Licence 1 Sciences & Technologies

Algèbre - Semestre 2

Université du Littoral - Côte d'Opale, La Citadelle

Laurent SMOCH

Janvier 2009

Laboratoire de Mathématiques Pures et Appliquées Joseph Liouville
Université du Littoral, zone universitaire de la Mi-Voix, bâtiment H. Poincarré
50, rue F. Buisson, BP 699, F-62228 Calais cedex

Table des matières

Chapitre 1

Ensembles, relations d'équivalence et applications

1.1 Introduction

Depuis le début du XX^{e} siècle, l'utilisation du vocabulaire de la théorie des ensembles a permis de clarifier, simplifier, unifier toutes les mathématiques. Depuis de nombreuses années, ce vocabulaire s'est fixé et est devenu la langue universelle de ceux et celles qui font ou utilisent des mathématiques. Son emploi induit des modes de raisonnement simples, clairs, généraux, et l'étudiant peut ainsi cheminer sur une voie sûre. Le but est ici d'exposer un vocabulaire et des propriétés utilisables et utilisés dans tous les domaines des mathématiques, sans masquer inutilement la puissance de leus généralité, mais également sans développement stérile.

On développera dans cette partie les notions suivantes :
- les objets fondamentaux de l'algèbre que sont les **ensembles**,
- les **relations**, qui mettent en liaison des éléments de deux ensembles ou d'un même ensemble,
- les **applications**, qui à chaque élément de l'ensemble de départ, associent un élément et un seul de l'ensemble d'arrivée.

1.2 Ensembles

1.2.1 Éléments de logique

Définition 1.2.1 *Une **assertion** (ou **propriété**) p peut être vraie (V) ou fausse (F), une **table de vérité** consignant ces deux possibilités.*

p	V	F

Un théorème, une proposition, sont des assertions vraies.

Définition 1.2.2 *La **négation** d'une asssertion p est l'assertion notée non p ou $\neg p$ (ou $\rceil p$), définie dans la table de vérité ci-dessous :*

p	V	F
non p	F	V

Définition 1.2.3 *les **connecteurs logiques** "et" (conjonction), "ou" (disjonction), "$\Rightarrow$" (implication), "$\Leftrightarrow$" (équivalence) sont définis par*

p	q	p *et* q	p *ou* q	$p \Rightarrow q$	$p \Leftrightarrow q$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	F	V	V	F
F	F	F	F	V	V

Remarque 1.2.1

- "et" peut se noter $\wedge$. "ou" peut se noter $\vee$.
- Il peut être commode de noter $\left\{ \begin{array}{l} p \\ q \end{array} \right.$ au lieu de "p et q".
- Dans l'implication $p \Rightarrow q$, p s'appelle l'**hypothèse** et q la **conclusion**.
- L'implication $q \Rightarrow p$ s'appelle la **réciproque** de l'implication $p \Rightarrow q$.
- On peut exprimer $p \Rightarrow q$ de l'une des façons suivantes :
  - pour que p, il faut que q,
  - pour que q, il suffit que p,
  - si p, alors q,
  - p est une condition suffisante (CS) pour q,
  - q est une condition nécessaire (CN) de p.
- L'équivalence logique $p \Leftrightarrow q$ peut s'exprimer par :
  - pour que p, il faut et il suffit que q,
  - p est une condition nécessaire et suffisante (CNS) pour q,
  - p si et seulement si (ssi) q.

Définition 1.2.4 *Un* ***théorème de logique****, appelé aussi* ***tautologie****, est une assertion vraie quelles que soient les valeurs de vérité des éléments qui la composent.*

Exemple 1.2.1

1. $(p$ ou $p) \Leftrightarrow p$,
2. $(p$ et $p) \Leftrightarrow p$,
3. p ou (non p) (tiers exclu)
4. non (p et (non p)),
5. $p \Rightarrow p$,
6. $p \Leftrightarrow p$,
7. (non (non p)) $\Rightarrow p$,
8. (p et ($p \Rightarrow q$)) $\Rightarrow q$) (règle d'inférence ou syllogisme),
9. $(p \Rightarrow q) \Leftrightarrow$ ((non p) ou q),
10. $(p \Rightarrow q) \Leftrightarrow$ ((non q) $\Rightarrow$ (non p) (principe de contraposition),
11. (non (p ou q)) $\Leftrightarrow$ ((non p) et (non q)) (loi de Morgan),
12. (non (p et q)) $\Leftrightarrow$ ((non p) ou (non q)) (loi de Morgan),
13. (non ($p \Rightarrow q$)) $\Leftrightarrow$ (p et (non q)) (négation d'une implication),
14. (p et q et $r) \Leftrightarrow$ (p et (q et r)) (associativité du "et"),
15. (p ou q ou $r) \Leftrightarrow$ (p ou (q ou r)) (associativité du "ou"),

16. $(p$ et q ou $r) \Leftrightarrow (p$ ou $r)$ et $(q$ ou $r))$ (distributivité de "ou" sur "et"),
17. $(p$ ou q et $r) \Leftrightarrow (p$ et $r)$ ou $(q$ et $r))$ (distributivité de "et" sur "ou"),
18. $((p \Rightarrow q)$ et $(q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$ (transitivité de l'implication),

Exercice 1 Illustrer à l'aide d'une table de vérité le théorème de logique relatif à la négation d'une implication.
Correction :

p	q	$p \Rightarrow q$	non $(p \Rightarrow q)$	non q	p et (non q)	(non $(p \Rightarrow q)) \Leftrightarrow (p$ et (non $q))$
V	V	V	F	F	F	V
V	F	F	V	V	V	V
F	V	V	F	F	F	V
F	F	V	F	V	F	V

Exercice 2 Montrer que la proposition composée $p \vee \neg p$ est une tautologie.
Correction :

p	$\neg p$	$p \vee \neg p$
V	F	V
F	V	V

Exercice 3 Montrer que la proposition composéee $p \wedge \neg p$ est une contradiction.
Correction :

p	$\neg p$	$p \wedge \neg p$
V	F	F
F	V	F

Exercice 4 (*non corrigé*) Prouver chaque théorème de logique proposé précédemment à l'aide d'une table de vérité.

Exercice 5 (*non corrigé*) Montrer les théorèmes de logique suivants :

1. $(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$,
2. $(p \Leftrightarrow (q \Rightarrow r)) \Leftrightarrow ((p$ et $q) \Rightarrow r)$
3. $\left\{ \begin{array}{l} p \Rightarrow q \\ q \Rightarrow r \\ r \Rightarrow p \end{array} \right. \Rightarrow \left\{ \begin{array}{l} p \Leftrightarrow q \\ p \Leftrightarrow r \\ q \Leftrightarrow r \end{array} \right.$,
4. $((p$ ou $q) \Rightarrow) \Leftrightarrow ((p \Rightarrow r)$ et $(q \Rightarrow r))$.

Exercice 6 (*non corrigé*) Nier les propositions suivantes :

1. Tous les hommes sont mortels.

2. Je mange beaucoup et je ne grossis pas.
3. Dans toute école, il y a un élève qui n'aime aucun professeur.
4. S'il pleut, je joue aux dominos ou je vais au cinéma.
5. En septembre, tous les jours, il a plu et il y a eu du brouillard.
6. Si je ne me trompe pas, tu es riche et célèbre.
7. Si tu travailles bien et si tu es doué, tu réussis tes examens.
8. Il existe un pays dont chaque ville possède un quartier mal famé.
9. Toutes les suédoises sont blondes et ont les yeux bleus.
10. Tout homme, quand il est amoureux, devient stupide.
11. Dans tout livre, une page au moins compte plusieurs coquilles.

