightarrow{x}_1\} \end{aligned}$$

La preuve de cette proposition est immédiate et on déduit :

$$\forall\, \alpha,\ \beta \in \mathbb{K}, \qquad \alpha E_1 + \beta E_2 \quad \text{est un sous espace vectoriel de } E.$$

Définition 5.4 [3] Soit B une partie non vide d'un $\mathbb{K}$-espace vectoriel E. On appelle combinaison linéaire d'élélements de B tout élément de la forme $\alpha_1 \overrightarrow{x}_1 + \alpha_2 \overrightarrow{x}_2 + \ \ldots\ + \ \alpha_n \overrightarrow{x}_n$, où $(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n$ et $(\overrightarrow{x}_1,\ \ldots,\ \overrightarrow{x}_n) \in E^n$.

Exemple : Soient $\overrightarrow{u} = (1, 2, -1)$, $\overrightarrow{v} = (-1, 0, 1) \in \mathbb{R}^3$, montrer que le vecteur $\overrightarrow{w} = (1, 4, -1)$ est une combinaison linéaire des vecteurs $\overrightarrow{u}$ et $\overrightarrow{v}$.
Pour cela on résout l'équation : $\alpha \overrightarrow{u} + \beta \overrightarrow{v} = \overrightarrow{w}$ (*)
or

$$\begin{array}{rcl}
(*) & \Longleftrightarrow & \alpha(1, 2, -1) + \beta(-1, 0, 1) = (1, 4, -1) \\
& \Longleftrightarrow & (\alpha - \beta, 2\alpha, -\alpha + \beta) = (1, 4, -1) \\
& \Longleftrightarrow & \left\{ \begin{array}{l} \alpha - \beta = 1 \\ 2\alpha = 4 \\ -\alpha + \beta = -1 \end{array} \right. \\
& \Longleftrightarrow & \alpha = 2, \quad \beta = 1
\end{array}$$

donc

$$\overrightarrow{w} = 2\overrightarrow{u} + 1\overrightarrow{v}$$

ce qui montre que $\overrightarrow{w}$ est une combinaison linéaire de $\overrightarrow{u}$ et $\overrightarrow{v}$. □

Définition 5.5 *Soit A une partie non vide d'un $\mathbb{K}$-espace vectoriel E. On appelle espace vectoriel engendré par A l'ensemble $[A]$ de toutes les combinaisons linéaires d'éléments de A.*

Proposition 5.7 *$[A]$ est le plus petit sous espace vectoriel de E contenent A.*

Démonstration :

I) $[A]$ est un sous espace vectoriel de E, car :

1. A étant non vide, alors il existe au moin un $\overrightarrow{x}$ dans A, donc

$$\overrightarrow{0} = 0\overrightarrow{x}$$

ce qui montre que $\overrightarrow{0} \in A$.

2. Soient $\alpha,\ \beta \in \mathbb{K}$ et $\overrightarrow{x},\ \overrightarrow{y} \in [A]$, alors :

$$\left\{ \begin{array}{l}
\overrightarrow{x} \in [A] \implies \exists \gamma_1,\ \ldots,\ \gamma_k \in \mathbb{K},\ \exists \overrightarrow{x}_1,\ \ldots,\ \overrightarrow{x}_k \in A; \quad \overrightarrow{x} = \gamma_1 \overrightarrow{x}_1 \ + \ \ldots \ + \ \gamma_k \overrightarrow{x}_k \\
\\
\overrightarrow{y} \in [A] \implies \exists \delta_1,\ \ldots,\ \delta_m \in \mathbb{K},\ \exists \overrightarrow{y}_1,\ \ldots,\ \overrightarrow{y}_m \in A; \quad \overrightarrow{y} = \delta_1 \overrightarrow{y}_1 \ + \ \ldots \ + \ \delta_m \overrightarrow{y}_m
\end{array} \right.$$

donc :

$$\begin{array}{rcl}
\alpha \overrightarrow{x} + \beta \overrightarrow{y} & = & \alpha(\gamma_1 \overrightarrow{x}_1 \ + \ \ldots \ + \ \gamma_k \overrightarrow{x}_k) + \beta(\delta_1 \overrightarrow{y}_1 \ + \ \ldots \ + \ \delta_m \overrightarrow{y}_m) \\
& = & \alpha\gamma_1 \overrightarrow{x}_1 \ + \ \ldots \ + \ \alpha\gamma_k \overrightarrow{x}_k + \beta\delta_1 \overrightarrow{y}_1 \ + \ \ldots \ + \ \beta\delta_m \overrightarrow{y}_m)
\end{array}$$

en posant

$$\begin{array}{llll}
Pour & i \in \{1, \ldots, k\}, & \alpha\gamma_i = \omega_i & et \quad \overrightarrow{x}_i = \overrightarrow{u}_i \\
Pour & i \in \{1, \ldots, m\}, & \alpha\delta_i = \omega_{i+k} & et \quad \overrightarrow{y}_i = \overrightarrow{u}_{i+k}
\end{array}$$

[3] Le n est un entier naturel arbitraire non nul.

on obtient

$$\alpha\overrightarrow{x}+\beta\overrightarrow{y}=\omega_1\overrightarrow{u}_1+\ \ldots\ +\omega_{k+m}\overrightarrow{u}_{k+m}$$

avec $\overrightarrow{u}_1,\ \ldots\ \overrightarrow{u}_{k+m}\in A$, ce qui montre que

$$\alpha\overrightarrow{x}+\beta\overrightarrow{y}\in[A].$$

De **1.** et **2.** on déduit que $[A]$ est un sous espace vectoriel de E.

II) $[A]$ est le plus petit sous espace vectoriel de E qui contient A.
En effet : Si F est un sous espace vectoriel de E qui contient A, alors de la propriété SV2. de la caractérisation des sous espaces vectoriels on déduit que toute combinaison linéaire d'éléments de F est dans F, en particulier toute combinaison linéaire d'éléments de $A\subset F$ est dans F, ce qui montre que $[A]\subset F$. □

Proposition 5.8 *Si E_1 et E_2 sont deux sous espaces vectoriels de E, alors*

$$[E_1\cup E_2]=E_1+E_2$$

Démonstration : Soit $\overrightarrow{x}\in E$, alors

$$\overrightarrow{x}\in[E_1\cup E_2]\Longleftrightarrow\exists\alpha_1,\ldots,\alpha_k\in\mathbb{K},\ \exists\overrightarrow{x}_1,\ldots,\overrightarrow{x}_k\in E_1\cup E_2;\quad\overrightarrow{x}=\alpha_1\overrightarrow{x}_1,\ldots,\alpha_k\overrightarrow{x}_k$$

Parmi ces k vecteurs, il existe un certain nombre $m\in\mathbb{N}$ d'entre eux qui sont dans E_1 et les autres sont dans E_2, donc

$$\overrightarrow{x}=(\beta_1\overrightarrow{y}_1+\ldots+\beta_m\overrightarrow{y}_m)+(\beta_{m+1}\overrightarrow{y}_{m+1}+\ldots+\beta_k\overrightarrow{y}_k)$$

avec $\overrightarrow{y}_1,\ldots,\overrightarrow{y}_m\in E_1$ et $\overrightarrow{y}_{m+1},\ldots,\overrightarrow{y}_k\in E_2$. Comme E_1 et E_2 sont des sous espaces vectoriels on déduit que

$$\overrightarrow{x}=\overrightarrow{u}_1+\overrightarrow{u}_2$$

avec $\overrightarrow{u}_1=\beta_1\overrightarrow{y}_1+\ldots+\beta_m\overrightarrow{y}_m\in E_1$ et $\overrightarrow{u}_2=\beta_{m+1}\overrightarrow{y}_{m+1}+\ldots+\beta_k\overrightarrow{y}_k\in E_2$, donc :

$$[E_1\cup E_2]\subset E_1+E_2.$$

Inversement, si $\overrightarrow{x}\in E_1+E_2$, alors il existe $\overrightarrow{x}_1\in E_1,\ \overrightarrow{x}_2\in E_2$ tels que

$$\overrightarrow{x}=\overrightarrow{x}_1+\overrightarrow{x}_2$$

donc

$$\overrightarrow{x}=1.\overrightarrow{x}_1+1.\overrightarrow{x}_2$$

avec $\overrightarrow{x}_1,\ \overrightarrow{x}_2\in E_1\cup E_2$, ce qui montre que $\overrightarrow{x}\in[E_1\cup E_2]$ donc

$$E_1+E_2\subset[E_1\cup E_2]$$

ce qui termine la preuve de la proposition. □

Proposition 5.9 *Si $E_1=[A_1]$ et $E_2=[A_2]$, alors*

$$[E_1\cup E_2]=[A_1\cup A_2]$$

Démonstration : on montre facilement que

$$[A_1\cup A_2]=[A_1]+[A_2]$$

et en utilisant la proposition précédente on conclu. □

5.2.3 Sous-espaces vectoriels supplémentaires

Définition 5.6 *On dit que deux sous espaces vectoriels E_1 et E_2 de E sont supplémentaires dans E si :*

1. $E_1 \cap E_2 = \{\overrightarrow{0}\}$

2. $E_1 + E_2 = E$.

On note alors :

$$E = E_1 \oplus E_2$$

et on dit que E est la somme directe de E_1 et E_2.

Exemple : Soit $E = \mathbb{R}_3[X]$ le $\mathbb{R}$-espace vectoriel des polynômes à coefficients réels de degré inférieur ou égal à 3, $E_1 = \mathbb{R}_2[X]$ et $E_2 = \{P \in \mathbb{R}_3[X];\ \exists \gamma \in \mathbb{R},\ P(X) = \gamma X^3\}$, alors :

1. $E_1 \cap E_2 = \{0\}$, car si $P \in E_1 \cap E_2$ alors

$$\exists a,\ b,\ c,\ \gamma \in \mathbb{R}; \qquad \Big(P(X) = a + bX + cX^2\Big) \wedge \Big(P(X) = \gamma X^3\Big)$$

donc $\gamma X^3 = a + bX + cX^2$ et en prenant des valeurs particulière de X (exemple $X = 0,\ 1,\ 2, 3$ on obtient un système d'équations linéaires dont la seule solution est $a = b = c = \gamma = 0$, ce qui montre que $E_1 \cap E_2 = \{0\}$.

2. $E_1 + E_2 = \mathbb{R}_3[X]$ est évident.

De **1.** et **2.** on déduit que : $\mathbb{R}_3[X] = E_1 \oplus E_2$. □

Théorème 5.1 *Les trois assertions suivantes sont équivalentes :*

i) E_1 *et* E_2 *sont supplémentaires dans* E.

ii) $\forall \overrightarrow{x} \in E,\ \exists! \overrightarrow{x}_2 \in E_1,\ \exists! \overrightarrow{x}_2 \in E_2, \quad \overrightarrow{x} = \overrightarrow{x}_1 + \overrightarrow{x}_2$.

iii) $\Big(E_1 + E_2 = E\Big) \wedge \Big(\forall \overrightarrow{x}_1 \in E_1,\ \forall \overrightarrow{x}_2 \in E_2, \quad [\overrightarrow{x}_1 + \overrightarrow{x}_2 = \overrightarrow{0}] \Longrightarrow [\overrightarrow{x}_1 = \overrightarrow{x}_2 = \overrightarrow{0}]\Big)$.

Démonstration : On va montrer que $i) \Longrightarrow ii) \Longrightarrow iii) \Longrightarrow i)$.

$i) \Longrightarrow ii)$

Supposons que E_1 et E_2 sont supplémentaires dans E.
Soit $\overrightarrow{x} \in E$ alors il existe $\overrightarrow{x}_1 \in E_1,\ \overrightarrow{x}_2 \in E_2$ tels que

$$\overrightarrow{x} = \overrightarrow{x}_1 + \overrightarrow{x}_2$$

Montrons l'unicité des $\overrightarrow{x}_i$.
Soient $\overrightarrow{y}_1 \in E_1,\ \overrightarrow{y}_2 \in E_2$ tels que

$$\overrightarrow{x} = \overrightarrow{y}_1 + \overrightarrow{y}_2$$

donc

$$\overrightarrow{0} = \overrightarrow{x} - \overrightarrow{x} = (\overrightarrow{x}_1 - \overrightarrow{y}_1) + (\overrightarrow{x}_2 - \overrightarrow{y}_2)$$

E_1 et E_2 étant des sous espaces vectoriels alors

$$E_2 \ni (\overrightarrow{x}_2 - \overrightarrow{y}_2) = (\overrightarrow{x}_1 - \overrightarrow{y}_1) \in E_1$$

et comme E_1 et E_2 sont supplémentaires, alors $E_1 \cap E_2 = \{\overrightarrow{0}\}$ et

$$(\overrightarrow{x}_2 - \overrightarrow{y}_2) = (\overrightarrow{x}_1 - \overrightarrow{y}_1) = \overrightarrow{0}$$

ce qui montre que $\overrightarrow{x}_2 = \overrightarrow{y}_2$ et $\overrightarrow{x}_1 = \overrightarrow{y}_1$, donc l'unicité de $\overrightarrow{x}_1$ et $\overrightarrow{x}_2$.

ii) $\Longrightarrow$ *iii)*
Supposons que

$$\forall\, \overrightarrow{x} \in E,\ \exists!\, \overrightarrow{x}_2 \in E_1,\ \exists!\, \overrightarrow{x}_2 \in E_2, \quad \overrightarrow{x} = \overrightarrow{x}_1 + \overrightarrow{x}_2.$$

Il est claire que d'ici on déduit $E = E_1 + E_2$.
Montrons que

$$\forall \overrightarrow{x}_1 \in E_1,\ \forall \overrightarrow{x}_2 \in E_2, \quad \left(\overrightarrow{x}_1 + \overrightarrow{x}_2 = \overrightarrow{0} \Longrightarrow \overrightarrow{x}_1 = \overrightarrow{x}_2 = \overrightarrow{0}\right).$$

Soient $\overrightarrow{x}_1 \in E_1$ et $\overrightarrow{x}_2 \in E_2$ tels que $\overrightarrow{x}_1 + \overrightarrow{x}_2 = \overrightarrow{0}$, comme $\overrightarrow{0} = \overrightarrow{0} + \overrightarrow{0}$, de l'unicité de $\overrightarrow{x}_1$ et $\overrightarrow{x}_2$ supposée dans *i)* on déduit que $\overrightarrow{x}_1 = \overrightarrow{x}_2 = \overrightarrow{0}$.

iii) $\Longrightarrow$ *i)*
Supposons que :

$$\left(E_1 + E_2 = E\ \right) \wedge \left(\forall \overrightarrow{x}_1 \in E_1,\ \forall \overrightarrow{x}_2 \in E_2, \quad [\overrightarrow{x}_1 + \overrightarrow{x}_2 = \overrightarrow{0}] \Longrightarrow [\overrightarrow{x}_1 = \overrightarrow{x}_2 = \overrightarrow{0}]\ \right).$$

Pour montrer que E_1 et E_2 sont supplémentaires il suffit de montrer que $E_1 \cap E_2 = \{\overrightarrow{0}\}$.
Soit $\overrightarrow{x} \in E_1 \cap E_2$, alors $\overrightarrow{0} = \overrightarrow{x} + (-\overrightarrow{x})$ avec $\overrightarrow{x} \in E_1$ et $(-\overrightarrow{x}) \in E_2$, de la deuxième partie de *iii)* on déduit que $\overrightarrow{x} = -\overrightarrow{x} = \overrightarrow{0}$, ce qui montre que $E_1 \cap E_2 = \{\overrightarrow{0}\}$.