Exercice 7 (*non corrigé*) Compléter les phrases suivantes par "il faut", "il suffit" ou "il faut et il suffit" :

1. Pour qu'un quadrilatère soit un carré, ... qu'il soit un rectangle.
2. Pour qu'un triangle soit équilatéral, ... qu'il ait deux angles de 60^o.
3. Pour qu'un rectangle soit un carré, ... qu'il soit un losange.
4. Pour qu'un quadrilatère soit un losange, ... qu'il soit un carré.
5. Pour qu'un parallélogramme soit un losange, ... que ses diagonales soient perpendicualires.
6. Pour qu'un quadrilatère soit un parallélogramme, ... que ses diagonales se coupent en leur milieu.
7. Pour que la vitesse moyenne d'un automobiliste sur un certain trajet soit supérieure à 90km/h, ... que sa vitesse instantanée ait été à un moment supérieure à 90km/h.
8. Pour que la vitesse moyenne d'un automobiliste sur un certain trajet soit supérieure à 90km/h, ... que sa vitesse instantanée ait été constamment supérieure à 90km/h.

1.2.2 Ensembles

On commence tout d'abord par présenter les quantificateurs universels $\forall$ et $\exists$.

- le quantificateur $\forall$ se lit "pour tout" ou "quel que soit".

$$\boxed{(\forall x \in E,\ P(x)) \text{ se lit : "pour tout } x \text{ appartenant à } E, \text{ on a } P(x)"}$$

- le quantificateur $\exists$ se lit "il existe au moins un élément".

$$\boxed{(\exists x \in E,\ P(x)) \text{ se lit : "il existe au moins un élément } x \text{ appartenant à } E \text{ tel que l'on ait } P(x)}$$

Remarque 1.2.2

- La notation $\exists!$ signifie "il existe un unique élément".
- La lettre affectée par un quantificateur est muette, elle peut être remplacée par n'importe quelle lettre n'ayant pas déja une signification :

$$(\forall x \in E, P(x)) \Leftrightarrow (\forall y \in E, P(y)),$$
$$(\exists x \in E, P(x)) \Leftrightarrow (\exists y \in E, P(y)).$$

– Les quantificateurs permettent également d'exprimer la négation d'une phrase quantifiée à savoir
$$(\text{non } (\forall x \in E, P(x))) \Leftrightarrow (\exists x \in E, \text{non } P(x)),$$
$$(\text{non } (\exists x \in E, P(x))) \Leftrightarrow (\forall x \in E, \text{non } P(x)).$$

– Dans une phrase quantifiée, on ne peut pas à priori modifier l'ordre des quantificateurs. Par exemple $(\forall x \in \mathbb{N}, \exists y \in \mathbb{N}, x \leq y)$ est vraie mais $(\exists y \in \mathbb{N}, \forall x \in \mathbb{N}, x \leq y)$ est fausse.

Cependant, si les ensembles E et E' sont fixés :
$$(\forall x \in E, \forall x' \in E', P(x, x')) \Leftrightarrow (\forall x' \in E', \forall x \in E, P(x, x'))$$
et
$$(\exists x \in E, \exists x' \in E', P(x, x')) \Leftrightarrow (\exists x' \in E', \exists x \in E, P(x, x'))$$

Exercice 8 Soit F l'ensemble des femmes et H celui des hommes et $M(x, y)$ la proposition "x est marié à y". Énoncer par des phrases correctes les propositions
$$(\exists y \in H)(\forall x \in F)M(x, y)$$
et
$$(\forall x \in F)(\exists y \in H)M(x, y)$$

Ces deux propositions ont-elles le même sens ?
Correction : La proposition $(\exists y \in H)(\forall x \in F)M(x, y)$ peut se traduire par "il existe au moins un homme qui est marié avec toutes les femmes".
La proposition $(\forall x \in F)(\exists y \in H)M(x, y)$ peut se traduire par "chaque femme est mariée avec au moins un homme".
Ces deux propositions n'ont bien évidemment pas le même sens.

Définition 1.2.5 *En théorie des ensembles, un* ***ensemble*** *désigne intuitivement une collection d'objets (que l'on appelle* ***éléments de l'ensemble****), "une multitude qui peut être comprise comme un tout", comme l'énonçait le créateur de cette théorie, le mathématicien Georg CANTOR (1845-1918).*

Ceci était particulièrement novateur, s'agissant d'ensembles éventuellement infinis (et ce sont ces derniers qui intéressent Cantor).

Un ensemble peut être vu comme une sorte de sac virtuel entourant ses éléments, ce que modélisent bien les **diagrammes de Venn**. Souvent (ce n'est pas toujours possible), on essaye de le distinguer typographiquement de ses éléments, par exemple en utilisant une lettre latine majuscule, par exemple "E" ou "A", pour représenter l'ensemble, et des minuscules, telles que "x" ou "n", pour ses éléments.
Les éléments peuvent être de n'importe quelle nature : nombres, points géométriques, droites, fonctions, autres ensembles ... On donne donc volontiers des exemples d'ensembles en dehors du monde mathématique. Par exemple, lundi est un élément de l'ensemble des jours de la semaine, une bibliothèque est un ensemble de livres, etc.
Un même objet peut être élément de plusieurs ensembles : 4 est un élément de l'ensemble des nombres entiers, ainsi que de l'ensemble des nombres pairs (forcément entiers). Ces deux derniers ensembles sont infinis, ils ont une infinité d'éléments.

Ce qui est manifestement en jeu au premier chef dans la notion d'ensemble, c'est la relation dappartenance : un élément appartient à un ensemble. Ce sont les propriétés de cette relation que l'on axiomatise en théorie des ensembles, et il est assez remarquable que l'on puisse s'en contenter pour une théorie qui peut potentiellement formaliser les mathématiques (ce qui n'était pas encore clair à l'époque de Cantor).

Définition 1.2.6

- *On appelle* ***ensemble vide****, et on note* $\emptyset$*, un ensemble ne contenant aucun élément. Il n'existe qu'un seul ensemble vide.*
- *Si* x *est un objet quelconque, on appelle* ***singleton*** x *ou* ***ensemble réduit à*** x*, et on note* $\{x\}$*, l'ensemble ne contenant qu'un seul objet, qui est égal à* x*.*
- *Par extension, on peut définir un* ***ensemble fini*** *en énumérant ses éléments :* $\{a, b, \dots, z\}$*.*
- *Si* $P(x)$ *est un prédicat, on note* $\{x; P(x)\}$*, ou* $\{x/P(x)\}$*, ou* $\{x, P(x)\}$*, l'ensemble des éléments* x *tels que l'assertion* $P(x)$ *soit vraie. Attention, tous les prédicats ne peuvent pas définir un ensemble.*

On désigne généralement les ensembles les plus usuels par une lettre en gras ou à double barre :
- $\mathbb{N}$ l'ensemble des entiers naturels,
- $\mathbb{N}^\star$ l'ensemble des entiers positifs,
- $\mathbb{Z}$ l'ensemble des entiers relatifs (positifs, négatifs ou nuls),
- $\mathbb{Z}^\star$ l'ensemble des entiers différents de 0,
- $\mathbb{Q}$ l'ensemble des nombres rationnels $\left(\frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{Z}^\star\right)$,
- $\mathbb{R}$ l'ensemble des réels,
- $\mathbb{R}^+$ l'ensemble des réels positifs,
- $\mathbb{R}^\star$ l'ensemble des réels autres que 0,
- $\mathbb{C}$ l'ensemble des nombres complexes.

Définition 1.2.7 *Soit* E *un ensemble, on appelle* ***élément de*** E *tout objet appartenant à* E*, et on note* $x \in E$*.*

Dans la suite, on utilisera souvent la notion de famille d'objets.