□

Remarque 5.2 *Il est à remarquer que le supplémentaire d'un sous espace vectoriel propre n'est pas unique. Pour s'en convaincre, soit dans* $\mathbb{R}^3$ *les sous espaces vectoriels :*

$$F = \left\{(x,y,z) \in \mathbb{R}^3;\ x = y \text{ et } z = 0\right\},\ F_1 = \left\{(x,y,z) \in \mathbb{R}^3;\ x = -y\ \right\} \text{ et } F_2 = \left\{(x,y,z) \in \mathbb{R}^3;\ x = 0\ \right\},$$

alors

$$\mathbb{R}^3 = F \oplus F_1 \qquad \text{et} \qquad \mathbb{R}^3 = F \oplus F_2$$

5.2.4 Sommes directes de sous-espaces vectoriels

Définition 5.7 *On dit que E est la somme directe des sous-espaces vectoriels E_1, E_2, $\ldots E_n$ si*

$$\forall \overrightarrow{x} \in E,\ \exists!\, \overrightarrow{x}_1 \in E_1,\ \exists!\, \overrightarrow{x}_2 \in E_2,\ \ldots\ ,\ \exists!\, \overrightarrow{x}_n \in E_n, \quad \overrightarrow{x} = \overrightarrow{x}_1 + \overrightarrow{x}_2 + \ \ldots\ + \overrightarrow{x}_n.$$

On note

$$E = E_1 \oplus E_2 \oplus \ldots \oplus E_n = \bigoplus_{i=1}^{n} E_i.$$

Exemple : Soient E et F deux $\mathbb{K}$-espaces vectoriels, alors

$$E \times F = \left(E \times \{\overrightarrow{0}_F\}\right) \bigoplus \left(\{\overrightarrow{0}_E\} \times F\right)$$

Proposition 5.10 *Soient E_1, E_2, ...E_n des sous-espaces vectoriels de E, alors*

$$E = E_1 \oplus E_2 \oplus \ldots \oplus E_n \Longleftrightarrow \begin{cases} \bullet & E = E_1 + E_2 + \ldots + E_n \\ \bullet & \forall i \neq j,\ E_i \cap E_j = \{\vec{0}\} \end{cases}$$

Cette proposition se démontre comme le théorème 5.1.

5.3 Bases et Dimension d'un espace vectoriel

Soit $(E, +, \bullet)$ un $\mathbb{K}$-espace vectoriel.

5.3.1 Parties libres

Définition 5.8 *On dit que les vecteurs $\{\overrightarrow{x}_1,\ \overrightarrow{x}_2,\ \ldots,\ \overrightarrow{x}_n\}$ sont linéairement indépendants si*

$$\forall \alpha_1,\ \ldots, \alpha_n \in \mathbb{K}, \quad \alpha_1 \overrightarrow{x}_1 + \ \ldots + \alpha_n \overrightarrow{x}_n = \overrightarrow{0} \Longrightarrow \alpha_1 = \ldots = \alpha_n = 0$$

Sinon, on dit qu'ils sont linéairement dépendants ou qu'ils sonts liés.

Définition 5.9 *On dit qu'une partie non vide $\mathcal{L} \subset E$ est libre si toute partie finie L de $\mathcal{L}$ est libre. Si $\mathcal{L}$ n'est pas libre, on dit que c'est une partie liée.*

Exemples :

1. $\{1,\ X,\ X^2,\ \ldots, X^n\}$ est une partie libre de $\mathbb{K}[X]$ et $\{X,\ X + X^2,\ X^2,\ \ldots, X^n\}$ est liée.
2. $\{(1,0,0),\ (0,5,0),\ (0,0,2)\}$ est une partie libre de $\mathbb{K}^3$

Preuve :

1. $\{X,\ X^2,\ \ldots, X^n\}$ est une partie libre de $\mathbb{K}[X]$, car : pour tout $\alpha_1,\ \ldots,\ \alpha_n \in \mathbb{K}$ si

(**) $\qquad \alpha_0 + \alpha_1 X + \ \ldots + \ \alpha_n X^n = 0_{\mathbb{K}},$

pour $X = 0_{\mathbb{K}}$ on obtient $\alpha_0 = 0$ et (**) devient

$$\alpha_1 X + \ \alpha_2 X^2 + \ \ldots + \ \alpha_n X^n = 0_{\mathbb{K}}$$

En prenant les dérivées des deux membres de cette identité on obtient

(***) $\qquad \alpha_1 + \ 2\alpha_2 X + \ \ldots + \ n\alpha_n X^{n-1} = 0_{\mathbb{K}}$

pour $X = 0_{\mathbb{K}}$ on obtient $\alpha_1 = 0_{\mathbb{K}}$ et (***) devient

$$2\alpha_2 X + 3\alpha_3 X^2 + \ \ldots \ + n\alpha_n X^n = 0_{\mathbb{K}}$$

et de proche en proche on obtient $\alpha_0 = \alpha_1 = \ \ldots \ = \alpha_n = 0_{\mathbb{K}}$, donc $\{X,\ X^2,\ \ldots, X^n\}$ est une partie libre de $\mathbb{K}[X]$.

2. La partie $\{X,\ X+X^2,\ X^2,\ \ldots, X^n\}$ est liée, car $X-(X+X^2)+X^2=0$ donc

$$\exists \alpha=1_{\mathbb{K}},\ \beta=-1_{\mathbb{K}},\ \gamma=1_{\mathbb{K}}\in\mathbb{K}^*;\qquad \alpha X+\beta(X+X^2)+\gamma X^2=0$$

ce qui montre que $\{X,\ (X+X^2),\ X^2\}$ est une partie liée de $\{X,\ X+X^2,\ X^2,\ \ldots, X^n\}$, donc cette dernière est aussi liée.

3. $\{(1,0,0),\ (0,5,0),\ (0,0,2)\}$ est une partie libre de $\mathbb{K}^3$, car pour tous $\alpha,\ \beta,\ \gamma\in\mathbb{K}$,

$$\begin{aligned}\alpha(1,0,0)+\ \beta(0,5,0)+\ \gamma(0,0,2)=(0,0,0) &\iff (\alpha,5\beta,2\gamma)=(0,0,0)\\ &\iff \begin{cases}\alpha=0\\ 5\beta=0\\ 2\gamma=0\end{cases}\\ &\iff \alpha=\beta=\gamma=0\end{aligned}$$

ce qui montre que $\{(1,0,0),\ (0,5,0),\ (0,0,2)\}$ est une partie libre de $\mathbb{K}^3$.

Propriété 5.2 *Soit $\mathcal{L}$ une partie non vide d'un espace vectoriel E.*
- *Si $\mathcal{L}$ est libre alors toute partie non vide de $\mathcal{L}$ est libre.*
- *Si $\mathcal{L}$ est liée, alors toute partie L contenant $\mathcal{L}$ est liée.*
- *Si $\overrightarrow{0}\in\mathcal{L}$, alors $\mathcal{L}$ est liée.*

5.3.2 Parties génératrices

Définition 5.10 *On dit qu'une partie non vide G de E est une partie génératrice de E si E est engendré par G, c'est-à-dire $E=[G]$.*
On dit aussi que G est un générateur de E ou que G engendre E.

Exemples :
1. $\{1,\ (X-1),\ X^2,\ \ldots,\ X^n\}$ est une partie génératrice de $\mathbb{K}_n[X]$.
2. $\{(0,1,0),\ (2,0,1),\ (0,0,6)\}$ est une partie génératrice de $\mathbb{K}^3$.

1. Soit $P\in\mathbb{K}_n[X]$, alors il existe $a_0,\ a_1,\ \ldots\ ,\ a_n\in\mathbb{K}$ tels que :

$$P(X)=a_0+a_1X+\ \ldots\ +a_nX^n$$

Soient $\alpha_0,\ \alpha_1,\ \ldots\ ,\ \alpha_n\in\mathbb{K}$, alors

$$\begin{aligned}P(X)=\alpha_0\ +\ \alpha_1X\ +\ \ldots\ +\ \alpha_nX^n \iff&\\ \iff\ \alpha_0\ +\ \alpha_1(X-1)\ +\ \ldots\ +\ \alpha_nX^n&=a_0+a_1X+\ \ldots\ +a_nX^n\\ \iff\ (\alpha_0\ -\ \alpha_1)+\ \alpha_1X\ +\ \ldots\ +\ \alpha_nX^n&=a_0+a_1X+\ \ldots\ +a_nX^n\\ \iff\ &\begin{cases}\alpha_0-\alpha_1=a_0\\ \alpha_1=a_1\\ \vdots\\ \alpha_n=a_n\end{cases}\\ \iff\ &\begin{cases}\alpha_0=a_0+a_1\\ \alpha_1=a_1\\ \vdots\\ \alpha_n=a_n\end{cases}\end{aligned}$$

donc :

$$\forall\, P \in \mathbb{K}_n[X],\ \exists \alpha_0,\ \ldots\ ,\ \alpha_n \in \mathbb{K};\quad P(X) = \alpha_0\ +\ \alpha_1\,(X-1)\ +\ \ldots\ +\ \alpha_n X^n$$

ce qui montre que $\{1,\ (X-1),\ X^2,\ \ldots,\ X^n\}$ est une partie génératrice de $\mathbb{K}_n[X]$.

2. Soient $\overrightarrow{X} = (x, y, z) \in \mathbb{K}^3$ et $\alpha,\ \beta,\ \gamma \in \mathbb{K}$, alors

$$\begin{aligned}
\overrightarrow{X} = \alpha(0,1,0) + \beta(2,0,1) + \gamma(0,0,6) \quad &\Longleftrightarrow \quad (x,y,z) = (2\beta, \alpha, \beta + 6\gamma) \\
&\Longleftrightarrow \quad \begin{cases} 2\beta = x \\ \alpha = y \\ \beta + 6\gamma = z \end{cases} \\
&\Longleftrightarrow \quad \begin{cases} \beta = x/2 \\ \alpha = y \\ \beta + 6\gamma = (2z - x)/12 \end{cases}
\end{aligned}$$

ce qui montre que $\{(0,1,0),\ (2,0,1),\ (0,0,6)\}$ est une partie génératrice de $\mathbb{K}^3$. □

Propriété 5.3 *Soit G est une partie non vide de E,*
- *Si G est une partie génératrice de E, il en sera de même de toute partie de E contenant G.*
- *Si G n'engendre pas E, il en sera de même de toute partie non vide de G.*

5.3.3 Dimension et bases d'un espace vectoriel

Soit $(E, +, \bullet)$ un $\mathbb{K}$-espace vectoriel, avec Card$E > 1$.

Définition 5.11 *On dit que E est un espace vectoriel de dimension finie s'il peut être engendré par une partie finie. Dans ce cas, on appelle dimension de E le nombre naturel*

$$n = \dim\ E = \inf\{\text{Card}G,\ G \in \mathcal{G}\},$$

où $\mathcal{G}$ est l'ensemble de tous les générateurs de E.

Définition 5.12 *Si E n'admet pas de générateur fini, on dit que E est de dimension infinie et on écrit*

$$\dim\ E = +\infty.$$

Convention : $F = \{\overrightarrow{0}\}$ est un espace vectoriel de dimension 0.

Exemple : L'espace vectoriel $\mathbb{K}[X]$, des polynômes à coefficients dans $\mathbb{K}$, est un espace vectoriel de dimension infinie.

Dans notre cours on se limitera au cas des espaces vectoriels de dimensions finies.

Définition 5.13 *Soit B une partie non vide de E, on dit que B est une base de E si tout vecteur non nul de E s'écrit comme combinaison linéaire unique d'éléments de B.*

Formellement, B base de E si

$$\forall \overrightarrow{x} \in E\backslash\{\overrightarrow{0}\},\ \exists!\ \overrightarrow{x}_1,\ \ldots,\overrightarrow{x}_n \in B, \exists!\ \alpha_1,\ \ldots,\alpha_n \in (\mathbb{K}^*)^n\,;\ \ \overrightarrow{x} = \alpha_1\overrightarrow{x}_1 + \ \ldots\ + \alpha_n\overrightarrow{x}_n$$

Proposition 5.11 *Toute partie B de E contenant $\overrightarrow{0} \in B$ n'est pas une base de E.*

Démonstration : Soit $\overrightarrow{x}$, si B est une base de E, alors il existe $\overrightarrow{x}_1,\ \ldots,\overrightarrow{x}_n \in B$ et $\alpha_1,\ \ldots,\alpha_n \in (\mathbb{K}^*)^n$ tels que

$$\overrightarrow{x} = \alpha_1\overrightarrow{x}_1 + \ \ldots\ + \alpha_n\overrightarrow{x}_n$$

et pour tout $\alpha_{n+1} \in (\mathbb{K}^*)^n$, en posant $\overrightarrow{0} = \overrightarrow{x}_{n+1}$, on a

$$\overrightarrow{x} = \alpha_1\overrightarrow{x}_1 + \ \ldots\ + \alpha_n\overrightarrow{x}_n + \alpha_{n+1}\overrightarrow{x}_{n+1}$$

ce qui contredit l'unicité de la décomposition de $\overrightarrow{x}$ dans B, donc B n'est pas une base de E. □

Exemple : $B = \{(1,0,0),(0,1,0),(0,0,1)\}$ est une base de $\mathbb{R}^3$. En effet, soit $\overrightarrow{X} = (x_1,x_2,x_3) \in \mathbb{R}^3$ et $\alpha,\ \beta,\ \gamma \in \mathbb{R}$, alors

$$\begin{array}{rcl}\overrightarrow{X} = \alpha(1,0,0) + \beta(0,1,0) + \gamma(0,0,1) & \Longleftrightarrow & (x_1,x_2,x_3) = (\alpha,\beta,\gamma)) \\ & \Longleftrightarrow & \begin{cases}\alpha = x_1\\ \beta = x_2\\ \gamma = x_3\end{cases}\end{array}$$

donc : $\forall\ \overrightarrow{X} = (x_1,x_2,x_3) \in \mathbb{R}^3,\ \ \exists!\alpha = x_1,\ \beta = x_2,\ \gamma = x_3 \in \mathbb{R}\,;$

$$\overrightarrow{X} = \alpha(1,0,0) + \beta(0,1,0) + \gamma(0,0,1)$$

ce qui montre que $B = \{(1,0,0),(0,1,0),(0,0,1)\}$ est une base de $\mathbb{R}^3$.

D'une manière générale on a

Propriété 5.4 *Soit $n \in \mathbb{N}^*$, $B = \{\overrightarrow{e}_1,\ \ldots,\ \overrightarrow{e}_n\}$, avec $\overrightarrow{e}_j$ le n-uple dont tous les éléments sont nuls sauf le j-ième est égal à $1_{\mathbb{K}}$, alors B est une base de $\mathbb{K}^n$, appelée* base canonique de $\mathbb{K}^n$.

Exemple : Donner une base de l'espace vectoriel $E = \{(x,y,z) \in \mathbb{R}^3;\ 2x - y = 0\}$.
Soit $\overrightarrow{X} \in \mathbb{R}^3$, alors il existe $x,\ y,\ z \in \mathbb{R}$ uniques tels que $\overrightarrow{X} = (x,y,z)$, donc :

$$\begin{array}{rcl}\overrightarrow{X} \in E & \Longleftrightarrow & \Big(\overrightarrow{X} = (x,y,z)\Big) \wedge \Big(2x - y = 0\Big) \\ & \Longleftrightarrow & \Big(\overrightarrow{X} = (x,y,z)\Big) \wedge \Big(y = 2x\Big) \\ & \Longleftrightarrow & \overrightarrow{X} = (x,2x,z) \\ & \Longleftrightarrow & \overrightarrow{X} = x(1,2,0) + z(0,0,1)\end{array}$$

d'où on déduit

$$\forall\, \overrightarrow{X} \in E, \quad \exists!\, x,\ z \in \mathbb{R};\ \overrightarrow{X} = x(1,2,0) + z(0,0,1)$$

ce qui montre que $B = \{(1,2,0),\ (0,0,1)\}$ est une base de E.