Définition 1.2.8 *On appelle* ***famille d'ensembles*** $(E_i)_{i\in I}$*, avec* $\forall i \in I$*,* $E_i \subset E$*, l'application*

$$\begin{array}{ccc} I & \to & E \\ i & \mapsto & E_i \end{array}.$$

Une famille est appelée ***suite*** *dans le cas particulier où* I *est l'ensemble* $\mathbb{N}$ *des entiers naturels, éventuellement privé d'un nombre fini d'éléments.*

Exercice 9 Écrire en extension (c'est-à-dire en donnant tous leurs éléments) les ensembles suivants :

$$A = \left\{\text{nombres entiers compris entre } \sqrt{2} \text{ et } 2\pi\right\},$$
$$B = \left\{x \in \mathbb{C};\ \exists (n,p) \in \mathbb{N}\times\mathbb{N}, x = \frac{n}{p} \text{ et } 1 \le p \le 2n \le 7\right\}.$$

Correction : On a $A = \{2, 3, 4, 5, 6\}$ et $B = \left\{\frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, 1, \frac{3}{2}, 2, 3\right\}$.

Définition 1.2.9 *On dit qu'un ensemble* E *est une* ***partie d'un ensemble*** F*, ou que* E *est un* ***sous-ensemble*** *de* F*, ou que* E *est* ***inclus*** *dans* F*, ou que* F *est un* ***sur-ensemble*** *de* E*, et on note* $E \subset F$*, si tout élément de* E *est aussi élément de* F*.*

Remarque 1.2.3 Soit E un ensemble. Alors E et $\emptyset$ sont des parties de E.

Notation : Soit E un ensemble, on note $\mathcal{P}(E)$ **l'ensemble des parties** de E.

Exercice 10 Écrire l'ensemble des parties de $E = \{a, b, c, d\}$.
Correction : $\mathcal{P}(E) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, E\}$.

Définition 1.2.10 *Soit E un ensemble. On appelle* ***partie propre*** *de E toute partie de E distincte de E et de $\emptyset$.*

Introduisons maintenant les notions de réunion, d'intersection, de complémentation, de différence et de différence symétrique.

Définition 1.2.11 *Soient A et B deux sous-ensembles de E.*

- *On appelle* ***réunion*** *de A et B, et on note $A \cup B$, l'ensemble formé par les éléments de A ou les éléments de B.*
$$\boxed{A \cup B = \{x \in E / x \in A \text{ ou } x \in B\}},$$
- *On appelle* ***intersection*** *de A et B, et on note $A \cap B$, l'ensemble des objets appartenant à la fois à A et à B.*
$$\boxed{A \cap B = \{x \in E / x \in A \text{ et } x \in B\}},$$
- *Deux sous-ensembles A et B de l'ensemble E sont dits* ***complémentaires*** *si leur réunion est l'ensemble E et leur intersection l'ensemble vide :*
$$\boxed{A \cup B = E \text{ et } A \cap B = \emptyset}$$
On note alors $B = C_E^A$ ou $B = \overline{A}$ ou $B = A^c$.
- *On appelle* ***différence*** *de A et B, et on note $A \backslash B$ (ou $A - B$), l'ensemble des éléments de A qui n'appartiennent pas à B soit $A \cap B^c$.*
- *On appelle* ***différence symétrique*** *de A et B, et on note $A \Delta B$, la réunion de $A \backslash B$ et $B \backslash A$.*

Exemple 1.2.2 *Posons $E = \{1, 2, 3, 4\}$, $A = \{1, 2\}$ et $B = \{2, 3\}$. On a alors $A \cup B = \{1, 2, 3\}$, $A \cap B = \{2\}$, $A^c = \{3, 4\}$, $B^c = \{1, 4\}$, $A \backslash B = \{1\}$, $B \backslash A = \{3\}$ et $A \Delta B = \{1, 3\}$.*

Remarque 1.2.4

- Les définitions de la réunion, de l'intersection et de la différence symétrique sont symétriques en E et F.
- Les définitions de la réunion et de l'intersection se généralisent à une famille quelconque d'ensembles $(E_i)_{i \in I}$:
$$\cup E_i = \{x; \exists i \in I, x \in E_i\}$$
$$\cap E_i = \{x; \forall i \in I, x \in E_i\}$$

Propriété 1.2.1 *Soient A, B, C des ensembles quelconques. On a les propriétés suivantes :*

- $A \cap B = B \cap A$, $A \cup B = B \cup A$ *(commutativité)*
- $(A \cap B) \cap C = A \cap (B \cap C)$, $(A \cup B) \cup C = A \cup (B \cup C)$ *(associativité)*
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(distributivité)*
- $A \cup A = A$, $A \cap A = A$
- $(A \subset C \text{ et } B \subset C) \Rightarrow (A \cup B) \subset C$
- $(C \subset A \text{ et } C \subset B) \Rightarrow C \subset (A \cap B)$
- $A \subset B \Rightarrow C \backslash B \subset C \backslash A$
- $A \subset B \Rightarrow A \backslash C \subset B \backslash C$
- $A = (A \cap B) \cup A \backslash B$

Propriété 1.2.2 *(Lois de Morgan) Quels que soient les sous-ensembles A et B de E, on a*

$$\boxed{\begin{array}{l}(A \cup B)^c = A^c \cap B^c \\ (A \cap B)^c = A^c \cup B^c\end{array}}$$

On dit qu'il existe une dualité entre les opérations de réunion et d'intersection.

Propriété 1.2.3 *(Généralisation) Soient $I \subset \mathbb{N}$ un ensemble et $(A_i)_{i\in I}$ une famille de parties de E. Les lois de Morgan ci-dessus s'étendent à une famille de parties de E sous la forme :*

$$(\bigcup_i A_i)^c = \bigcap_i A_i^c$$
$$(\bigcap_i A_i)^c = \bigcup_i A_i^c$$

Exercice 11 (*non corrigé*) On appelle **fonction caractéristique** de A (partie de l'ensemble E) une application f de E dans l'ensemble à deux éléments $\{0, 1\}$ telle que

$$f(x) = 0 \text{ si } x \notin A$$
$$f(x) = 1 \text{ si } x \in A$$

Soient A et B deux parties de E et leurs fonctions caractéristiques f et g. Quels sont les ensembles A_1, A_2 et A_3 dont les fonctions caractéristiques sont

1. $1 - f$,
2. fg,
3. $f + g - fg$.

Définition 1.2.12 *Soient E un ensemble et $(E_i)_{i\in I}$ une famille de parties de E. On appelle* ***recouvrement*** *de E la réunion $E = \cup_i E_i$ c'est-à-dire que $\forall x \in E$, $\exists E_i$ tel que $x \in E_i$. Si de plus*
- *$\forall (i, j) \in I \times I$, $i \neq j \Rightarrow E_i \cap E_j = \emptyset$,*
- *les E_i sont tous non vides.*

on dit que les E_i forment une ***partition*** *de E.*

Exemple 1.2.3 Dans le cas $E = \mathbb{R}^2$, les perpendiculaires à l'axe $(0x)$ aux points d'abscisses $x_1, x_2, \ldots, x_n, \ldots$, $\forall x_i \in \mathbb{R}$ forment une partition de E.

Introduisons enfin la notion d'ensemble-produit :

Définition 1.2.13 *Soient deux ensembles A et B et deux éléments a et b avec $a \in A$ et $b \in B$. L'ensemble des couples (a, b) pris dans cet ordre est appelé* ***produit cartésien*** *des ensembles A et B. On le note $A \times B$.*

Remarque 1.2.5 La précision de l'ordre a puis b n'est pas superflue. Tout couple appartenant à $A \times B$ est constitué d'un élément appartenant à A puis d'un élément appartenant à B. (b, a) n'est pas en général un élément de $A \times B$ (ce n'est le cas que si a et $b \in A \cap B$).

Définition 1.2.14 *Soit $(E_i)_{i\in I}$ une famille d'ensembles. On note E_i, et on appelle* ***ensemble-produit*** *des E_i, l'ensemble des familles $(x_i)_{i\in I}$ avec $x_i \in E_i$.*

Si les E_i sont en nombre fini, par exemple $I = \{1, 2, \ldots, n\}$, on peut noter $E = E_1 \times E_2 \times \ldots E_n$. Si de plus tous les E_i sont égaux, on peut écrire $E \times E \times \ldots \times E = E^n$.

1.2.3 Lois de composition

Définition 1.2.15 *Étant donnés trois ensembles E, F et G (non vides), toute application de $E \times F$ (produit cartésien de E par F) vers G est appelée* ***loi de composition*** *de $E \times F$ à valeurs dans G.*

Définition 1.2.16 *Une loi de composition* ***interne*** *- lci - (ou simplement loi interne) dans E est une loi de composition de $E \times E$ à valeurs dans E (cas $E = F = G$).*

Exemple 1.2.4
- L'addition est une loi interne dans $\mathbb{N}$, ensemble des entiers naturels.

– la soustraction n'est pas une loi interne dans $\mathbb{N}$, $2-3$ n'est pas un entier naturel, mais elle en est une dans $\mathbb{Z}$, ensemble des entiers relatifs.

Définition 1.2.17 *Une loi de composition* ***externe*** *(ou simplement loi externe) dans E est une loi de composition de $F \times E$ à valeurs dans E, où F est un ensemble distinct de E. Une telle loi à valeurs dans E est aussi appelée* ***action*** *de F sur E. L'ensemble F est alors le domaine d'opérateurs. On dit aussi que F opère sur E.*

Pour simplifier, on donne un nom et une notation pour désigner la loi de composition : si c est l'image du couple (a, b) par la loi de composition notée T, on note $c = aTb$. Lorsque la loi s'apparente à une multiplication on la note souvent $\times$. L'appellation opération est généralement utilisée et réservée pour les lois de composition interne.

Exemple 1.2.5
- La multiplication d'un vecteur par un nombre réel où F est généralement un corps (voir plus loin), dit corps de scalaires, est une loi de composition externe d'un espace vectoriel.
- L'application qui à tout couple (E, F) d'ensembles, associe l'ensemble $E \times F$ pourrait être considérée comme une loi de composition interne dans l'ensemble de tous les ensembles. Hélas, ce dernier ensemble n'est pas un ensemble ...

Définition 1.2.18 *Soit E un ensemble muni d'une loi de composition interne T.*
- *Si, pour tout couple (x, y) d'éléments de E, on a $xTy = yTx$, la loi T est dite* ***commutative.***
- *Si, pour tout triplet (x, y, z) d'éléments de E, on a $(xTy)Tz = xT(yTz)$, la loi T est dite* ***associative.***
- *Soit $e \in E$ vérifiant $\forall x \in E$, $xTe = eTx = x$, on dit alors que e est un* ***élément neutre*** *de E pour la loi T.*

Exercice 12 (*non corrigé*) Soit l'ensemble des parties d'un ensemble à deux éléments, par exemple $E = \mathcal{P}(\{0, 1\})$. Donc, $E = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$. On considère les lois de composition "$\star$" suivantes sur l'ensemble E.
- Réunion : $A \star B = A \cup B$
- Intersection : $A \star B = A \cap B$
- Différence symétrique : $A \star B = A \Delta B = (A \backslash B) \cup (B \backslash A)$
- Réunion des complémentaires : $A \star B = A^c \cup B^c$
- Intersection des complémentaires : $A \star B = A^c \cap B^c$

Pour chacune d'entre elles :
1. Écrire la table de composition de la loi .
2. L'ensemble E possède-t-il un élément neutre pour la loi $\star$?
3. La loi est-elle associative ?
4. La loi est-elle commutative ?
5. Répondre aux questions 2. à 4. en remplaçant E par l'ensemble des parties d'un ensemble quelconque.

Exercice 13 (*non corrigé*) Sur $E = \{a, b, c\}$ on définit une loi de composition interne $*$ par sa table de Pythagore :

$*$	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

1. Calculer $(a * b) * c$ et $(a * c) * b$.
2. Trouver les propriétés de cette loi (commutativité, associativité).
3. Admet-elle un élément neutre ?

Exercice 14 (*non corrigé*) On munit $\mathbb{R}$ de la loi de composition interne $*$ définie par :

$$\forall x, y \in \mathbb{R},\ x * y = xy + (x^2 - 1)(y^2 - 1)$$

Montrer que $*$ est commutative, non associative, et que 1 est élément neutre.

1.3 Relations d'équivalence et relations d'ordre

Le concept de relation est la base de toute la mathématique dont le but est d'étudier - par observation et déduction (raisonnement), calcul et comparaison - des configurations abstraites ou concrètes de ses objets (nombres, formes, structures) en cherchant à établir les liens logiques, numériques ou conceptuels entre ces objets.

1.3.1 Relations binaires

Définition 1.3.1 *Soit x un élément d'un ensemble E et y un élément d'un ensemble F. Une **relation** $\mathcal{R}$ entre x et y est un lien verbal caractérisant la correspondance entre x et y.*

Lorsque le couple (x, y) vérifie la relation $\mathcal{R}$, on note $x\mathcal{R}y$. On dit que x est en relation avec y.

Définition 1.3.2 *L'ensemble des couples (x, y) de $E \times F$ tels que $x\mathcal{R}y$ est appelé **graphe** de la relation. On note*

$$G = \{(x, y) \in E \times F / x\mathcal{R}y\}$$

On remarque que $G \subset E \times F$.

Définition 1.3.3 *Si x et y appartiennent au même ensemble E, la relation $\mathcal{R}$ est appelée **relation binaire** dans E. C'est une partie du produit $E \times E$.*

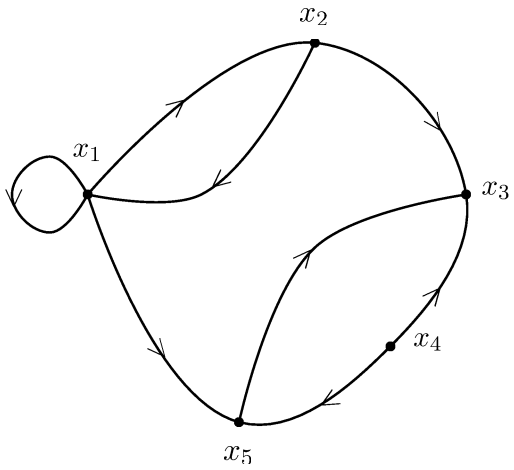
Proposition 1.3.1 *Une relation binaire est caractérisée*

- *par son graphe*
- *par sa **représentation sagittale***
- *par sa **représentation cartésienne***
- *par sa **matrice booléenne***
- *par son **dictionnaire des sommets***
  - *. des **suivants** ou des **successeurs** (si $x\mathcal{R}y$, y est le suivant de x).*
  - *. des **précédents** ou des **prédécesseurs** (si $x\mathcal{R}y$, x est le précédent de y)*

Exemple 1.3.1 Soit $E = \{x_1, x_2, x_3, x_4, x_5\}$. On se donne

$$G = \{(x_1, x_1), (x_1, x_2), (x_1, x_5), (x_2, x_1), (x_2, x_3), (x_4, x_3), (x_4, x_5), (x_5, x_3)\}$$

- G est donc le graphe de la relation binaire $\mathcal{R}$.
- La représentation sagittale de $\mathcal{R}$ est :



– La représentation cartésienne de $\mathcal{R}$ est :

départ \ arrivée	x_1	x_2	x_3	x_4	x_5
x_1	$\star$	$\star$			$\star$
x_2	$\star$		$\star$		
x_3					
x_4			$\star$		$\star$
x_5			$\star$		

– La matrice booléenne de $\mathcal{R}$ est :

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

– Le dictionnaire des suivants de $\mathcal{R}$ est :

x	$S(x)$
x_1	x_1, x_2, x_5
x_2	x_1, x_3
x_3	
x_4	x_3, x_5
x_5	x_3

– Le dictionnaire des précédents de $\mathcal{R}$ est :

x	$P(x)$
x_1	x_1, x_2
x_2	x_1
x_3	x_2, x_4, x_5
x_4	
x_5	x_1, x_4

Remarque 1.3.1 La relation $\mathcal{R}^{-1}$ est définie par le graphe

$$G' = \{(x_1, x_1), (x_1, x_2), (x_2, x_1), (x_5, x_1), (x_3, x_2), (x_3, x_4), (x_5, x_4), (x_3, x_5)\}$$

En effet, $x\mathcal{R}y \Leftrightarrow y\mathcal{R}^{-1}x$. La matrice booléenne de $\mathcal{R}^{-1}$ est

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

On remarque alors que les matrices booléennes de $\mathcal{R}$ et $\mathcal{R}^{-1}$ ont leurs termes symétriques par rapport à la diagonale principale.