□

Proposition 5.12 *Soit B une partie de E, alors B est une base si et seulement si B est une partie libre et génératrice de E.*

Démonstration :

$\Longrightarrow$?

Supposons que B est une base de E, alors d'après la définition 5.14 B est une partie génératrice de E, montrons que B est libre.
Soient $\overrightarrow{x}_1,\ \ldots,\ \overrightarrow{x}_n, \in B$ et $\alpha_1,\ \ldots,\ \alpha_n \in \mathbb{K}$ tels que

$$\alpha_1 \overrightarrow{x}_1 + \ \ldots + \ \alpha_n \overrightarrow{x}_n = \overrightarrow{0}$$

comme

$$0\overrightarrow{x}_1 \ + \ \ldots \ + \ 0\overrightarrow{x}_n = \overrightarrow{0}$$

de l'unicité de la décomposition de $\overrightarrow{0}$ on déduit que $\alpha_1 = \ \ldots = \ \alpha_n = 0_{\mathbb{K}}$, ce qui montre que B est libre.

$\Longleftarrow$?

Inversement, on suppose que B est une partie libre et génératrice de E et montrons que B est une base de E.
Soit $\overrightarrow{x} \in E\backslash\{\overrightarrow{0}\}$, comme B engendre E alors :

$$\exists \overrightarrow{x}_1,\ \ldots,\ \overrightarrow{x}_n \in B,\ \ \exists \alpha_1,\ \ldots,\ \alpha_n \in \mathbb{K}^*; \qquad \overrightarrow{x} = \alpha_1 \overrightarrow{x}_1 + \ \ldots + \ \alpha_n \overrightarrow{x}_n$$

Montrons que les α_j sont uniques. Soient $\beta_1,\ \ldots,\ \beta_n \in \mathbb{K}^*$ tels que

$$\overrightarrow{x} = \beta_1 \overrightarrow{x}_1 + \ \ldots + \ \beta_n \overrightarrow{x}_n$$

en faisant la soustraction entre les deux écritures de $\overrightarrow{x}$ on trouve

$$(\alpha_1 - \beta_1)\overrightarrow{x}_1 + \ \ldots + \ (\alpha_n - \beta_n)\overrightarrow{x}_n = \overrightarrow{0}$$

et comme B est libre, on déduit que $\alpha_1 = \beta_1,\ \ldots,\ \alpha_n = \beta_n$, ce qui montre l'unicité des α_j.
De la même manière on déduit l'unicité des $\overrightarrow{x}_j$ en montrant que les coefficients des $\overrightarrow{y}_j$ qui ne sont pas parmi les $\overrightarrow{x}_j$ sont nuls dans toute écriture de $\overrightarrow{x}$.

□

5.3.4 Théorème de la base incomplète

Proposition 5.13 *Soit E un espace vectoriel de dimension n et G une partie non vide de E, alors*

$$\text{Card}G < n \Longrightarrow G \text{ n'engendre pas } E$$

Démonstration : D'après la définition 5.11 de la dimension d'un espace vectoriel, on a :

$$G \text{ engendre } E \Longrightarrow \text{Card}G \geq n$$

en prenant la contarposée de cette implication on obtient la proposition. □

Proposition 5.14 *Soit E un espace vectoriel de dimension $n \in \mathbb{N}^*$, alors il existe au moins une base B de E de cardinal n.*

Démonstration : E étant de dimension n, alors il existe au moins une partie $B = \{\overrightarrow{e}_1, \ldots, \overrightarrow{e}_n\}$ qui engendre E. Montrons que B est libre.
Supposons que B est liée, alors il existe $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$, non tous nuls tels que :

$$\alpha_1 \overrightarrow{e}_1 + \ \ldots \ + \alpha_n \overrightarrow{e}_n = \overrightarrow{0}$$

si $\alpha_j \neq 0$, alors en divisant cette équation par α_j on exprime $\overrightarrow{e}_j$ comme combinaison linéaire des $(n-1)$ autres vecteurs et comme B est une partie génératrice de E on déduit que $B\backslash\{\overrightarrow{e}_j\}$ est une partie génératrice de E et vu que

$$\text{Card}B\backslash\{\overrightarrow{e}_j\} = n - 1 < n,$$

on tombe en contradiction avec le resultat de la proposition 5.13 donc notre supposition est fausse, c'est à dire : B est libre. □

D'après cette démonstration, on a la proposition suivante :

Proposition 5.15 *Soit E un espace vectoriel de dimension n, alors toute partie génératrice de E de cardinal n est une base de E.*

En dimension quelconque, cette proposition peut être exprimée comme suit :

Une base est une partie génératrice minimale de E

Proposition 5.16 *Soient E un espace vectoriel de dimension $n \in \mathbb{N}^*$ et G une partie de E, alors*

$$\text{Card}G \geq n + 1 \Longrightarrow G \text{ est liée.}$$

Démonstration : Il suffit de montrer que toute partie de $E\backslash\{\overrightarrow{0}\}$ de cadinal $n+1$ est liée. On fera la démonstration pour $n=1$ et 2 et par analogie on donnera la démonstration pour n quelconque.

a. Pour $n=1$.
Soit $G=\{\overrightarrow{f}_1,\ \overrightarrow{f}_2\}\subset E$. D'après la proposition 5.14, il existe $B=\{\overrightarrow{e}\}$ une base de E, donc :

$$\exists a,\ b\in\mathbb{K};\quad \left(\overrightarrow{f}_1=a\overrightarrow{e}\right)\wedge\left(\overrightarrow{f}_2=b\overrightarrow{e}\right)$$

Montrons que G est liée. Soient $\alpha,\ \beta\in\mathbb{K}$, alors

$$\begin{array}{rcl}\alpha\overrightarrow{f}_1+\beta\overrightarrow{f}_2=\overrightarrow{0} & \Longleftrightarrow & \alpha a\overrightarrow{e}+\beta b\overrightarrow{=}\overrightarrow{0}\\ & \Longleftrightarrow & (\alpha a+\beta b)\overrightarrow{e}=\overrightarrow{0}\\ & \Longleftrightarrow & (\alpha a+\beta b)=0\end{array}$$

comme la dernière équation admet une infinité de solutions, ceci montre que G est une partie liée.

b. Pour $n=2$.
Soit $G=\{\overrightarrow{f}_1,\ \overrightarrow{f}_2,\ \overrightarrow{f}_2\}\subset E$. D'après la proposition 5.14, il existe $B=\{\overrightarrow{e}_1,\ \overrightarrow{e}_2\}$ une base de E, donc : $\exists a_1,\ a_2,\ b_1,\ b_2,\ c_1,\ c_2\in\mathbb{K}$;

$$\left(\overrightarrow{f}_1=a_1\overrightarrow{e}_1+a_2\overrightarrow{e}_2\right)\wedge\left(\overrightarrow{f}_2=b_1\overrightarrow{e}_1+b_2\overrightarrow{e}_2\right)\wedge\left(\overrightarrow{f}_3=c_1\overrightarrow{e}_1+c_2\overrightarrow{e}_2\right)$$

Montrons que G est liée. Soient $\alpha,\ \beta,\ \gamma\in\mathbb{K}$, alors

$$\begin{array}{rcl}\alpha\overrightarrow{f}_1+\beta\overrightarrow{f}_2+\gamma\overrightarrow{f}_2=\overrightarrow{0} & \Longleftrightarrow & \alpha(a_1\overrightarrow{e}_1+a_2\overrightarrow{e}_2)+\beta(b_1\overrightarrow{e}_1+b_2\overrightarrow{e}_2)+\gamma(c_1\overrightarrow{e}_1+c_2\overrightarrow{e}_2)=\overrightarrow{0}\\ & \Longleftrightarrow & (\alpha a_1+\beta b_1+\gamma c_1)\overrightarrow{e}_1+(\alpha a_2+\beta b_2+\gamma c_2)\overrightarrow{e}_2=\overrightarrow{0}\\ & \Longleftrightarrow & \begin{cases}\alpha a_1+\beta b_1+\gamma c_1=0\\ \alpha a_2+\beta b_2+\gamma c_2=0\end{cases}\end{array}$$

comme le dernier système est sur-déterminé (2 équations et 3 inconnues $\alpha,\ \beta,\ \gamma$) alors il admet une infinité de solutions, ce qui montre que G est liée.

c. Pour n quelconque, on reprend le même schéma qui nous mènera à un système de n équations et (n+1)inconnues qui admet une infinité de solutions.

□

Comme conséquence directe de cette proposition et de la définition de la dimension, on a :

Théorème 5.2 *Toutes les bases d'un espace vectoriel de dimension n sont de cardinal n.*

Démonstration : En effet, si B est une base d'un espace vectoriel de dimension n alors B est une partie libre et génératrice de E ; en prenant la contraposée de la proposition précédente on déduit que Card $B\leq n$ et de la définition de la dimension d'un espace vectoriel on déduit que Card $B\geq n$, donc Card $B=n$.

□

Proposition 5.17 *Soit E un espace vectoriel de dimension n, alors toute partie libre de E de cardinal n est une base de E.*

Démonstration : Soit $B = \{\overrightarrow{e}_1, \ldots, \overrightarrow{e}_n\}$ une partie libre de E.
Supposons que B n'est pas une partie génératrice de E, alors il existe au moins un vecteur $\overrightarrow{e} \in E$ qui n'est pas combinaison linéaire des éléments de B, c'est à dire :

$$\forall\, \alpha_1, \ldots, \alpha_n \in \mathbb{K}, \qquad \overrightarrow{e} \neq \alpha_1 \overrightarrow{e}_1 + \ldots + \alpha_n \overrightarrow{e}_n$$

Montrons que $B' = \{\overrightarrow{e}_1, \ldots, \overrightarrow{e}_n, \overrightarrow{e}\}$ est libre.
Soient $\beta, \beta_1, \ldots, \beta_n \in \mathbb{K}$ tels que

$$\beta\overrightarrow{e} + \beta_1\overrightarrow{e}_1 + \beta_2\overrightarrow{e}_2 + \ldots + \beta_n\overrightarrow{e}_n = \overrightarrow{0}$$

1. Si $\beta = 0$, on déduit que $\beta_1\overrightarrow{e}_1 + \beta_2\overrightarrow{e}_2 + \ldots + \beta_n\overrightarrow{e}_n = \overrightarrow{0}$ et comme B est libre on déduit que $\beta_1 = \ldots = \beta_n = 0$.
2. Si $\beta \neq 0$, en multipliant par β^{-1} on obtient

$$\overrightarrow{e} = (-\beta_1\beta^{-1})\overrightarrow{e}_1 + (-\beta_2\beta^{-1})\overrightarrow{e}_2 + \ldots + (-\beta_n\beta^{-1})\overrightarrow{e}_n$$

ce qui contredit le choix de $\overrightarrow{e}$.
De **1.** et **2.** on déduit que $\beta = \beta_1 = \ldots = \beta_n = 0$, ce qui montre que B' est libre et comme $\mathrm{Card}B' = n+1$, de la proposition5.16 on déduit que B' est liée, ce qui est absurde, par conséquent notre supposition est fausse, donc B est une partie génératrice de E, par suite B est une base de E.

□

Théorème 5.3 (de la bse incomplète) *Soient E un espace vectoriel de dimension n, $B = \{\overrightarrow{e}_1, \ldots, \overrightarrow{e}_n\}$ une base de E et $\mathcal{L}$ une partie libre de E telle que* $\mathrm{Card}\mathcal{L} = m < n$*, alors on peut compléter $\mathcal{L}$ par $n-m$ vecteurs de B pour former une nouvelle base de E.*

Avant de donner la démonstration du théorème on va établir les deux résultats suivants :

Lemme 5.1 *Soient $\mathcal{L} = \{\overrightarrow{f}_1, \ldots, \overrightarrow{f}_k\}$ une partie libre de E et $\overrightarrow{e} \in E$, alors*

$$\Big((\mathcal{L} \cup \{\overrightarrow{e}\}) \ \textit{est liée}\Big) \Longrightarrow \Big(\exists\, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{K};\ \ \overrightarrow{e} = \alpha_1\overrightarrow{f}_1 + \ldots + \alpha_k\overrightarrow{f}_k\Big)$$

Démonstration : Supposons que $\mathcal{L} \cup \{\overrightarrow{e}\}$ est liée, alors il existe $\beta_1, \ldots, \beta_{k+1} \in \mathbb{K}$, non tous nuls, tels que

$$\beta_1\overrightarrow{f}_1 + \ldots + \beta_k\overrightarrow{f}_k + \beta_{k+1}\overrightarrow{e} = \overrightarrow{0}$$

alors deux cas se présentent :

1) $(\beta_{k+1} = 0) \wedge (\beta_1\overrightarrow{f}_1 + \ldots + \beta_k\overrightarrow{f}_k = \overrightarrow{0},$ avec les β_j non tous nuls).
Comme $\mathcal{L}$ est libre, ceci est impossible.

2) $(\beta_{k+1} \neq 0) \wedge (\beta_1 \overrightarrow{f}_1 + \ \ldots \ + \beta_k \overrightarrow{f}_k + \beta_{k+1} \overrightarrow{e} = \overrightarrow{0})$.
En multipliant par ${\beta_{k+1}}^{-1}$ on obtient

$$\overrightarrow{e} = \alpha_1 \overrightarrow{e}_1 + \ \ldots \ + \alpha_k \overrightarrow{e}_k$$

avec $\alpha_j = -{\beta_{k+1}}^{-1}\beta_j$, ce qui termine la preuve du lemme.

□

Lemme 5.2 *Soient $B = \{\overrightarrow{e}_1, \ \ldots, \ \overrightarrow{e}_n\}$ une base de E et $\mathcal{L} = \{\overrightarrow{f}_1, \ \ldots, \ \overrightarrow{f}_m\}$ une partie libre de E, avec $m < n$, alors il existe au moins un vecteur $\overrightarrow{e}_j \in B$ tel que $\mathcal{L} \cup \{\overrightarrow{e}_j\}$ est libre.*

Démonstration. Soient $B = \{\overrightarrow{e}_1, \ \ldots, \ \overrightarrow{e}_n\}$ une base de E et $\mathcal{L} = \{\overrightarrow{f}_1, \ \ldots, \ \overrightarrow{f}_m\}$ une partie libre de E, avec $m < n$.
Supposons que : $\forall\, j = 1, \ \ldots \ , n, \ \mathcal{L} \cup \{\overrightarrow{e}_j\}$ est liée.
D'après le lemme 5.1, les $\overrightarrow{e}_j$ sont alors des combinaisons linéaires de $\overrightarrow{f}_1, \ \ldots, \ \overrightarrow{f}_m$, et comme B engendre E on déduit que : Tout vecteur $\overrightarrow{x} \in E$ est combinaison linéaire des $\overrightarrow{e}_j$ qui sont à leur tour des combinaisons linéaires de $\overrightarrow{f}_1, \ \ldots, \ \overrightarrow{f}_m$, donc $\overrightarrow{x}$ est combinaison linéaire de $\overrightarrow{f}_1, \ \ldots, \ \overrightarrow{f}_m$, ce qui montre que $\mathcal{L} = \{\overrightarrow{f}_1, \ \ldots, \ \overrightarrow{f}_m\}$ est une partie génératrice de E de cardinal strictement inférieur à la dimension de E, ce qui est absurde, d'après la proposition 5.13, donc notre supposition est fausse et on déduit qu'il existe $\overrightarrow{e}_j \in B$ tel que $\mathcal{L} \cup \{\overrightarrow{e}_j\}$ est libre.