Exercice 15 (*non corrigé*) On se donne la relation binaire définie par l'ensemble de sommets $E = \{x_1, x_2, x_3, x_4, x_5\}$ et le graphe

$$G = \{(x_1, x_2); (x_1, x_5); (x_2, x_3); (x_2, x_4); (x_4, x_3); (x_4, x_4); (x_4, x_5)\}$$

Caractériser cette relation binaire par

1. sa représentation sagittale,
2. sa représentation cartésienne,
3. sa matrice booléenne.

Définition 1.3.4 *Soit $(E, \odot, \mathcal{R})$ un ensemble muni d'une loi de composition interne et d'une relation binaire. On dit que la relation $\mathcal{R}$ est **compatible avec la loi** $\odot$ si $\forall (x, x', y, y') \in E^4$, $(x\mathcal{R}y$ et $x'\mathcal{R}y') \Rightarrow (x \odot x')\mathcal{R}(y \odot y')$.*
On dit aussi que la relation $\odot$ respecte la loi T.

Exemple 1.3.2 Soit $E = \mathbb{R}$, la relation "$\leq$" est compatible avec la loi "+" car $\forall (x, x', y, y') \in \mathbb{R}^4$, $(x \leq y$ et $x' \leq y') \Rightarrow (x + x') \leq (y + y')$.

1.3.2 Fonctions et applications

Définition 1.3.5 *Si $x\mathcal{R}y$, on dit que y est une **image** de x par la relation $\mathcal{R}$ et que x est un **antécédent** de y par cette même relation.*

Exemple 1.3.3

- Soit $\mathcal{S} : \mathbb{N} \to \mathbb{Z}$ ($E = \mathbb{N}$ et $F = \mathbb{Z}$) et $x\mathcal{S}y$ ssi $x = |y|$. On a $3\mathcal{S}3$ et $3\mathcal{S}(-3)$: 3 possède deux images. Seul 0 possède une seule image.
- Dans $E = F = \mathbb{Z}$, on pose $x\mathcal{R}y$ ssi y est le carré de x. On a $3\mathcal{R}9$ mais l'assertion $z\mathcal{R}8$ est fausse pour tout z de $\mathbb{Z}$: on dira que 8 n'a pas d'antécédent par $\mathcal{R}$ ou que 8 n'est pas une image. On remarque que -3 et 3 ont la même image. 9 est l'unique image de 3 mais 9 est aussi l'image de -3 : le nombre 9 admet deux antécédents qui sont -3 et 3.

Définition 1.3.6 *L'ensemble $\mathcal{D}_\mathcal{R}$ des éléments de E qui ont au moins une image par $\mathcal{R}$ est l'**ensemble** (ou **domaine**) **de définition de** $\mathcal{R}$.*

Définition 1.3.7 *Lorsque chaque élément de E possède au plus une image (aucune ou une seule) par une relation $\mathcal{R}$, on dit que $\mathcal{R}$ est une **fonction** et on note $y = \mathcal{R}(x)$, plutôt que $x\mathcal{R}y$. On dira que y est exprimé en fonction de x : c'est l'unique image de x par $\mathcal{R}$.*

Cette notation, dite fonctionnelle, est due à Gottfried Wilhelm LEIBNIZ (1646-1716) qui utilisait une notation comme $\mathcal{R}_x$ ou f_x. La notation $f(x)$ pour désigner l'image par f d'un élément x nous vient de Alexis Claude CLAIRAUT (1713-1765), Joseph Louis LAGRANGE (1736-1813) et Jean Le Rond d'ALEMBERT (1717-1783). x prend le nom de **variable**.

Exemple 1.3.4 Dans le cas $E = F = \mathbb{Z}$, la relation $\mathcal{R}$ définie par "$x\mathcal{R}y$ si et seulement si y est le carré de x" est une fonction. On peut la rebaptiser f ou bien c comme carré : on écrira $9 = c(-3)$ et d'une façon générale $y = c(x)$ avec $y = x^2$.

Définition 1.3.8 *Si $\mathcal{D}_f = E$, on dira que la fonction f est partout définie, elle prend alors le nom d'**application**.*

Exemple 1.3.5
- La fonction $\mathcal{R}$ ci-dessus (rebaptisée c) est une application.
- La fonction $f : \mathbb{N} \to \mathbb{Q}$, $x \mapsto f(x) = 1/x$ n'est pas une application : 0 n'a pas d'image.
- La projection des points d'une droite D sur un plan P est une application de D dans P.

Notation : On note F^E l'ensemble des applications de E dans F.

Définition 1.3.9 *Soient $(E, \mathcal{R})$ un ensemble muni d'une relation binaire, F un ensemble et f une application de E dans F. On dit que la relation $\mathcal{R}$ est **compatible avec l'application** f si $\forall (x, y) \in E^2$, $x\mathcal{R}y \Rightarrow f(x) = f(y)$.*

Définition 1.3.10 *Soit $f : E \to F$ une fonction. L'ensemble des images par f des éléments de E est noté $f(E)$, ou parfois $Im(f)$ ou $\Im(f)$ si cela n'est pas ambigu, et est appelé **image de E par f**. Si A est inclus dans E, l'image de A par f est l'ensemble des éléments $f(x)$ où x est élément de A :*

$$f(A) = \{y \in F / x \in A, y = f(x)\}$$

Remarque 1.3.2
- si $A \subset B$, alors $f(A) \subset f(B)$. La réciproque est fausse sauf si f est bijective (voir plus loin). Voici un contre-exemple : Soit $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, $A = [-2, 1]$ et $B = [-1, 3]$. $f(A) = [0, 4]$, $f(B) = [0, 9]$. On a $f(A) \subset f(B)$ mais pas $A \subset B$.
- On devra aussi savoir que $f(A \cap B) \subset f(A) \cap f(B)$ et que l'égalité est fausse en général mais que $f(A \cup B) = f(A) \cup f(B)$.

Exercice 16 (*non corrigé*)

1. Prouver les résultats énoncés dans la remarque précédente.
2. Soit $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, $A = [-2, 1]$ et $B = [-1, 3]$. $f(A) = [0, 4]$, $f(B) = [0, 9]$. Comparer $f(A \cap B)$ à $f(A) \cap f(B)$.
   Prouver que $f(A \cup B) = f(A) \cup f(B)$.

Définition 1.3.11 *Soit E un ensemble. L'**application identique** de E (ou **identité** de E), notée Id_E, est l'application de E dans E définie par $\forall x \in E$, $Id_E(x) = x$.*

Nous verrons que cette application joue un rôle important dans la caractérisation des bijections ; elle est également utile en topologie.