□

Démonstration du théorème. Soient $B = \{\overrightarrow{e}_1, \ \ldots, \ \overrightarrow{e}_n\}$ une base de E et $\mathcal{L} = \{\overrightarrow{f}_1, \ \ldots, \ \overrightarrow{f}_m\}$ une partie libre de E, avec $m < n$. En appliquant le lemme 5.2 $(n-m)$-fois on complète la partie $\mathcal{L}$; par des vecteurs de B ; en une partie libre B' de cardinal n et à l'aide de la proposition5.17 on conclut que B' est une base de E.

□

En dimension finie, on a la caractérisation suivante d'une base.

Propriété 5.5 *Soit B une partie d'un espace vectoriel E telle que* Card$B$=dim$E$, *alors les propriétés suivantes sont équivalentes :*
- *B est une base de E*
- *B est une partie génératrice de E.*
- *B est une partie libre de E*

Démonstration : C'est des aaplications des propositions 5.15 et 5.17.

□

On peut exprimer ces propriétés comme suit :

Propriété 5.6 *Dans un espace vectoriel E, une base de E est une partie libre maximale ou bien une partie génératrice minimale.*

On va dans ce qui suit faire un résumé des principales propriétés concernant les espaces vectoriels de dimension finie.

Propriété 5.7 Soit E un espace vectoriel de dimension finie n, alors

1. Le cardinal de toute base de E est égal à n.
2. Toute partie libre de E de cardinal n est une base de E.
3. Toute partie génératrice de E de cardinal n est une base de E.
4. Toute partie de E dont le cardinal est supérieur à n est liée.
5. Toute partie de E dont le cardinal est inférieur à n n'est pas génératrice de E.

5.3.5 Application aux sommes d'espaces vectoriels

Soit E un espace vectoriel de dimension finie n.

Proposition 5.18 *Tout sous espace vectoriel de E possède un sous espace supplémentaire dans E.*

Démonstration : Soit E_1 un sous espace vectoriel de E.

1. Si $E_1 = E$, alors le sous espace vectoriel supplémentaire de E_1 dans E est $E_2 = \{\overrightarrow{0}\}$.

2. Si $E_1 = \{\overrightarrow{0}\}$, alors le sous espace vectoriel supplémentaire de E_1 dans E est $E_2 = E$.

3. Si $E_1 \neq \{\overrightarrow{0}\}$ et $E_1 \neq E$, alors $0 < \dim E_1 < n$. Soit $B = \{\overrightarrow{e}_1, \ \dots \ , \overrightarrow{e}_n\}$ une base de E et $B_1 = \{\overrightarrow{f}_1, \ \dots \ , \overrightarrow{f}_m\}$ une base de E_1, alors d'après le théorème de la base incomplète 5.3 il existe $(n-m)$ vecteurs de B, qu'on notera $\overrightarrow{f}_{m+1}, \ \dots \ , \overrightarrow{f}_n$, tels que $B' = \left\{\overrightarrow{f}_1, \ \dots \ , \overrightarrow{f}_m, \overrightarrow{f}_{m+1}, \ \dots \ , \overrightarrow{f}_n\right\}$ est une base de E, alors :

$E_2 = \left[\{\overrightarrow{f}_{m+1}, \ \dots \ , \overrightarrow{f}_n\}\right]$ est le supplémentaire de E_1 dans E, car :
$\forall\, \overrightarrow{x} \in E, \ \exists !\ \alpha_1, \ \dots \ , \alpha_m, \ \alpha_{m+1}, \ \dots \ , \alpha_n \in \mathbb{K}$;

$$\overrightarrow{x} = \alpha_1 \overrightarrow{f}_1 + \ \dots \ + \alpha_m \overrightarrow{f}_m + \ \alpha_{m+1} \overrightarrow{f}_{m+1} \ \dots \ + \alpha_n \overrightarrow{f}_n$$

Donc : $\forall\, \overrightarrow{x} \in E, \ \exists !\ \overrightarrow{x}_1 = \alpha_1 \overrightarrow{f}_1 + \ \dots \ + \alpha_m \overrightarrow{f}_m \in E_1, \ \ \overrightarrow{x}_2 = \alpha_{m+1} \overrightarrow{f}_{m+1} \ \dots \ + \alpha_n \overrightarrow{f}_n \in E_2$;

$$\overrightarrow{x} = \overrightarrow{x}_1 + \overrightarrow{x}_2$$

ce qui montre que

$$E = E_1 \oplus E_2$$

□

Proposition 5.19 *Soient B_1 et B_2 deux partie d'un espace vectoriel E telles que $B_1 \cup B_2$ est une base de E, alors*

$$E = [B_1] \oplus [B_2]$$

Démonstration : Elle se fait de la même manière que celle de la proposition précédente. □

Proposition 5.20 *Soient E_1 et E_2 deux sous espaces vectoriels de E, alors*

$$\dim(E_1 + E_2) = \dim E_1 + \dim E_2 - \dim(E_1 \cap E_2)$$

Démonstration : Soit $B_0 = \{\overrightarrow{e}_1, \ldots, \overrightarrow{e}_k\}$ une base de $E_1 \cap E_2$, comme $E_1 \cap E_2 \subset E_1$ $E_1 \cap E_2 \subset E_2$ on complète B_0 par $B_1 = \left\{\overrightarrow{f}_{k+1}, \ldots, \overrightarrow{f}_{m_1}\right\}$ et $B_2 = \left\{\overrightarrow{g}_{k+1}, \ldots, \overrightarrow{g}_{m_2}\right\}$ pour que $B_0 \cup B_1$ soit une base de E_1 et $B_0 \cup B_1 \cup B_2$ une base E_2.

a) Il est claire que $B_0 \cup B_2 \cup B_2$ engendre $E_1 + E_2$.

b) Montrons que $B_0 \cup B_2 \cup B_2$ est libre.
Soient $\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_{m_1}, \gamma_{k+1}, \ldots, \gamma_{m_2} \in \mathbb{K}$, tels que

$$(*)\quad \alpha_1\overrightarrow{e}_1 + \ldots + \alpha_k\overrightarrow{e}_k + \beta_{k+1}\overrightarrow{f}_{k+1} + \ldots + \beta_{m_1}\overrightarrow{f}_{m_1} + \gamma_{k+1}\overrightarrow{g}_{k+1} + \ldots + \gamma_{m_2}\overrightarrow{g}_{m_2} = \overrightarrow{0}$$

alors

$$\alpha_1\overrightarrow{e}_1 + \ldots + \alpha_k\overrightarrow{e}_k + \beta_{k+1}\overrightarrow{f}_{k+1} + \ldots + \beta_{m_1}\overrightarrow{f}_{m_1} = (-\gamma_{k+1})\overrightarrow{g}_{k+1} + \ldots + (-\gamma_{m_2})\overrightarrow{g}_{m_2}$$

$B_0 \cup B_1$ étant une base de E_1 et $B_2 \subset E_2$, alors

$$\begin{cases} \alpha_1\overrightarrow{e}_1 + \ldots + \alpha_k\overrightarrow{e}_k + \beta_{k+1}\overrightarrow{f}_{k+1} + \ldots + \beta_{m_1}\overrightarrow{f}_{m_1} \in E_1 \\ (-\gamma_{k+1})\overrightarrow{g}_{k+1} + \ldots + (-\gamma_{m_2})\overrightarrow{g}_{m_2} \in E_2 \end{cases}$$

donc

$$\begin{cases} \alpha_1\overrightarrow{e}_1 + \ldots + \alpha_k\overrightarrow{e}_k + \beta_{k+1}\overrightarrow{f}_{k+1} + \ldots + \beta_{m_1}\overrightarrow{f}_{m_1} \in E_1 \cap E_2 \\ (-\gamma_{k+1})\overrightarrow{g}_{k+1} + \ldots + (-\gamma_{m_2})\overrightarrow{g}_{m_2} \in E_1 \cap E_2 \end{cases}$$

et comme $(-\gamma_{k+1})\overrightarrow{g}_{k+1} + \ldots + (-\gamma_{m_2})\overrightarrow{g}_{m_2} \in [B_2]$, $E_1 \cap E_2 = [B_0]$ et $E_2 = [B_0] \oplus [B_2]$, on déduit que

$$(-\gamma_{k+1})\overrightarrow{g}_{k+1} + \ldots + (-\gamma_{m_2})\overrightarrow{g}_{m_2} = \overrightarrow{0}$$

et sachant que B_2 est libre, alors

$$(-\gamma_{k+1}) = \ldots = (-\gamma_{m_2}) = 0$$

en reportant celà dans (*) on déduit :

$$\alpha_1\overrightarrow{e}_1 + \ldots + \alpha_k\overrightarrow{e}_k + \beta_{k+1}\overrightarrow{f}_{k+1} + \ldots + \beta_{m_1}\overrightarrow{f}_{m_1} = \overrightarrow{0}$$

et comme $B_0 \cup B_1$ est une base, on déduit que

$$\alpha_1 = \ \ldots \ = \alpha_k = \beta_{k+1} = \ \ldots \ = \beta_{m_1} = 0$$

ce qui montre que $B_0 \cup B_1 \cup B_2$ est libre.

c. De **a.** et **b.** on déduit que $B_0 \cup B_1 \cup B_2$ est une base de $E_1 + E_2$, donc

$$\begin{array}{rcl} \dim(E_1 + E_2) & = & \mathrm{Card}(B_0) + \mathrm{Card}(B_1) + \mathrm{Card}(B_2) \\ & = & \Big[\mathrm{Card}(B_0) + \mathrm{Card}(B_1)\Big] + [\mathrm{Card}(B_0) + \mathrm{Card}(B_1)] - \mathrm{Card}(B_0) \\ & = & \dim E_1 \ + \ \dim(E_2) \ - \ \dim(E_1 \cap E_2) \end{array}$$

ce qui termine la preuve de la proposition.

□

Propriété 5.8 *Soient E un espace vectoriel et E_1 et E_2 deux sous espaces vectoriels de E, alors les trois propositions suivantes sont équivalentes*

- $E = E_1 \oplus E_2$
- $\Big(E_1 + E_2 = E\Big) \wedge \Big(\dim \mathrm{E}_1 + \dim E_2 = \dim E\Big)$
- $\Big(E_1 \cap E_2 = \{0\}\Big) \wedge \Big(\dim \mathrm{E}_1 + \dim E_2 = \dim E\Big)$

Chapitre 6

Applications linéaires

6.1 Définitions et propriétés générales

Soient $(E,+,.)$ et $(F,+,.)$ deux $\mathbb{K}$-espaces vectoriels.

Définition 6.1 *On appelle application linéaire de E dans F, toute application $f : E \longrightarrow F$ tel que :*

$\mathcal{L}_1$: $\quad \forall \overrightarrow{x},\ \overrightarrow{y} \in E, \quad f(\overrightarrow{x}+\overrightarrow{y}) = f(\overrightarrow{x}) + f(\overrightarrow{y}),$

$\mathcal{L}_2$: $\quad \forall \overrightarrow{x} \in E,\ \forall \alpha \in \mathbb{K}, \quad f(\alpha\overrightarrow{x}) = \alpha f(\overrightarrow{x}).$

On note $\mathcal{L}(E,F)$ l'ensemble de toutes les applications linéaires de E dans F.

Exemple 1 : Soit $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ telle que :

$$\forall \overrightarrow{X} = (x,y,z) \in \mathbb{R}^3, \qquad f(\overrightarrow{X}) = (x+2y, 3y-z, x+z).$$

alors $f \in \mathcal{L}(\mathbb{R}^3, \mathbb{R}^3)$.
En effet :

1. Soient $\overrightarrow{X} = (x,y,z),\ \overrightarrow{Y} = (x',y',z') \in \mathbb{R}^3$, alors

$$\begin{array}{rcl} f(\overrightarrow{X}+\overrightarrow{Y}) & = & f\left((x,y,z)+(x',y',z')\right) \\ & = & f(x+x', y+y', z+z') \\ & = & \Big((x+x')+2(y+y')\,,\ 3(y+y')-(z+z')\,,\ (x+x')+(z+z')\Big) \\ & = & (x+2y, 3y-z, x+z)+(x'+2y', 3y'-z', x'+z') \\ & = & f(x,y,z)+f(x',y',z') \\ & = & f(\overrightarrow{X})+f(\overrightarrow{Y}) \end{array}$$

2. Soient $\overrightarrow{X} = (x, y, z) \in \mathbb{R}^3$ et $\alpha \in \mathbb{R}$, alors

$$\begin{aligned} f(\alpha\overrightarrow{X}) &= f\left(\alpha(x, y, z)\right) \\ &= f(\alpha x, \alpha y, \alpha z) \\ &= \Big((\alpha x) + 2(\alpha y)\,,\, 3(\alpha y) - (\alpha z)\,,\, (\alpha x) + (\alpha z)\Big) \\ &= \alpha(x + 2y, 3y - z, x + z) \\ &= \alpha f(x, y, z) \\ &= \alpha f(\overrightarrow{X}) \end{aligned}$$

De **1.** et **2.** on déduit que $f \in \mathcal{L}(\mathbb{R}^3, \mathbb{R}^3)$.

□

Exemple 2 : Soit $\ell :\ \mathbb{R}_2[X] \longrightarrow \mathbb{R}_3[X]$ telle que :

$$\forall\, P = ax^2 + bx + c, \qquad \ell(P) = (a - b)x^3 + (c - a)x - b$$

alors $\ell \in \mathcal{L}\Big(\mathbb{R}_2[X], \mathbb{R}_3[X]\Big)$.
En effet :

1. Soient $P = ax^2 + bx + c$ et $Q = a'x^2 + b'x + c'$ dans $\mathbb{R}_2[X]$, alors

$$\begin{aligned} \ell(P + Q) &= \ell\left((a + a')x^2 + (b + b')x + (c + c')\right) \\ &= [(a + a') - (b + b')]x^3 + [(c + c') - (a + a')]x - (b + b') \\ &= [(a - b)x^3 + (c - a)x - b] + [(a' - b')x^3 + (c' - a')x - b'] \\ &= \ell(P) + \ell(Q) \end{aligned}$$

donc :

$$\forall\, P,\ Q \in \mathbb{R}_2[X], \qquad \ell(P + Q) = \ell(P) + \ell(Q)$$

2. Soient $\alpha \in \mathbb{R}$ et $P = ax^2 + bx + c \in \mathbb{R}_2[X]$, alors

$$\begin{aligned} \ell(\alpha P) &= \ell(\alpha(ax^2 + bx + c)) \\ &= \ell(\alpha a\, x^2 + \alpha b\, x + \alpha c) \\ &= (\alpha a - \alpha b)x^3 + (\alpha c - \alpha a)x - \alpha b \\ &= \alpha\Big[(a - b)x^3 + (c - a)x - b\Big] \\ &= \alpha\ell(P) \end{aligned}$$

donc

$$\forall\, \alpha \in \mathbb{R},\ \forall\, P \in \mathbb{R}_2[X], \qquad \ell(\alpha P) = \alpha\ell(P)$$

De **1.** et **2.** on déduit que ℓ est linéaire.

Remarque 6.1 *Soit $f \in \mathcal{L}(E, F)$,*

- *Si f est bijective, on dit que c'est un isomorphisme (d'espaces vectoriels) et que E et F sont isomorphes.*
- *Si de plus $E = F$, on dit que f est un automorphisme de E.*

Proposition 6.1 *Soit $f : E \longrightarrow F$, alors f est linéaire si et seulement si*

$$\forall \overrightarrow{x},\ \overrightarrow{y} \in E,\ \forall \alpha,\ \beta \in \mathbb{K}, \quad f(\alpha \overrightarrow{x} + \beta \overrightarrow{y}) = \alpha f(\overrightarrow{x}) + \beta f(\overrightarrow{y})$$

Démonstration :

$\Longrightarrow ?$: Supposons que $f \in \mathcal{L}(E, F)$, alors

$$\begin{array}{rcl} \forall\, \overrightarrow{x},\ \overrightarrow{y} \in E,\ \forall\, \alpha,\ \beta \in \mathbb{K}, \quad f(\alpha \overrightarrow{x} + \beta \overrightarrow{y}) & = & f(\alpha \overrightarrow{x}) + f(\beta \overrightarrow{y}) \\ & = & \alpha f(\overrightarrow{x}) + \beta f(\overrightarrow{y}) \end{array}$$

donc

$$\forall\, \overrightarrow{x},\ \overrightarrow{y} \in E,\ \forall\, \alpha,\ \beta \in \mathbb{K}, \quad f(\alpha \overrightarrow{x} + \beta \overrightarrow{y}) = \alpha f(\overrightarrow{x}) + \beta f(\overrightarrow{y})$$

$\Longleftarrow ?$: Inversement, supposons que

$$\forall\, \overrightarrow{x},\ \overrightarrow{y} \in E,\ \forall\, \alpha,\ \beta \in \mathbb{K}, \quad f(\alpha \overrightarrow{x} + \beta \overrightarrow{y}) = \alpha f(\overrightarrow{x}) + \beta f(\overrightarrow{y})$$

alors pour $\alpha = \beta = 1_{\mathbb{K}}$ on retrouve la première condition de la définition d'une application linéaire, et pour α quelconque dans $\mathbb{K}$ et $\beta = 0$ on déduit la deuxième condition, donc $f \in \mathcal{L}(E, F)$.

□

En ittérant $(n-1)$-fois ce résultat, on obtient :

Proposition 6.2 *Soit $f \in \mathcal{L}(E, F)$, alors : $\forall\, \alpha_1,\, \alpha_2, \cdots \alpha_n \in \mathbb{K}$, $\forall\, \overrightarrow{x}_1,\, \overrightarrow{x}_2, \cdot, \overrightarrow{x}_n \in E$,*

$$f(\alpha_1 \overrightarrow{x}_1,\, \alpha_2 \overrightarrow{x}_2, \cdot, \alpha_n \overrightarrow{x}_n) = \alpha_1 f(\overrightarrow{x}_1) + \alpha_2 f(\overrightarrow{x}_2) + \cdot + \alpha_n f(\overrightarrow{x}_n)$$

6.2 Noyau et Image d'une application linéaire

Remarque 6.2 *Etant donnée $f \in \mathcal{L}(E, F)$, sachant que $(E, +, .)$ et $(F, +, .)$ sont des $\mathbb{K}$-espaces vectoriels, alors $(E, +)$ et $(F, +)$ sont des groupes et de la première condition $\mathcal{L}_1$ de linéarité on déduit que f est un homomorphisme de groupes de $(E, +)$ dans $(F, +)$.*
L'élément neutre de $(E, +)$, respectivement $(F, +)$, étant $\overrightarrow{0}_E$, respectivement $\overrightarrow{0}_F$, on adopte alors pour les applications linéaires les mêmes définitions du noyau et de l'image d'un homomorphisme, c'est à dire :

Définition 6.2 *Soit $f \in \mathcal{L}(E, F)$,*

1. *On appelle Noyau de f, l'ensemble*

$$\operatorname{Ker} f = f^{-1}(\{\overrightarrow{0}_F\}) = \{\overrightarrow{x} \in E;\ \ f(\overrightarrow{x}) = \overrightarrow{0}_E\}$$

2. *On appelle Image de f, l'ensemble*

$$\operatorname{Im} f = f(E) = \{f(\overrightarrow{x});\ \ \overrightarrow{x} \in E\}$$

En reprenant les mêmes résultats des homomorphismes de groupes, on obtient :

Proposition 6.3 *Soit $f \in \mathcal{L}(E,F)$, alors :*

1. $f(\overrightarrow{0}_E) = \overrightarrow{0}_F$.

2. *f est injective si et seulement si* $\operatorname{Ker} f = \{\overrightarrow{0}_E\}$.

3. *f est surjective si et seulement si* $\operatorname{Im} f = F$.

Proposition 6.4 *Soient $f \in \mathcal{L}(E,F)$, E' un sous espace vectoriel de E et F' un sous espace vectoriel de F, alors*

1. *$f(E')$ est un sous espace vectoriel de F,*

2. *$f^{-1}(F')$ est un sous espace vectoriel de E.*

Démonstration : On va utiliser la caractérisation des sous espaces vectoriels 5.3.

1. Montrons que $f(E')$ est un sous espace vectoriel de F.

1.a. Sachant que E' est un sous espace vectoriel de E alors $\overrightarrow{0}_E \in E'$. Comme $f(\overrightarrow{0}_E) = \overrightarrow{0}_F$, on déduit que :

$$\overrightarrow{0}_F \in f(E')$$

1.b. Soient $\overrightarrow{y},\ \overrightarrow{y}' \in f(E')$, alors

$$\exists \overrightarrow{x},\ \overrightarrow{x}' \in E';\quad \overrightarrow{y} = f(\overrightarrow{x}) \text{ et } \overrightarrow{y}' = f(\overrightarrow{x}'),$$

donc

$$\begin{array}{rcll} \overrightarrow{y} + \overrightarrow{y}' & = & f(\overrightarrow{x}) + f(\overrightarrow{x}') & \\ & = & f(\overrightarrow{x} + \overrightarrow{x}') & \text{car } f \text{ est linéaire} \end{array}$$

E' étant un sous espace vectoriel de E, alors $(\overrightarrow{x} + \overrightarrow{x}') \in E'$ et par suite

$$\overrightarrow{y} + \overrightarrow{y}' \in f(E')$$

1.c. Soient $\overrightarrow{y} \in f(E')$ et $\alpha \in \mathbb{K}$, alors

$$\begin{array}{rcll} \alpha\overrightarrow{y} & = & \alpha f(\overrightarrow{x}) & \\ & = & f(\alpha\overrightarrow{x}) & \text{car } f \text{ est linéaire} \end{array}$$

E' étant un sous espace vectoriel de E, alors $\alpha\overrightarrow{x} \in E'$ et par suite

$$\alpha\overrightarrow{y} \in f(E')$$

De **1.a.**, **1.b.** et **1.c.** on déduit que $f(E')$ est un sous espace vectoriel de F.

2. Montrons que $f^{-1}(F')$ est un sous espace vectoriel de E.

2.a. F' étant un sous espace vectoriel de F, alors $\overrightarrow{0}_F \in F'$. Comme $f(\overrightarrow{0}_E) = \overrightarrow{0}_F$, on déduit que

$$\overrightarrow{0}_E \in f^{-1}(F')$$

2.b. Soient $\overrightarrow{x},\ \overrightarrow{x}' \in f^{-1}(F')$, alors $f(\overrightarrow{x}),\ f(\overrightarrow{x}') \in F'$, donc :

$$f(\overrightarrow{x}+\overrightarrow{x}') = f(\overrightarrow{x}) + f(\overrightarrow{x}'), \quad \text{car } f \text{ est linéaire}$$

et comme F' est un sous espace vectoriel de F alors

$$f(\overrightarrow{x}) + f(\overrightarrow{x}') \in F'$$

par suite

$$(\overrightarrow{x}+\overrightarrow{x}') \in f^{-1}(F')$$

2.c. Soient $\overrightarrow{x} \in f^{-1}(F')$ et $\alpha \in \mathbb{K}$, alors

$$f(\alpha\overrightarrow{x}) = \alpha f(\overrightarrow{x}) \quad \text{car } f \text{ linéaire}$$

Comme F' est un sous espace vectoriel de F, alors

$$\alpha f(\overrightarrow{x}) \in F'$$

par suite

$$\alpha\overrightarrow{x} \in f^{-1}(F')$$

De **2.a.**, **2.b.** et **2.c.** on déduit que $\boxed{f^{-1}(F') \text{ est un sous espace vectoriel de } E.}$

□

Exemple 6.1 *Soit l'application linéaire* $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ *telle que :*

$$\forall\,(x,y,z) \in \mathbb{R}^3, \quad f(x,y,z) = (x+y-z, 2x-y+z, 3x+y-z)$$

Déterminer une base de $\operatorname{Ker} f$ *et une base de* $\operatorname{Im} f$ *ainsi que leurs dimensions respectives.*

I. Soit $\overrightarrow{X} = (x,y,z) \in \mathbb{R}^3$, alors :

$$\overrightarrow{X} \in \mathbb{R}^3 \iff f(x,y,z) = \overrightarrow{0}_F \iff (x+y-z, 2x-y+z, 3x+y-z) = (0,0,0)$$

$$\iff \begin{cases} x+y-z=0 \\ 2x-y+z=0 \\ 3x+y-z=0 \end{cases} \iff \begin{cases} z=x+y \\ 2x-y+x+y=0 \\ 3x+y-z=0 \end{cases} \iff \begin{cases} z=x+y \\ 3x=0 \\ 0+y-x-y=0 \end{cases}$$

$$\iff \begin{cases} z=x+y \\ 3x=0 \\ 0+y-x-y=0 \end{cases} \iff \begin{cases} z=y \\ x=0 \\ 0=0 \end{cases} \iff \overrightarrow{X} = (0,y,y) = y(0,1,1)$$

d'où on déduit que $\operatorname{Ker} f$ est engendrée par $B = \{(0,1,1)\}$, qui est aussi une partie libre car $(0,1,1) \neq \overrightarrow{0}$, donc :

$$\boxed{B = \{(0,1,1)\} \text{ est une base de } \operatorname{Ker} f \ \text{ et } \ \dim \operatorname{Ker} f = 1}$$

II. Soit $\overrightarrow{Y} \in \mathbb{R}^3$, alors :

$$\begin{array}{rcl} \overrightarrow{Y} \in \operatorname{Im} f & \Longleftrightarrow & \exists x,\ y,\ z \in \mathbb{R};\quad \overrightarrow{Y} = f(x,y,z) \\ & \Longleftrightarrow & \exists x,\ y,\ z \in \mathbb{R};\quad \overrightarrow{Y} = (x+y-z, 2x-y+z, 3x+y-z) \\ & \Longleftrightarrow & \exists x,\ y,\ z \in \mathbb{R};\quad \overrightarrow{Y} = x(1,2,3)+y(1,-1,1)+z(-1,1,-1) \\ & \Longleftrightarrow & \exists x,\ y,\ z \in \mathbb{R};\ \overrightarrow{Y} = x(1,2,3)+y(1,-1,1)+z(-1,1,-1) \end{array}$$

donc $\operatorname{Im} f$ est engendrée par $G = \{\overrightarrow{e}_1, \overrightarrow{e}_2, \overrightarrow{e}_3\}$, avec $\overrightarrow{e}_1 = (1,2,3)$, $\overrightarrow{e}_2 = (1,-1,1)$ et $\overrightarrow{e}_3 = (-1,1,-1)$.

Vérifions si G est libre ?

Soient $\alpha,\ \beta,\ \gamma \in \mathbb{R}$, alors

$$\begin{array}{rcl} \alpha\overrightarrow{e}_1 + \beta\overrightarrow{e}_2 + \gamma\overrightarrow{e}_3 = \overrightarrow{0} & \Longleftrightarrow & \alpha(1,2,3)+\beta(1,-1,1)+\gamma(-1,1,-1) = \overrightarrow{0} \\ & \Longleftrightarrow & (\alpha+\beta-\gamma, 2\alpha-\beta+\gamma, 3\alpha+\beta-\gamma) = (0,0,0) \\ & \Longleftrightarrow & \begin{cases} \alpha+\beta-\gamma = 0 \\ 2\alpha-\beta+\gamma = 0 \\ 3\alpha+\beta-\gamma = 0 \end{cases} \\ & \Longleftrightarrow & (\alpha = 0) \wedge (\gamma = \beta) \end{array}$$

En choisissant $\gamma = 1$, on voit que $\overrightarrow{e}_3 = -\overrightarrow{e}_2$, par suite $\mathcal{B}' = \{\overrightarrow{e}_1, \overrightarrow{e}_2\}$ est une partie génératrice de $\operatorname{Im} f$ et il est très facile de montrer que $\mathcal{B}'$ est libre, d'où on déduit :

$$\boxed{\mathcal{B}' = \{(1,2,3),\ (1,-1,1)\} \text{ est une base de } \operatorname{Im} f \ \text{ et } \ \dim \operatorname{Im} f = 2}$$

□

6.2.1 Structure de $\mathcal{L}(E,F)$

On définit les opérations suivantes sur les applications linéaires.

Définition 6.3 [1] *Soient E, F et G trois $\mathbb{K}$-espaces vectoriels, $f,\ g \in \mathcal{L}(E,F)$, $h \in \mathcal{L}(G,E)$ et $\alpha \in \mathbb{K}$. On définit les applications $f+g$, $\alpha \bullet f$ et $f \circ h$ par :*

- $\forall\ \overrightarrow{x} \in E,\ (f+g)(\overrightarrow{x}) = f(\overrightarrow{x}) + g(\overrightarrow{x})$
- $\forall\ \overrightarrow{x} \in E,\ (\alpha \bullet f)(\overrightarrow{x}) = \alpha f(\overrightarrow{x})$
- $\forall\ \overrightarrow{x} \in E,\ f \circ g\,(\overrightarrow{x}) = f(g(\overrightarrow{x}))$

Il est très facile de montrer que ces applications sont elles aussi linéaires.

Proposition 6.5 *$(\mathcal{L}(E,F), +, \bullet)$ est un $\mathbb{K}$-espace vectoriel.*

Démonstration :

I) $(\mathcal{L}(E,F), +, \bullet)$ est un $\mathbb{K}$-espace vectoriel.

i. "+" est associative dans $\mathcal{L}(E,F)$ car dans l'espace vectoriel F la première loi "+" est associative.

[1] Les lois des trois espaces vectoriels sont notées de la même façon, à savoir "+" et "." .

ii. "+" est commutative dans $\mathcal{L}(E,F)$ car dans l'espace vectoriel F la première loi "+" est commutative.

iii. L'élément neutre de "+" dans $\mathcal{L}(E,F)$ est l'application $\mathcal{O}: E \longrightarrow F$ telle que :

$$\forall\, \overrightarrow{x} \in E, \quad \mathcal{O}(\overrightarrow{x}) = \overrightarrow{0}_F$$

iv. Le symétrique d'une application $f \in \mathcal{L}(E,F)$ est l'application

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

Donc :

1. $(\mathcal{L}(E,F),+)$ est un groupe abélien.