Définition 1.3.12 *Soient E un ensemble, f une application de E dans E et A une partie de E. On dit que A est **stable** par f si $f(A) \subset A$.*

Définition 1.3.13 *Soient E, F, G trois ensembles, f une application de E dans F, g une application de F dans G. On appelle* ***application composée*** *de f par g l'application*

$$\begin{array}{rcl}(g_o f) : E & \to & G \\ x & \mapsto & (g_o f)(x) = g(f(x))\end{array}$$

Proposition 1.3.2 *Soient E, F, G, H quatre ensembles, f une application de E vers F, g une application de F vers G, h une application de G vers H. On a $(f_o g)_o h = f_o(g_o h)$.*

Définition 1.3.14

- *Soient E et F deux ensembles et f une application de E dans F. On dit que f est une* ***injection*** *de E dans F (ou f est injective) si :*

$$\boxed{\forall (x, x') \in E^2,\ f(x) = f(x') \Rightarrow x = x'}$$

- *On dit que f est une* ***surjection*** *de E dans F (ou f est surjective) si :*

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

- *On dit que f est une bijection de E sur F (ou f est bijective) si f est à la fois injective et surjective.*

Caractérisation : Avec les mêmes notations, on a :

- f est surjective si et seulement si il existe une application g de F dans E telle que $f_o g = Id_F$. g est alors injective.
- f est injective si et seulement si il existe une fonction g de F dans E telle que $g_o f = Id_E$. g est alors surjective.
- f est bijective si et seulement si il existe une application g de F dans E telle que $f_o g = Id_F$ et $g_o f = Id_E$. g est alors unique, elle est appelée **application inverse** (ou **réciproque**) de f et notée f^{-1}. g est alors également bijective, de réciproque f.

Corollaire 1.3.1 *: Il existe une injection de E dans F si et seulement si il existe une surjection de F dans E.*

Proposition 1.3.3

- *La composée de deux surjections est une surjection.*
- *La composée de deux injections est une injection.*
- *La composée de deux bijections est une bijection.*

Exercice 17 E, F, G sont des ensembles non vides, f est une application de E dans F et g une application de F dans G. Justifier

1. gof injective $\Rightarrow$ f injective
2. gof surjective $\Rightarrow$ g surjective

Correction :

1. Supposons tout d'abord que $g_o f$ soit injective et montrons que f est injective. Soit $(a, a') \in E^2$ avec $f(a) = f(a')$ alors $g_o f(a) = g_o f(a')$ or $g_o f$ est injective donc $a = a'$ ce qui signifie que f est injective.
2. Supposons maintenant que $g_o f$ soit surjective et montrons que g est surjective. Soit $c \in G$, comme $g_o f$ est surjective, il existe $a \in E$ tel que $g_o f(a) = c$. Posons $b = f(a)$ alors $g(b) = c$ ceci quel que soit $c \in G$ donc g est surjective.

Exercice 18 Soit f l'application de $\mathbb{N}$ dans $\mathbb{N}$ qui à un nombre n associe la somme de ses chiffres (par exemple $f(17) = 8$). Soit g l'application de $\mathbb{N}$ dans $\mathbb{N}$ qui à un nombre n associe son dernier chiffre (par exemple $g(17) = 7$).

1. Étudier l'injectivité de f
2. Étudier la surjectivité de f
3. Déterminer $f^{-1}(\{1\})$ et $f^{-1}(\{3\}) \cap [1, 100]$
4. Étudier l'injectivité de g
5. Étudier la surjectivité de g
6. Calculer $g(\mathbb{N})$
7. L'application gof est-elle surjective ? Même question pour fog.

Correction :

1. f est injective ssi $\forall (x, x') \in \mathbb{N}^2$, $f(x) = f(x') \Rightarrow x = x'$. Or $f(17) = f(26) = 8$ et $17 \neq 26$ donc f n'est pas injective.
2. f est surjective ssi $\forall y \in \mathbb{N}$, $\exists x \in \mathbb{N}, f(x) = y$. Il suffit de considérer (par exemple) $x = \underbrace{11\ldots1}_{y \text{ fois}}$.
3. $f^{-1}(\{1\}) = 10^n$ avec $n \in \mathbb{N}$; $f^{-1}(\{3\}) \cap [1, 100] = \{3, 12, 21, 30\}$.
4. On remarque par exemple que $g(27) = g(17) = 7$ donc g n'est pas injective.
5. Soit $y \in \mathbb{N}$. Il est évident que g est surjective lorsque $y \in \{0, \ldots, 9\}$. Mais si $y \geq 10$, y ne représente plus un chiffre mais un nombre ; par conséquent g n'est pas surjective sur $\{y \in \mathbb{N} / y \geq 10\}$. On conclut donc que g n'est pas surjective.
6. $g(\mathbb{N}) = \{0, \ldots, 9\}$ puisqu'on travaille dans la base décimale.
7. – On sait que "$g_o f$ surjective $\Rightarrow$ g surjective ". Il suffit alors d'utiliser la contraposée de cette implication c'est-à-dire "g non surjective $\Rightarrow$ $g_o f$ non surjective" pour affirmer que dans notre cas $f_o g$ n'est pas surjective.
   – Étudions la surjectivité de $f_o g$. On sait que si f et g sont surjectives alors $f_o g$ est surjective mais également que si $f_o g$ est surjective alors f est surjective. On note donc que la surjectivité de f est une condition nécessaire mais pas toujours suffisante pour que $f_o g$ soit surjective. Prenons par exemple $y = 6$ alors, il existe $z \in \mathbb{N}$ ($z = 15$ par exemple) tel que $f(z) = 6$. Mais comme g n'est pas surjective pour $z \geq 10$, $\nexists x \in \mathbb{N}$ tel que $g(x) = 15$ ce qui signifie $\nexists x \in \mathbb{N}$ tel que $f_o g(x) = y$. Donc $f_o g$ n'est pas surjective.

Exercice 19 Soit $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = \dfrac{2x}{1 + x^2}$.

1. f est-elle injective ? surjective ?
2. Montrer que $f(\mathbb{R}) = [-1, 1]$.
3. Montrer que la restriction $g : [-1, 1] \to [-1, 1], g(x) = f(x)$ est une bijection.

Correction :

1. f n'est pas injective car $f(2) = f(1/2) = 4/5$. f n'est pas surjective car $y = 2$ n'a pas d'antécédent. En effet l'équation $f(x) = 2$ devient $2x = 2(1 + x^2)$ soit $x^2 - x + 1 = 0$ qui n'a pas de solution dans $\mathbb{R}$.
2. L'équation $f(x) = y$ est équivalente à l'équation $yx^2 - 2x + y = 0$. Cette équation a des solutions si et seulement si $\Delta = 4 - 4y^2 \geq 0$ donc il y a des solutions ssi $y \in [-1, 1]$. Ainsi on a exactement $f(\mathbb{R}) = [-1, 1]$.
3. Soit $y \in [-1, 1]$. Les solutions possibles de l'équation $g(x) = y$ sont $x = \dfrac{1 - \sqrt{1 - y^2}}{y}$ ou $x = \dfrac{1 + \sqrt{1 - y^2}}{y}$. La deuxième solution n'appartient pas à $[-1, 1]$. D'autre part, $x = \dfrac{1 - \sqrt{1 - y^2}}{y} = \dfrac{y}{1 + \sqrt{1 - y^2}}$ est dans $[-1, 1]$. L'équation $g(x) = y$ admet donc une unique solution avec $x \in [-1, 1]$ ce qui prouve que g est une bijection.

Exercice 20 Soit $f : X \to Y$. Montrer que les conditions suivantes sont équivalentes :

1. f est injective.
2. Pour tous A,B de X, on a $f(A \cap B) = f(A) \cap f(B)$.