2. $\forall\, f,\ g \in \mathcal{L}(E,F), \forall\, \alpha \in \mathbb{K}, \alpha \bullet (f+g) = (\alpha \bullet f) + (\alpha \bullet g)$, car

$$\begin{array}{rcll} \forall\, \overrightarrow{x} \in E, \quad \Big(\alpha \bullet (f+g)\Big)(\overrightarrow{x}) & = & \alpha(f+g)(\overrightarrow{x}) & \\ & = & \alpha\Big(f(\overrightarrow{x}) + g(\overrightarrow{x})\Big) & \\ & = & \alpha f(\overrightarrow{x}) + \alpha g(\overrightarrow{x}), & \text{car } F \text{ est un } \mathbb{K}-\text{espace vectoriel} \\ & = & (\alpha \bullet f)(\overrightarrow{x}) + (\alpha \bullet f)(\overrightarrow{x}) & \end{array}$$

3. $\forall\, f \in \mathcal{L}(E,F), \forall\, \alpha,\ \beta \in \mathbb{K}, (\alpha+\beta) \bullet f = (\alpha \bullet f) + (\beta \bullet f)$, car

$$\begin{array}{rcll} \forall\, \overrightarrow{x} \in E, \quad \Big((\alpha+\beta) \bullet f\Big)(\overrightarrow{x}) & = & (\alpha+\beta) f(\overrightarrow{x}) & \\ & = & \alpha f(\overrightarrow{x}) + \beta f(\overrightarrow{x}), & \text{car } F \text{ est un } \mathbb{K}-\text{espace vectoriel} \\ & = & \Big((\alpha \bullet f) + (\beta \bullet f)\Big)(\overrightarrow{x}) & \end{array}$$

4. $\forall\, f \in \mathcal{L}(E,F), \forall\, \alpha,\ \beta \in \mathbb{K}, (\alpha\beta) \bullet f = \alpha \bullet (\beta \bullet f)$, car :
F étant un $\mathbb{K}$-espace vectoriel, alors

$$\begin{array}{rcll} \forall\, \overrightarrow{x} \in E, \quad ((\alpha\beta) \bullet f)(\overrightarrow{x}) & = & (\alpha\beta)(f(\overrightarrow{x})) & \\ & = & \alpha\Big(\beta(f(\overrightarrow{x}))\Big), & \text{car } F \text{ est un } \mathbb{K}-\text{espace vectoriel} \\ & = & \alpha\Big((\beta \bullet f)(\overrightarrow{x})\Big) & \\ & = & \Big(\alpha \bullet (\beta \bullet f)\Big)(\overrightarrow{x}) & \end{array}$$

5. $\forall\, f \in \mathcal{L}(E,F), 1_{\mathbb{K}} \bullet f = f$ car :

$$\begin{array}{rcll} \forall\, \overrightarrow{x} \in E, \quad (1_{\mathbb{K}} \bullet f)(\overrightarrow{x}) & = & 1_{\mathbb{K}}(f(\overrightarrow{x})) & \\ & = & f(\overrightarrow{x}), & \text{car } F \text{ est un } \mathbb{K}-\text{espace vectoriel} \end{array}$$

De **1.** - **5.**, on déduit que $(\mathcal{L}(E,F),+,\bullet)$ est un $\mathbb{K}$-espace vectoriel.

6.2.2 Le groupe linéaire d'un espace vectoriel

Propriété 6.1 *Si $f \in \mathcal{L}(E,F)$ est bijective, alors $f^{-1} \in \mathcal{L}(F,E)$.*

Démonstration : Soit $f \in \mathcal{L}(E,F)$ bijective, alors il existe une application $f^{-1} : F \longrightarrow E$ telle que $f^{-1} \circ f = id_E$ et $f \circ f^{-1} = id_F$.
Montrons que f^{-1} est linéaire.
Soient $\alpha,\ \beta \in \mathbb{K}$ et $\overrightarrow{x},\ \overrightarrow{y} \in F$, alors :

$$\begin{aligned} f^{-1}(\alpha\overrightarrow{x} + \beta\overrightarrow{y}) &= f^{-1}\Big(\alpha \cdot f(f^{-1}(\overrightarrow{x})) + \beta \cdot f(f^{-1}(\overrightarrow{y}))\Big) \\ &= f^{-1}\left(f\Big(\alpha \cdot f^{-1}(\overrightarrow{x}) + \beta \cdot f^{-1}(\overrightarrow{y})\Big)\right), \quad \text{car } f \text{ est linéaire} \\ &= f^{-1} \circ f\Big(\alpha f^{-1}(\overrightarrow{x}) + \beta f^{-1}(\overrightarrow{y})\Big) \\ &= \alpha f^{-1}(\overrightarrow{x}) + \beta f^{-1}(\overrightarrow{y}), \quad \text{car } f^{-1} \circ f = id_E \end{aligned}$$

ce qui montre que f^{-1} est linéaire. □

Définition 6.4 *Soient $(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel, on appelle "groupe linéaire" de E l'ensemble* GL(E) *des isomorphismes de E dans E.*

Proposition 6.6 *$(\mathrm{GL}(E), \circ)$ est un groupe dont l'élément neutre est l'application identité dans E.*

La preuve de cette proposition est immédiate.

6.2.3 Caracrérisation des applications linéaires injectives, surjectives et bijectives

Proposition 6.7 *Soit $f \in \mathcal{L}(E,F)$, alors :*
1. *f est injective si et seulement si l'image de toute partie libre de E est une partie libre de F.*
2. *f est surjective si et seulement si l'image de toute partie génératrice de E est une partie génératrice de F.*
3. *f est bijective si et seulement si l'image de toute base de E est base de F.*

Démonstration :
1.a. Supposons que f est injective et montrons que l'image de toute partie libre de E est une partie libre de F.
Soit $L = \{\overrightarrow{e}_1,\ \ldots\ , \overrightarrow{e}_m\}$ une partie libre de E, montrons que $f(L)$ est aussi libre dans F.
Soient $\alpha_1,\ \ldots\ , \alpha_m \in \mathbb{K}$, alors

$$\begin{aligned} \alpha_1 f(\overrightarrow{e}_1) + \ \ldots\ + \alpha_m f(\overrightarrow{e}_m) = \overrightarrow{0} \quad &\Longleftrightarrow \quad f\left(\alpha_1\overrightarrow{e}_1 + \ \ldots\ + \alpha_m\overrightarrow{e}_m\right) = \overrightarrow{0} \\ &\Longleftrightarrow \quad (\alpha_1\overrightarrow{e}_1 + \ \ldots\ + \alpha_m\overrightarrow{e}_m) \in \mathrm{Ker}\, f \\ &\Longleftrightarrow \quad \alpha_1\overrightarrow{e}_1 + \ \ldots\ + \alpha_m\overrightarrow{e}_m = \overrightarrow{0}_E, \quad \text{car } f \text{ est injective} \\ &\Longleftrightarrow \quad \alpha_1 = \ \ldots\ = \alpha_m = 0\ , \qquad \text{car } L \text{ est libre} \end{aligned}$$

ce qui montre que $f(L)\{f(\overrightarrow{e}_1),\ \ldots\ , f(\overrightarrow{e}_m)\}$ est libre.

1.b. Supposons que l'image de toute partie libre de E est une partie libre de F et montrons que f est injective.
Soit $B = \{\overrightarrow{e}_1, \ldots, \overrightarrow{e}_n\}$ une base de E, alors $f(B) = \{f(\overrightarrow{e}_1), \ldots, f(\overrightarrow{e}_n)\}$ est une partie libre de F car B est libre.
Soit $\overrightarrow{x} \in E$, alors :

$$\exists \alpha_1, \ldots, \alpha_n \in \mathbb{K}; \quad \overrightarrow{x} = \alpha_1 \overrightarrow{e}_1 + \ldots + \alpha_n \overrightarrow{e}_n,$$

donc

$$\begin{array}{rcll} \overrightarrow{x} \in \operatorname{Ker} f & \Longleftrightarrow & f(\overrightarrow{x}) = \overrightarrow{0}_F & \\ & \Longleftrightarrow & f(\alpha_1 \overrightarrow{e}_1 + \ldots + \alpha_n \overrightarrow{e}_n) = \overrightarrow{0}_F & \\ & \Longleftrightarrow & \alpha_1 f(\overrightarrow{e}_1) + \ldots + \alpha_n f(\overrightarrow{e}_n) = \overrightarrow{0}_F, & \text{car } f \text{ est linéaire} \\ & \Longleftrightarrow & \alpha_1 = \ldots = \alpha_n = 0, & \text{car } f(B) \text{ est libre} \\ & \Longleftrightarrow & \overrightarrow{x} = \overrightarrow{0}_E & \end{array}$$

d'où on déduit que $\operatorname{Ker} f = \{\overrightarrow{0}_E\}$, donc f injective.

2.a. Supposons que f est surjective et montrons que l'image de toute partie génératrice de E est une partie génératrice de F.
Soit $G = \{\overrightarrow{e}_1, \ldots, \overrightarrow{e}_k\}$ une partie génératrice de E, montrons que $f(G)$ est une partie génératrice de F.
Soit $\overrightarrow{y} \in F$, comme f est surjective alors il existe $\overrightarrow{x} \in E$ tel que $\overrightarrow{y} = f(\overrightarrow{x})$. Sachant que G est une partie génératrice de E, alors :

$$\exists\, \alpha_1, \ldots, \alpha_k \in \mathbb{K}; \qquad \overrightarrow{x} = \alpha_1 \overrightarrow{e}_1 + \ldots + \alpha_k \overrightarrow{e}_k\ ,$$

donc

$$\begin{array}{rcll} \overrightarrow{y} & = & f(\overrightarrow{x}) & \\ & = & f(\alpha_1 \overrightarrow{e}_1 + \ldots + \alpha_k \overrightarrow{e}_k) & \\ & = & \alpha_1 f(\overrightarrow{e}_1) + \ldots + \alpha_k f(\overrightarrow{e}_k), & \text{car } f \text{ est linéaire} \end{array}$$

d'où on déduit que $f(G) = \{f(\overrightarrow{e}_1), \ldots, f(\overrightarrow{e}_k)\}$ est une partie génératrice de F.

2.b. Supposons que l'image de toute partie génératrice de E est une partie génératrice de F et montrons que f est surjective.
Soit $B = \{\overrightarrow{e}_1, \ldots, \overrightarrow{e}_m\}$ une base de E, alors $f(B)$ est une partie génératrice de F, donc :

$$\begin{array}{lrcl} \forall\, \overrightarrow{y} \in F,\ \exists\, \alpha_1, \ldots, \alpha_m \in \mathbb{K}; & \overrightarrow{y} = & \alpha_1 f(\overrightarrow{e}_1) + \ldots + \alpha_m f(\overrightarrow{e}_m) & \\ & = & f(\alpha_1 \overrightarrow{e}_1 + \ldots + \alpha_m \overrightarrow{e}_m) & \text{car } f \text{ est linéaire,} \end{array}$$

par suite :

$$\forall\, \overrightarrow{y} \in F,\ \exists\, \overrightarrow{x} = \alpha_1 \overrightarrow{e}_1 + \ldots + \alpha_m \overrightarrow{e}_m \in E; \qquad \overrightarrow{y} = f(\overrightarrow{x})$$

d'où on déduit que f est surjective.

□

6.2.4 Formule du rang

Proposition 6.8 *Soit $f \in \mathcal{L}(E,F)$, alors :*

$$\boxed{\dim \mathrm{Ker}\, f + \dim \mathrm{Im} f = \dim E}$$

Démonstration : Soient E un espace vectoriel de dimension n et $B_1 = \{\overrightarrow{e}_1, \ldots, \overrightarrow{e}_m\}$ une base de $\mathrm{Ker}\, f$. D'après le théorème de la base incomplète, il existe $B_2 = \{\overrightarrow{e}_{m+1}, \ldots, \overrightarrow{e}_n\}$ telle que $B_1 \cup B_2$ est une base de E.
Montrons que $f(B_2)$ est une base de $\mathrm{Im}\, f$.

a. $f(B_2)$ est libre ?
Soient $\alpha_{m+1}, \ldots, \alpha_n \in \mathbb{K}$, alors

$$\begin{aligned}
&\alpha_{m+1} f(\overrightarrow{e}_{m+1}) + \ldots + \alpha_n f(\overrightarrow{e}_n) = \overrightarrow{0}_F \\
&\quad\Longrightarrow f(\alpha_{m+1}\overrightarrow{e}_{m+1} + \ldots + \alpha_n \overrightarrow{e}_n) = \overrightarrow{0}_F, \quad \text{car } f \text{ linéaire} \\
&\quad\Longrightarrow \alpha_{m+1}\overrightarrow{e}_{m+1} + \ldots + \alpha_n \overrightarrow{e}_n \in \mathrm{Ker}\, f \\
&\quad\Longrightarrow \exists\, \alpha_1, \ldots, \alpha_m \in \mathbb{K}; \\
&\qquad\qquad \alpha_{m+1}\overrightarrow{e}_{m+1} + \ldots + \alpha_n \overrightarrow{e}_n = \alpha_1 \overrightarrow{e}_1 + \ldots + \alpha_m \overrightarrow{e}_m \\
&\quad\Longrightarrow \alpha_1 \overrightarrow{e}_1 + \ldots + \alpha_m \overrightarrow{e}_m - \alpha_{m+1}\overrightarrow{e}_{m+1} - \ldots - \alpha_n \overrightarrow{e}_n = \overrightarrow{0}_E \\
&\quad\Longrightarrow \alpha_1 = \ldots = \alpha_m = \alpha_{m+1} = \ldots = \alpha_n = 0, \qquad \text{car } B_1 \cup B_2 \text{ est une base de } E \\
&\quad\Longrightarrow \alpha_{m+1} = \ldots = \alpha_n = 0
\end{aligned}$$

d'où on déduit que $f(B_2)$ est libre.

b. $f(B_2)$ engendre $\mathrm{Im}\, f$?
Soit $\overrightarrow{y} \in \mathrm{Im}\, f$, alors il existe $\overrightarrow{x} \in E$ tel que $\overrightarrow{y} = f(\overrightarrow{x})$. Comme B est une base de E, il existe $\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n \in \mathbb{K}$ tels que

$$\overrightarrow{x} = \alpha_1 \overrightarrow{e}_1 + \ldots + \alpha_m \overrightarrow{e}_m + \alpha_{m+1}\overrightarrow{e}_{m+1}, \ldots, \alpha_n \overrightarrow{e}_n$$

donc

$$\begin{aligned}
\overrightarrow{y} &= f(\alpha_1 \overrightarrow{e}_1 + \ldots + \alpha_m \overrightarrow{e}_m + \alpha_{m+1}\overrightarrow{e}_{m+1} + \ldots + \alpha_n \overrightarrow{e}_n) \\
&= f(\alpha_1 \overrightarrow{e}_1 + \ldots + \alpha_m \overrightarrow{e}_m) + \alpha_{m+1} f(\overrightarrow{e}_{m+1}) + \ldots + \alpha_n f(\overrightarrow{e}_n), \quad \text{car } f \text{ linéaire} \\
&= \alpha_{m+1} f(\overrightarrow{e}_{m+1}) + \ldots + \alpha_n f(\overrightarrow{e}_n), \qquad \text{car } (\alpha_1 \overrightarrow{e}_1 + \ldots + \alpha_m \overrightarrow{e}_m) \in \mathrm{Ker}\, f
\end{aligned}$$

d'où on déduit que $f(B_2)$ est une partie génératrice de $\mathrm{Im}\, f$.

De **a.** et **b.** on déduit que $f(B_2)$ est une base de $\mathrm{Im}\, f$, et comme $Card\,(f(B_2)) = \mathrm{Card}(B_2)$, alors :

$$\boxed{\dim E = \dim \mathrm{Ker}\, f + \dim \mathrm{Im}\, f}$$

□

Une première conséquence de cette formule est que : $\forall\, f \in \mathcal{L}(E,F)$,

$$\boxed{\dim [\mathrm{Im}\, f] \leq \dim E}$$

De même, si E et F sont deux espaces vectoriels de dimensions finies et $f \in \mathcal{L}(E,F)$, alors :

Proposition 6.9

1. *Si* $\dim E > \dim F$ *alors* f *n'est pas injective.*
2. *Si* $\dim E < \dim F$ *alors* f *n'est pas surjective.*

Démonstration :

1. Si $\dim E > \dim F$, comme $\operatorname{Im} f \subset F$ alors $\dim [\operatorname{Im} f] \leq \dim F$, donc

$$\dim \operatorname{Ker} f = \dim E - \dim \operatorname{Im} f > 0$$

d'où on déduit que $\operatorname{Ker} f \neq \{\overrightarrow{0}_E\}$, par suite f n'est pas injective.