Correction :

- Montrons que 1. $\Rightarrow$ 2. Soit $y \in f(A \cap B)$, alors il existe $x \in A \cap B$ tel que $y = f(x)$. Mais alors, $y \in f(A)$ puisque $y = f(x)$ avec $x \in A$. De même $y \in f(B)$. On en déduit donc que $y \in f(A) \cap f(B)$. Réciproquement, si $y \in f(A) \cap f(B)$ alors il existe $a \in A$ tel que $y = f(a)$ et $b \in B$ tel que $y = f(b)$. Mais puisque f est injective, on a $a = b$, et donc $a \in A \cap B$. On en déduit que $y \in f(A \cap B)$.
- Montrons que 2. $\Rightarrow$ 1. Soient a et b tels que $f(a) = f(b) = y$. Prenons $A = \{a\}$ et $B = \{b\}$. Remarquons que $f(A) = f(B) = \{y\}$. En particulier, $A \cap B \neq \emptyset$ et donc $a = b$.

Exercice 21 (*non corrigé*) Les fonctions suivantes sont-elles injectives ? surjectives ? bijectives ?

1. $f_1 : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto 2n$
2. $f_2 : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto -n$
3. $f_3 : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$
4. $f_4 : \mathbb{R} \to \mathbb{R}^+$, $x \mapsto x^2$

Exercice 22 (*non corrigé*) Les fonctions suivantes sont-elles injectives ? surjectives ? bijectives ?

1. $f_1 : \mathbb{C} \to \mathbb{C}$, $z \mapsto z^2$
2. $f_2 : \mathbb{N} \to \mathbb{N}$, $n \mapsto n + 1$
3. $f_3 : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto n + 1$
4. $f_4 : \mathbb{R}^2 \to \mathbb{R}^2$, $(x, y) \mapsto (x + y, x - y)$

Exercice 23

1. Déterminer une bijection de $\mathbb{N} \to \mathbb{N}^\star$.
2. Déterminer une bijection de $\left\{\frac{1}{n}; n \geq 1\right\}$ dans $\left\{\frac{1}{n}; n \geq 2\right\}$.
3. Déduire de la question précédente une bijection de $[0, 1]$ dans $[0, 1[$.
4. Déterminer une bijection de $\mathbb{N} \to \mathbb{Z}$.

Correction :

1. On pose $f : \mathbb{N} \to \mathbb{N}^\star$ définie par $f(n) = n + 1$ et on remarque que f est bien à image dans $\mathbb{N}^\star$. Il reste à prouver que f est bijective : si $n \in \mathbb{N}^\star$ on a $f(k) = n \Leftrightarrow k + 1 = n \Leftrightarrow k = n - 1$, l'équation $f(k) = n$ admet une unique solution dans $\mathbb{N}$ ce qui permet d'affirmer que f est bijective.
2. On pose $g : \left\{\frac{1}{n}, n \geq 1\right\} \to \left\{\frac{1}{n}, n \geq 2\right\}$ définie par $g\left(\frac{1}{n}\right) = \frac{1}{n+1}$. On remarque que l'ensemble d'arrivée est bien cohérent avec l'ensemble de départ. On verifie aisément que g est bijective.
3. Écrivons $[0, 1] = \left\{\frac{1}{n}, n \geq 1\right\} \cup A$ où A est le complémentaire de $\left\{\frac{1}{n}, n \geq 1\right\}$ dans $[0, 1]$. On définit h de la manière suivante :

$$h(x) = \begin{cases} \frac{1}{n+1} \text{ si } x = \frac{1}{n} \\ x \text{ si } x \in A \end{cases}$$

Alors h est bijective. Prouvons tout d'abord qu'elle est injective : si $h(x) = h(x')$, on peut distinguer 3 cas :

- si $x \in A$ et $x' \in A$ alors $h(x) = x$ et $h(x') = x'$ ce qui implique $x = x'$,
- si $x \in A$ et $x' \notin A$ (ou $x \notin A$ et $x' \in A$), en écrivant $x' = \dfrac{1}{k}$ on a $x = h(x) = h(x') = \dfrac{1}{k+1}$ ce qui implique $x \notin A$, ce qui est impossible,
- si $x \notin A$ et $x' \notin A$, en écrivant $x = \dfrac{1}{k}$ et $x' = \dfrac{1}{n}$ on a $\dfrac{1}{k+1} = h(x) = h(x') = \dfrac{1}{n+1}$ ce qui entraîne $k+1 = n+1$ et par suite $x = x'$.

Dans tous les cas possibles on trouve $x = x'$ et h est injective.
Prouvons maintenant que h est surjective. Choisissons $y \in [0,1]$. Si $y \in A$, en particulier $y \neq 1$, on a $h(y) = y$. Si $y \notin A$, $y = \dfrac{1}{n}$ où n est un entier strictement plus grand que 1 puisque $y \neq 1$. On a alors $h(\dfrac{1}{n-1}) = y$. Dans tous les cas, y possède un antécédent, ce qui prouve la surjectivité de h.

4. Rappelons que tout entier peut s'écrire $2k$ s'il est pair et $2k+1$ s'il est impair. On pose $f(2k) = k$ et $f(2k+1) = -k$. Il reste alors à vérifier que f est bijective ce qui est aisé.

Exercice 24 Soient X, Y deux ensembles et $f : X \to Y$ une application.

1. Montrer que f est injective si et seulement si, pour tout $g : Z \to X$ et tout $h : Z \to X$, on a $f_o g = f_o h \Rightarrow g = h$.
2. Montrer que f est surjective si et seulement si, pour tout $g : Y \to Z$ et tout $h : Y \to Z$, on a $g_o f = h_o f \Rightarrow g = h$.

Correction :

1. Supposons que f soit injective. Soient $g : Z \to X$ et $h : Z \to X$ telles que $f_o g = f_o h$. Alors, pour tout z de Z on a $f(g(z)) = f(h(z)) \Rightarrow g(z) = h(z)$ puisque f est injective. On a donc bien $g = h$.
   Pour montrer l'implication réciproque, on procède par contraposée en supposant que f n'est pas injective. Soit $x \neq y$ tel que $f(x) = f(y)$. Posons $Z = \{0\}$, $g(0) = x$ et $h(0) = y$. Alors on a $f_o g(0) = f_o h(0)$ soit $f(x) = f(y)$ alors que $g \neq h$.
2. Supposons que f soit surjective. Soient $g : Y \to Z$ et $h : Y \to Z$ telles que $g_o f = h_o f$. Soit $y \in Y$, il existe alors $x \in X$ tel que $y = f(x)$. On en déduit que $g(y) = g_o f(x) = h_o f(x) = h(y)$ ce qui prouve $g = h$.
   Pour montrer l'implication réciproque, on procède par contraposée en supposant que f n'est pas surjective. Il existe donc un point y_0 de Y qui n'est pas dans $f(X)$. On considère alors $Z = \{0,1\}$, g définie sur Y par $g(y_0) = 1$ et $g(y) = 0$ sinon, h définie sur Y par $h(y) = 0$ pour tout y. On a bien $g_o f = h_o f$ (car $f(x) \neq y_0$ pour tout x de X) et $h \neq g$.

Exercice 25 Soit $f : E \to F$. Montrer que f est bijective si et seulement si, pour tout A de $\mathcal{P}(E)$ (l'ensemble des parties de E), on a $f(\overline{A}) = \overline{f(A)}$ (où $\overline{A}$ désigne le complémentaire de A).