2. Si $\dim E < \dim F$, sachant que $\dim \operatorname{Im} f \leq \dim E$, alors

$$\dim \operatorname{Im} f \leq \dim E < \dim F$$

donc $\operatorname{Im} f \neq F$, par suite f n'est pas surjective.

□

Exemple 6.2 *On considère l'application* $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^3$, *telle que*

$$\forall\, (x, y) \in \mathbb{R}^2, \quad f(x, y) = (x - 2y, y - \frac{1}{2}x, 2x - 4y)$$

1. *Montrer que* f *est linéaire.*
2. f *est-elle surjective ?*
3. f *est-elle injective ?*

Réponses :

1. Soient $\overrightarrow{X} = (x, y)$, $\overrightarrow{Y} = (x', y')$ et $\alpha,\ \beta \in \mathbb{R}$, alors :

$$\begin{aligned}
f(\alpha\overrightarrow{X} + \beta\overrightarrow{Y}) &= f(\alpha x + \beta x', \alpha y + \beta y') \\
&= \Big((\alpha x + \beta x') - 2(\alpha y + \beta y'), (\alpha y + \beta y') - \tfrac{1}{2}(\alpha x + \beta x'), 2(\alpha x + \beta x') - 4(\alpha y + \beta y')\Big) \\
&= (\alpha x - 2\alpha y, \alpha y - \tfrac{1}{2}\alpha x, 2\alpha x - 4\alpha y) + (\beta x' - 2\beta y', \beta y' - \tfrac{1}{2}\beta x', 2\beta x' - 4\beta y') \\
&= \Big(\alpha(x - 2y), \alpha(y - \tfrac{1}{2}x), \alpha(2x - 4y)\Big) + \Big(\beta(x' - 2y'), \beta(y' - \tfrac{1}{2}x'), \beta(2x' - 4y')\Big) \\
&= \alpha(x - 2y, y - \tfrac{1}{2}x, 2x - 4y) + \beta(x' - 2y', y' - \tfrac{1}{2}x', 2x' - 4y') \\
&= \alpha f(x, y) + \beta f(x', y') \\
&= \alpha f(\overrightarrow{X}) + \beta f(\overrightarrow{Y})
\end{aligned}$$

ce qui montre que f est linéaire.

2. D'après la proposition 6.9 f n'est pas surjective car la dimension de l'espace d'arrivée $\mathbb{R}^3$ est supérieure à la dimension de l'espace de départ $\mathbb{R}^2$.

3. Comme la dimension de l'espace de départ n'est pas supérieure à la dimension de l'espace d'arrivée, la proposition 6.9 ne nous renseigne pas sur l'injectivité de l'application linéaire f, il

faut alors déterminer le noyau de cette dernière.
Soit $\overrightarrow{X} = (x, y)$, alors

$$\begin{aligned} f(\overrightarrow{X}) = \overrightarrow{0} &\iff (x - 2y, y - \tfrac{1}{2}x, 2x - 4y) = (0, 0, 0) \\ &\iff \begin{cases} x - 2y = 0 \\ y - \frac{1}{2}x = 0 \\ 2x - 4y = 0 \end{cases} \\ &\iff \begin{cases} x = 2y \\ y - \frac{1}{2}2x = 0 \\ 2.2x - 4y = 0 \end{cases} \\ &\iff x = 2y \\ &\iff \overrightarrow{X} = (2y, y) = y(2, 1) \end{aligned}$$

Ainsi,

$$\overrightarrow{X} \in \operatorname{Ker} f \iff \exists y \in \mathbb{R}; \quad \overrightarrow{X} = y(2, 1)$$

en particulier $\overrightarrow{X} = (2, 1) \in \operatorname{Ker} f$, ce qui montre que f n'est pas injective.

□

Remarque 6.3 *Cette exemple montre que la réciproque de la première implication de la proposition 6.9 est fausse.*

Exemple 6.3 *On considère l'application* $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$, *telle que*

$$\forall\, (x, y, z) \in \mathbb{R}^3, \quad f(x, y, z) = (x - 2y + z, 2y - x - z)$$

1. *Montrer que f est linéaire.*
2. *f est-elle injective ?*
3. *f est-elle surjective ?*

Réponses :

De la même manière que l'exemple précédent, on montre facilement que f est linéaire.

2. D'après la proposition 6.9, f n'est pas injective car la dimension de l'espace de départ est supérieure à celle de l'espace d'arrivée.

3. Comme la dimension de l'espace de départ n'est pas inférieure à la dimension de l'espace d'arrivée, la proposition 6.9 ne nous renseigne pas sur la surjectivité de l'application linéaire f, il faut alors voir si tout vecteur de l'espace d'arrivée admet ou non un antécédent.
Soit $\overrightarrow{Y} = (u, v) \in \mathbb{R}^2$, alors

$$\begin{aligned} \overrightarrow{Y} = f(\overrightarrow{X}) &\iff (u, v) = (x - 2y + z, 2y - x - z) \\ &\iff \begin{cases} x - 2y + z = u \\ 2y - x - z = v \end{cases} \\ &\iff \begin{cases} x = u + 2y - z \\ 2y - (u + 2y - z) - z = v \end{cases} \\ &\iff \begin{cases} x = u + 2y - z \\ -u = v \end{cases} \end{aligned}$$

Ainsi, pour tout vecteur $\overrightarrow{Y} = (u, v) \in \overrightarrow{R}^2$ tel que $-u \neq v$, l'équation

$$\overrightarrow{Y} = f(\overrightarrow{X})$$

n'a pas de solution $\overrightarrow{X} \in \mathbb{R}^3$, ce qui montre que f n'est pas surjective.

Remarque 6.4 *Cet exemple montre que la réciproque de la deuxième implication de la proposition 6.9 est fausse.*

Exemple 6.4 *On considère l'application* $h : \mathbb{R}_3[X] \longrightarrow \mathbb{R}_3[X]$, *telle que*

$$\forall\, P = ax^3 + bx^2 + cx + d \in \mathbb{R}_3[X], \quad h(P) = (a-b)x^2 + (a+b)x + (c+d)$$

1. *Montrer que f est linéaire.*
2. *Déterminer la dimension de* $\operatorname{Ker} f$
3. *Déduire la dimension de* $\operatorname{Im} f$
4. *h est-elle injective ? Surjective ? Bijective ?*

Réponses :

1. Soient $P = ax^3+bx^2+cx+d \in \mathbb{R}_3[X]$, $Q = a'x^3+b'x^2+c'x+d' \in \mathbb{R}_3[X]$ et $\alpha,\ \beta \in \mathbb{R}$, alors :

$$\begin{aligned}
h(\alpha P + \beta Q) &= h\Big((\alpha a + \beta a')x^3 + (\alpha b + \beta b')x^2 + (\alpha c + \beta c')x + (\alpha d + \beta d')\Big) \\
&= \Big((\alpha a + \beta a') - (\alpha b + \beta b')\Big)x^2 + \Big((\alpha a + \beta a') + (\alpha b + \beta b')\Big)x + \\
&\qquad + \Big((\alpha c + \beta c') + (\alpha d + \beta d')\Big) \\
&= \Big((\alpha a - \alpha b)x^2 + (\alpha a + \alpha b)x + (\alpha c + \alpha d)\Big) + \\
&\qquad + \Big((\beta a' - \beta b')x^2 + (\beta a' + \beta b')x + (\beta c' + \beta d')\Big) \\
&= \alpha\Big((a-b)x^2 + (a+b)x + (c+d)\Big) + \beta\Big((a-b)x^2 + (a+b)x + (c+d)\Big) \\
&= \alpha h(P) + \beta h(Q)
\end{aligned}$$

ce qui montre que h est linéaire.

2. Soit $P = ax^3 + bx^2 + cx + d \in \mathbb{R}_3[X]$, alors

$$\begin{aligned}
P \in \operatorname{Ker} h &\iff h(P) = 0 \\
&\iff (a-b)x^2 + (a+b)x + (c+d) = 0 \\
&\iff \begin{cases} a - b = 0 \\ a + b = 0 \\ c + d = 0 \end{cases} \\
&\iff \begin{cases} a = b \\ b + b = 0 \\ c = -d \end{cases} \\
&\iff \begin{cases} a = b = 0 \\ c = -d \end{cases} \\
&\iff P = -dx + d \\
&\iff P = d(x-1)
\end{aligned}$$

Ainsi,

$$\forall P \in \operatorname{Ker} h,\ \exists d \in \mathbb{R};\quad P = d(x-1)$$

ce qui montre que $\mathcal{B} = \{(x-1)\}$ est une partie génératrice de $\operatorname{Ker} h$ et comme $\operatorname{Card} h = 1$ et $\Big(x - 1 \neq 0\Big)$, on déduit que $\mathcal{B}$ est une base de $\operatorname{Ker} h$, par suite :

$$\boxed{\dim \operatorname{Ker}(h) = 1}$$

3. Sachant que la dimension de l'espace de départ, $\mathbb{R}_3[X]$, est n=4, de la formule du rang on déduit

$$\boxed{\dim \operatorname{Im}(h) = 4 - 1 = 3}$$

4. D'après 2. on déduit que h n'est pas injective, donc elle n'est pas aussi bijective et de la question 3. on déduit que h n'est pas aussi surjective.

Proposition 6.10 *Si* $\dim E = \dim F$*, les trois propriètés suivantes sont équivalentes :*

1. f *est bijective.*
2. f *est injective.*
3. f *est surjective.*

Démonstration : En effet, on a :

$$\begin{array}{rcl} f \text{ est injective} & \Longleftrightarrow & \dim \operatorname{Ker} f = 0 \\ & \Longleftrightarrow & \dim \operatorname{Im} f = \dim E = \dim F, \quad \text{d'après la formule du rang} \\ & \Longleftrightarrow & f \text{ est surjective} \end{array}$$

d'où on déduit le résultat de notre proposition.

□

Remarque 6.5 *De la proposition 6.10, la deuxième question suffit pour dire que l'application* h *de l'exemple 6.4 n'est pas surjective.*

6.2.5 Rang d'une application linéaire

Définition 6.5 *On appelle rang d'une application linéaire* $f : E \longrightarrow F$ *la dimension de son image noté* $\operatorname{rg}(f)$.

Comme $\operatorname{Im} f \subset F$, de la formule du rang on déduit les propriétés suivantes :

Propriété 6.2 *Soit* $f \in \mathcal{L}(E, F)$*, alors*

- $\operatorname{rg}(f) \leq \dim F$
- $\operatorname{rg}(f) \leq \dim E$
- $\dim E = \dim \operatorname{Ker} f + \operatorname{rg}(f)$
- f *est surjective si et seulement si* $\operatorname{rg}(f) = \dim F$

6.2.6 Les projecteurs

Définition 6.6 *Soient E_1 et E_2 deux sous espaces vectoriels supplémentaires dans E. On appelle projection de E sur E_1 (parallèlement à E_2) l'application $\mathrm{Pr}_{E_1} : E \longrightarrow E_1$ définie par*

$$\forall \overrightarrow{x} = \overrightarrow{x}_1 + \overrightarrow{x}_2 \in E = E_1 \oplus E_2, \quad \mathrm{Pr}_{E_1}(\overrightarrow{x}) = \overrightarrow{x}_1$$

Proposition 6.11 *Pr_{E_1} est une application linéaire surjective dont le noyau est égal à E_2.*

Démonstration :

1. $\mathrm{Pr}_{E_1} \in \mathcal{L}(E, E_1)$, car : $\forall\, \overrightarrow{x},\ \overrightarrow{y} \in E$,

$$\exists\, \overrightarrow{x}_1,\ \overrightarrow{y}_1 \in E_1,\ \exists\, \overrightarrow{x}_2,\ \overrightarrow{y}_2 \in E_2; \qquad (\overrightarrow{x} = \overrightarrow{x}_1 + \overrightarrow{x}_2) \wedge (\overrightarrow{y} = \overrightarrow{y}_1 + \overrightarrow{y}_2)$$

donc

$$\begin{aligned}
\forall\, \alpha,\ \beta \in \mathbb{K}, \quad \mathrm{Pr}_{E_1}(\alpha\overrightarrow{x} + \beta\overrightarrow{y}) &= \mathrm{Pr}_{E_1}\Big(\alpha(\overrightarrow{x}_1 + \overrightarrow{x}_2) + \beta(\overrightarrow{y}_1 + \overrightarrow{y}_2)\Big) \\
&= \mathrm{Pr}_{E_1}\Big((\alpha\overrightarrow{x}_1 + \beta\overrightarrow{y}_1) + (\alpha\overrightarrow{x}_2 + \beta\overrightarrow{y}_2)\Big) \\
&= \alpha\overrightarrow{x}_1 + \beta\overrightarrow{y}_1 \\
&= \alpha\,\mathrm{Pr}_{E_1}\Big((\overrightarrow{x}_1 + \overrightarrow{x}_2)\Big) + \beta\,\mathrm{Pr}_{E_1}\Big((\overrightarrow{y}_1 + \overrightarrow{y}_2)\Big) \\
&= \alpha\,\mathrm{Pr}_{E_1}(\overrightarrow{x}) + \beta\,\mathrm{Pr}_{E_1}\Big(\overrightarrow{y}\Big)
\end{aligned}$$

2. Pr_{E_1} est surjective, car

$$\forall \overrightarrow{y} \in E_1,\ \exists\, \overrightarrow{x} = \overrightarrow{y} + \overrightarrow{0} \in E; \quad \mathrm{Pr}_{E_1}(\overrightarrow{x}) = \overrightarrow{y}$$

3. $\mathrm{Ker}\,(\mathrm{Pr}_{E_1}) = E_2$, car :

$$\forall\, \overrightarrow{x} \in E,\ \exists!\, \overrightarrow{x}_1 \in E_1,\ \exists!\, \overrightarrow{x}_2 \in E_2; \qquad \overrightarrow{x} = \overrightarrow{x}_1 + \overrightarrow{x}_2$$

donc

$$\begin{aligned}
\overrightarrow{x} \in \mathrm{Ker}\,(\mathrm{Pr}_{E_1}) &\iff \mathrm{Pr}_{E_1}(\overrightarrow{x}) = \overrightarrow{0} \\
&\iff \Big(\overrightarrow{x} = \overrightarrow{x}_1 + \overrightarrow{x}_2\Big) \wedge \Big(\overrightarrow{x}_1 = \overrightarrow{0}\Big) \\
&\iff \overrightarrow{x} = \overrightarrow{x}_2
\end{aligned}$$

d'où on déduit que $\mathrm{Ker}\,(\mathrm{Pr}_{E_1}) = E_2$.

□

Définition 6.7 *On appelle projecteur sur E toute application linéaire p de E dans E telle que*

$$p \circ p = p$$

Il est clair que : Pr_{E_1} est un projecteur sur E.

Inversement,

Proposition 6.12 *Si p est un projecteur sur E, alors $p = Pr_{\mathrm{Im}\, f}$.*

Démonstration : En effet,

1. $E = \operatorname{Ker} p + \operatorname{Im} p$, car

$$\begin{aligned} \forall\, \overrightarrow{x} \in E, \qquad \overrightarrow{x} \in \operatorname{Ker} p \cap \operatorname{Im} p &\iff \Big(\overrightarrow{x} \in \operatorname{Ker} p\Big) \wedge \Big(\overrightarrow{x} \in \operatorname{Im} p\Big) \\ &\iff \Big(p(\overrightarrow{x}) = \overrightarrow{0}\Big) \wedge \Big(\exists \overrightarrow{z} \in E;\ \overrightarrow{x} = p(\overrightarrow{z})\Big) \end{aligned}$$

comme $p \circ p = p$, alors

$$\overrightarrow{x} = p(\overrightarrow{z}) = p(p(\overrightarrow{z})) = p(\overrightarrow{x}) = \overrightarrow{0}$$

donc

$$\boxed{\operatorname{Ker} p \cap \operatorname{Im} p = \{\overrightarrow{0}\}}$$

et de la formule du rang on a

$$\boxed{\dim E = \dim \operatorname{Ker} p + \dim \operatorname{Im} p}$$

d'où on déduit que

$$\boxed{E = \operatorname{Ker} p \oplus \operatorname{Im} p.}$$

2. $p = Pr_{\operatorname{Im} p}$, car :

$$\forall \overrightarrow{x} \in E,\ \exists \overrightarrow{x}_1 \in \operatorname{Ker} p,\ \exists \overrightarrow{x}_2 \in \operatorname{Im} p\,; \quad \overrightarrow{x} = \overrightarrow{x}_1 + \overrightarrow{x}_2$$

et on a : $\overrightarrow{x}_2 \in \operatorname{Im} p \Longrightarrow \exists \overrightarrow{z} \in E;\ \ \overrightarrow{x}_2 = p(z)$,
donc

$$\begin{aligned} p(\overrightarrow{x}) &= p(\overrightarrow{x}) \\ &= p(\overrightarrow{x}_1 + \overrightarrow{x}_2) \\ &= p(\overrightarrow{x}_1) + p(\overrightarrow{x}_2), \quad \text{car } p \text{ linéaire} \\ &= p(\overrightarrow{x}_2), \quad \text{car } \overrightarrow{x}_1 \in \operatorname{Ker} p \\ &= p \circ p\Big(\overrightarrow{z}\Big), \quad \text{car } \overrightarrow{x}_2 = p(\overrightarrow{z}) \\ &= p(\overrightarrow{z}), \quad \text{car } p \circ p = p \\ &= \overrightarrow{x}_2 \\ &= Pr_{\operatorname{Im} p}(\overrightarrow{x}) \end{aligned}$$

par suite

$$p = Pr_{\operatorname{Im} p}$$

□

6.2.7 Espace dual et base duale

Définition 6.8 *On appelle forme linéaire, sur un $\mathbb{K}$-espace vectoriel E, toute application linéaire de E dans $\mathbb{K}$. L'ensemble de toutes les formes linéaires sur E est appelé espace dual de E et noté E^* ou E'.*

Comme $E^* = \mathcal{L}(E, \mathbb{K})$ est un $\mathbb{K}$-espace vectoriel, on peut définir l'espace dual de E^* qu'on appelle **bidual** de E et qu'on note E^{**}.

Soit $\mathcal{B} = \{\overrightarrow{e}_1, \ \ldots\ , \overrightarrow{e}_n\}$ une base de E, alors

Proposition 6.13 *Pour tout $j \in \{1, \ \dots \ , n\}$, l'application $e'_j : E \longrightarrow \mathbb{K}$ définie par*

$$\forall\, \overrightarrow{x} = \alpha_1 \overrightarrow{e}_1 + \ \dots \ + \alpha_n \overrightarrow{e}_n, \qquad e'_j(\alpha_1 \overrightarrow{e}_1 + \ \dots \ + \alpha_n \overrightarrow{e}_n) = \alpha_j \overrightarrow{e}_j$$

est une forme linéaire sur E.

Démonstration : Soient $\overrightarrow{x} = \alpha_1 \overrightarrow{e}_1 + \ \dots \ + \alpha_n \overrightarrow{e}_n$ et $\overrightarrow{y} = \beta_1 \overrightarrow{e}_1 + \ \dots \ + \beta_n \overrightarrow{e}_n$ dans E et $\gamma, \ \lambda \in \mathbb{K}$, alors

$$\begin{aligned} e'_j(\gamma \overrightarrow{x} + \lambda \overrightarrow{y}) &= e'_j\Big(\gamma(\alpha_1 \overrightarrow{e}_1 + \ \dots \ + \alpha_n \overrightarrow{e}_n) \ + \ \lambda(\beta_1 \overrightarrow{e}_1 + \ \dots \ + \beta_n \overrightarrow{e}_n) \Big) \\ &= e'_j\Big(\ (\gamma\alpha_1 + \lambda\beta_1)\overrightarrow{e}_1 + \ \dots \ + (\gamma\alpha_n + \lambda\beta_n)\overrightarrow{e}_n) \Big) \\ &= (\gamma\alpha_j + \lambda\beta_j)\overrightarrow{e}_j \\ &= \gamma\alpha_j \overrightarrow{e}_j + \lambda\beta_j \overrightarrow{e}_j \\ &= \gamma\,(\alpha_j \overrightarrow{e}_j) + \lambda\,(\beta_j \overrightarrow{e}_j) \\ &= \gamma e'_j(\overrightarrow{x}) + \lambda e'_j(\overrightarrow{y}) \end{aligned}$$

d'où on déduit que $e'_j \in \mathcal{L}(E, \mathbb{K})$.

□

Remarque 6.6 *En utilisant le symbole de Kcroneker*[2]

$$\delta^i_j = \begin{cases} 1, \ si \ i = j \\ 0, \ sii \neq j \end{cases}$$

e'i est définie par

$$\forall\, i, \ j \in \{1, \ \dots \ , n\}, \qquad e'_i(\overrightarrow{e}_j) = \delta^i_j \overrightarrow{e}_j$$

Proposition 6.14 *Soit $\mathcal{B} = \{e_1, \ \dots \ , e_n\}$ une base de E, alors $\mathcal{B}' = \{e_1{}', \dots, e_n{}'\}$ est une base de E^* appelée base duale de B.*

Démonstration :

1. $\mathcal{B}'$ est une partie génératrice de E^*.

Soit $f \in E^*$, donc :

$$\forall\, \overrightarrow{X} \in E, \ \exists!\, \alpha_1, \ \alpha_2, \ \dots \ , \alpha_n \in \mathbb{K}; \quad \overrightarrow{X} = \alpha_1 \overrightarrow{e}_1 + \alpha_2 \overrightarrow{e}_2 + \ \dots \ + \alpha_n \overrightarrow{e}_n$$

Comme f est linéaire et $f(\overrightarrow{e}_1), \ f(\overrightarrow{e}_2), \ \dots \ , f(\overrightarrow{e}_n) \in \mathbb{K}$, alors

$$\begin{aligned} f(\overrightarrow{X}) &= \alpha_1 f(\overrightarrow{e}_1) + \alpha_2 f(\overrightarrow{e}_2) + \ \dots \ + \alpha_n f(\overrightarrow{e}_n) \\ &= f(\overrightarrow{e}_1)\, e_1{}'\Big(\alpha_1 \overrightarrow{e}_1 + \alpha_2 \overrightarrow{e}_2 + \ \dots \ + \alpha_n \overrightarrow{e}_n\Big) + \\ &\qquad + f(\overrightarrow{e}_2)\, e_2{}'\Big(\alpha_1 \overrightarrow{e}_1 + \alpha_2 \overrightarrow{e}_2 + \ \dots \ + \alpha_n \overrightarrow{e}_n\Big) \\ &\qquad + \ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots + \\ &\qquad + f(\overrightarrow{e}_1)\, e_n{}'\Big(\alpha_1 \overrightarrow{e}_1 + \alpha_2 \overrightarrow{e}_2 + \ \dots \ + \alpha_n \overrightarrow{e}_n\Big) \\ &= f(\overrightarrow{e}_1)\, e_1{}'(\overrightarrow{X}) + f(\overrightarrow{e}_2)\, e_2{}'(\overrightarrow{X}) + \ldots + f(\overrightarrow{e}_n)\, e_n{}'(\overrightarrow{X}) \end{aligned}$$

[2]Léopold Kronecker (7 décembre 1823 - 29 décembre 1891) est un mathématicien et logicien allemand. Il est l'élève et l'ami à vie d'Ernst Kummer. Persuadé que l'arithmétique et l'analyse doivent être fondées sur les " nombres entiers ", il est célèbre pour la citation suivante : " Dieu fit les nombres naturels ; tout autre est l'oeuvre de l'homme " (Bell, 1986, p. 477). Cela met Kronecker en opposition avec Georg Cantor au sujet de quelques-unes de ses extensions mathématiques. Le point de vue de Kronecker sera repris par Hermann Weyl au siècle suivant. http ://fr.wikipedia.org/wiki/Leopold_Kronecker

par suite : $\forall\, f \in E^*,\ \exists\, \alpha_1 = f\left(\overrightarrow{e}_1\right),\ \alpha_2 = f\left(\overrightarrow{e}_2\right),\ \ldots\ , f\left(\overrightarrow{e}_n\right) \in \mathbb{K}$;

$$f = \alpha_1 {e_1}' + \alpha_2 {e_2}' + \ \ldots\ + \alpha_n {e_n}'$$

ce qui montre que $\mathcal{B}'$ est une partie génératrice de E'.

2. $\mathcal{B}'$ est une partie libre de E^*.
Soient $\alpha_1,\ \ldots\ , \alpha_n \in \mathbb{K}$, alors :

$$\begin{aligned}
\alpha_1 {e_1}' + \ \ldots\ + \alpha_n {e_n}' = 0 \quad &\Longrightarrow \forall\, j \in \{1, \ldots, n\},\ \ \Big(\alpha_1 {e_1}' + \ \ldots\ + \alpha_n {e_n}'\Big)(\overrightarrow{e}_j) = 0 \\
&\Longrightarrow \forall\, j \in \{1, \ldots, n\},\ \ \alpha_j {e_j}'(\overrightarrow{e}_j) = 0, \text{ car } k \neq j \Longrightarrow {e_k}'(\overrightarrow{e}_j) = 0 \\
&\Longrightarrow \forall\, j \in \{1, \ldots, n\},\ \ \alpha_j = 0
\end{aligned}$$

ce qui montre que $\mathcal{B}'$ est libre.
De **1.** et **2.** on déduit que $\mathcal{B}'$ est une base de $E*$. □

De cette proposition, il est clair que

$$\boxed{\dim E = \dim E^*}$$

Chapitre 7

MATRICES

7.1 Matrice associée à une application linéaire

Soient E et F deux $\mathbb{K}$-espaces vectoriels de dimensions finies, n et m, et $\mathcal{B}_1 = \{\overrightarrow{e_1}, \ldots, \overrightarrow{e_n}\}$ et $\mathcal{B}_2 = \{\overrightarrow{f_1}, \ldots, \overrightarrow{f_m}\}$ des bases, respectivement de E et F. On considère une application linéaire $g : E \longrightarrow F$.
Sachant que pour tout $\overrightarrow{x} \in E$, il existe $x_1, \ldots, x_n \in \mathbb{K}$, uniques, tels que

$$\overrightarrow{x} = \sum_{i=1}^{n} x_i \, \overrightarrow{e_i}$$

alors de la linéarité de l'application g on obtient :

$$g(\overrightarrow{x}) = \sum_{i=1}^{n} x_i g(\overrightarrow{e_i})$$

et comme $\mathcal{B}_2$ est une base de F, alors pour tout $i \in \{1, \ldots, n\}$ il existe β_{ij}, $j = 1, \ldots, m$, uniques tels que

$$g(\overrightarrow{e_i}) = \sum_{j=1}^{m} \beta_{ij} \, \overrightarrow{f_j}$$

d'où on déduit

Proposition 7.1 *Etant données $\mathcal{B}_1$ et $\mathcal{B}_2$ des bases de E et F, alors pour tout $i = 1, \ldots, n$, il existe m scalaires uniques β_{ij}, $j = 1, \ldots, m$ tels que :*

$$\forall \, \overrightarrow{x} = \sum_{i=1}^{n} x_i \, \overrightarrow{e_i} \in E, \quad g(\overrightarrow{x}) = \sum_{j=1}^{m} \sum_{i=1}^{n} x_i \beta_{ij} \, \overrightarrow{f_i}$$

- On convient de noter : $\overrightarrow{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, et les x_i sont appelés "composantes du vecteur x dans la base $\mathcal{B}_1$"

- ${}^T(x_1, \ldots, x_n)$ est le "*transposé du vecteur* $\overrightarrow{x}$"
- $M_g(\mathcal{B}_1, \mathcal{B}_2) = \begin{pmatrix} \beta_{11} & \beta_{21} & \ldots & \beta_{n1} \\ \beta_{12} & \beta_{22} & \ldots & \beta_{n2} \\ \beta_{13} & \beta_{23} & \ldots & \beta_{n3} \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \beta_{1m} & \beta_{2m} & \ldots & \beta_{nm} \end{pmatrix}$ est appelée "*Matrice associée à l'application g, relativement aux bases* $\mathcal{B}_1$ *et* $\mathcal{B}_2$".
- $(\beta_{1j}\ \beta_{2j}\ \ldots\ \beta_{nj})$ est la j-ème ligne de la matrice $M_g(\mathcal{B}_1, \mathcal{B}_2)$, $j \in \{1, \ldots, m\}$, et $\begin{pmatrix} \beta_{i1} \\ \beta_{i2} \\ \vdots \\ \beta_{im} \end{pmatrix}$ sa i-ème colonne, $i \in \{1, \ldots, n\}$.

$$ {}^T M_g(\mathcal{B}_1, \mathcal{B}_2) = \begin{pmatrix} \beta_{11} & \beta_{12} & \ldots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \ldots & \beta_{2n} \\ \beta_{31} & \beta_{32} & \ldots & \beta_{3n} \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \beta_{m1} & \beta_{m2} & \ldots & \beta_{mn} \end{pmatrix} $$

est la "*Matrice transposée de* $M_g(\mathcal{B}_1, \mathcal{B}_2)$". Cette matrice est obtenue en mettant les colonnes de $M_g(\mathcal{B}_1, \mathcal{B}_2)$ sous forme de lignes.

On remarque que :

Proposition 7.2 *A toute application linéaire* $g \in \mathcal{L}(E, F)$ *est associée une unique matrice* $M_g(\mathcal{B}_1, \mathcal{B}_2)$*, relativement à deux bases données* $\mathcal{B}_1$ *et* $\mathcal{B}_2$*, respectivement de* E *et* F*.*

Inversement, étant donnée une matrice

$$ M = \begin{pmatrix} \beta_{11} & \beta_{21} & \ldots & \beta_{n1} \\ \beta_{12} & \beta_{22} & \ldots & \beta_{n2} \\ \beta_{13} & \beta_{23} & \ldots & \beta_{n3} \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \beta_{1m} & \beta_{2m} & \ldots & \beta_{nm} \end{pmatrix} $$

alors l'application $g : E \longrightarrow F$ définie par :

$$ \forall\ \overrightarrow{x} = \sum_{i=1}^{n} x_i\ \overrightarrow{e_i} \in E, \quad g(\overrightarrow{x}) = \sum_{j=1}^{m} \sum_{i=1}^{n} x_i \beta_{ij}\ \overrightarrow{f_i} $$

est une application linéaire et la matrice associée à g, relativement aux bases $\mathcal{B}_1$ et $\mathcal{B}_2$, est égale à M.

7.1.1 Matrices de passage

7.2 Opérations sur les matrices

7.2.1 Somme des deux matrices

7.2.2 Produit de matrices

7.2.3 Matrices et Changements de bases

7.3 Anneaux des matrices carrées

7.4 Applications multilinéaires

7.4.1 Déterminants de matrices carrées

7.4.2 Rang d'une matrice

7.4.3 Application du calcul des déterminants

7.4.4 Matrice des co-facteurs

7.4.5 Inversion de matrices carrées

7.5 Résolution de systèmes de Cramer

[1]

7.6 Valeurs propres et vecteurs propres

multiplicité d'une valeur propre
Espace propre associé à une valeur propre

7.6.1 Diagonalisation des matrices

7.6.2 Tringularisation des matrices

[1] Mathématiciens ...