Correction :

- Pour l'implication directe, on suppose que f est bijective. Prenons A un élément de $\mathcal{P}(E)$. On doit montrer une double inclusion : soit d'abord x dans $f(\overline{A})$ alors $x = f(y)$ où $y \in \overline{A}$. Supposons que $x \in f(A)$ alors $x = f(z)$ où $z \in A$. Alors, $f(x) = f(z)$ et par injectivité de f on a $y = z$. Comme $y \in A$ et $z \in \overline{A}$, cette égalité est impossible et donc $x \notin f(A)$ c'est-à-dire qu'on a prouvé que $f(\overline{A}) \subset \overline{f(A)}$. Prouvons maintenant l'autre inclusion. Soit $x \in \overline{f(A)}$. Puisque f est surjective, il existe $y \in E$ tel que $x = f(y)$. Mais $y \notin A$ car sinon $x \in f(A)$ ce qui n'est pas vrai. Donc $y \in \overline{A}$ et $x \in f(\overline{A})$.
- Étudions maintenant l'implication réciproque, c'est-à-dire qu'on suppose que pour tout A de $\mathcal{P}(E)$ on a $f(\overline{A}) = \overline{f(A)}$. Prouvons tout d'abord que ceci implique f injective. En effet, pour tous x, y tels que $f(x) = f(y)$, supposons que $x \neq y$. Posons $A = \{x\}$, on a $y \in \overline{A}$ et donc $f(y) \in f(\overline{A}) \subset \overline{f(A)}$. Or, $f(A) = \{f(x)\}$ et donc $f(y) \neq f(x)$ d'où une contradiction. Prouvons enfin que f est surjective. Par hypothèse appliquée à $A = E$, on sait que $f(\overline{E}) = \overline{f(E)}$. Mais $f(\overline{E}) = f(\emptyset) = \emptyset$ et donc $\overline{f(E)} = \emptyset$ ce qui, en prenant le complémentaire, se traduit par $f(E) = F$ c'est-à-dire que f est surjective.

Exercice 26 Soient E un ensemble, $\mathcal{P}(E)$ l'ensemble de ses parties, et A et B deux parties de E. On définit

$$\begin{array}{rcl} f : \mathcal{P}(E) & \to & \mathcal{P}(A) \times \mathcal{P}(B) \\ X & \mapsto & (X \cap A, X \cap B) \end{array} .$$

1. Montrer que f est injective si et seulement si $A \cup B = E$.
2. Montrer que f est surjective si et seulement si $A \cap B = \emptyset$.
3. Donner une condition nécessaire et suffisante sur A et B pour que f soit bijective. Donner dans ce cas la bijection réciproque.

Correction :

1. Pour démontrer le sens direct, on raisonne par contraposée : si $A \cup B \neq E$, on prend $x \in E \backslash (A \cup B)$ et $X = \{x\}$. Alors, $f(X) = (X \cap A, X \cap B) = (\emptyset, \emptyset)$ car x n'appartient ni à A ni à B. D'autre part, $f(\emptyset) = (\emptyset, \emptyset)$. Donc, $f(X) = f(\emptyset)$ alors que $X \neq \emptyset$: f n'est pas injective.
   Pour la réciproque, montrons que pour tout $X \subset E$, puisque $A \cup B = E$, on a
   $$X = X \cap E = X \cap (A \cup B) = (X \cap A) \cup (X \cap B).$$
   Ainsi, si $X, X' \subset E$ sont tels que $f(X) = f(X')$ c'est-à-dire $X \cap A = X \cap A'$ et $X \cap B = X \cap B'$ on a
   $$X = (X \cap A) \cup (X \cap B) = (X' \cap A) \cup (X' \cap B) = X'$$
   Donc f est injective.
2. Supposons d'abord que f est surjective et prenons $x \in A$ alors il existe $X \subset E$ tel que $f(X) = (\{x\}, \emptyset)$. Alors on a $X \cap B = \emptyset$ et $x \in X \cap A$. Ainsi, $x \in X$ et donc $x \notin B$ donc $A \cap B = \emptyset$.
   Réciproquement, si $A \cap B = \emptyset$, prenons $X \cap A = A'$ et $X \cap B = B'$. Donc $f(X) = (A', B')$ et f est surjective.
3. D'après les questions précédentes, on a f bijective ssi $A \cup B = E$ et $A \cap B = \emptyset$ (c'est-à-dire si (A, B) est une partition de E). La bijection réciproque a été établie à la question précédente et est donnée par $(A', B') \mapsto A' \cup B'$.

1.3.3 Relations d'équivalence

Définition 1.3.15 *Soit $(E, \mathcal{R})$ un ensemble muni d'une relation binaire.*
- *La relation $\mathcal{R}$ est dite **réflexive** si $\forall x \in E$, $x\mathcal{R}x$.*
- *La relation $\mathcal{R}$ est dite **symétrique** si $\forall (x, y) \in E \times E$, $x\mathcal{R}y \Leftrightarrow y\mathcal{R}x$.*
- *La relation $\mathcal{R}$ est dite **antisymétrique** si $\forall (x, y) \in E \times E$, $(x\mathcal{R}y$ et $y\mathcal{R}x) \Rightarrow x = y$.*
- *La relation $\mathcal{R}$ est dite **transitive** si $\forall (x, y, z) \in E \times E \times E$, $(x\mathcal{R}y$ et $y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.*

Définition 1.3.16 *On appelle **relation d'équivalence sur un ensemble** E toute relation binaire sur E réflexive, transitive et symétrique.*

Exemple 1.3.6 L'équivalence de deux fonctions au voisinage d'un point, l'égalité de deux objets sont des relations d'équivalence.

Définition 1.3.17 *On dit que deux ensembles E et F sont **équipotents** s'il existe une bijection de E sur F. Cette "relation" est réflexive, symétrique et transitive. Mais, en toute rigueur, ce n'est pas une relation d'équivalence car l'ensemble de tous les ensembles n'est pas un ensemble.*

Définition 1.3.18 *Soit $(E, \mathcal{R})$ un ensemble muni d'une relation d'équivalence. Si x est un élément de E, on appelle **classe d'équivalence** de x, et on note $cl(x)$, l'ensemble des éléments y de E tels que $x\mathcal{R}y$. On note $E/\mathcal{R}$ (E **modulo** $\mathcal{R}$) l'ensemble des classes d'équivalence des éléments de E.*

Proposition 1.3.4 *L'ensemble des classes d'équivalence forme une* ***partition*** *de l'ensemble E.*

$E/\mathcal{R}$ est également appelé **ensemble quotient**. C'est un sous-ensemble de $\mathcal{P}(E)$, ensemble des parties de E. L'ensemble quotient peut aussi être désigné comme "l'ensemble E quotienté par $\mathcal{R}$" ou "l'ensemble E considéré modulo $\mathcal{R}$". L'idée derrière ces appellations est de travailler dans l'ensemble quotient comme dans E, mais sans distinguer entre eux les éléments équivalents selon $\mathcal{R}$.

Exemple 1.3.7

- La relation de congruence modulo n, due à Karl Friedrich GAUSS (1777-1855), notée $x \equiv y$ modulo $n \Leftrightarrow x - y$ est multiple de n est une relation d'équivalence. Ses classes, ensembles des entiers donnant le même reste dans la division par n constituent n sous-ensembles de $\mathbb{Z}$ que l'on note généralement x (ou x surmonté d'un point, voire simplement x') avec $x = 0, 1, \ldots, n-1$. Ce sont les classes résiduelles modulo n (ou encore les classes de congruence). Muni de l'addition induite par $\mathbb{Z}$, cet ensemble de classes "modulo n" est appelé **groupe quotient** de $\mathbb{Z}$ par la relation de congruence et noté $\mathbb{Z}/n\mathbb{Z}$.
- L'ensemble des entiers relatifs peut être muni de la relation "a le même signe que" (comprise au sens strict). Il y a trois classes d'équivalence :
  . l'ensemble des entiers strictement positifs,
  . l'ensemble des entiers strictement négatifs,
  . le singleton $\{0\}$.
  On peut noter ces trois classes par, respectivement, $(+)$, $(-)$ et (0).
  On connaît la "règle des signes" pour le produit de deux entiers relatifs : elle montre que si on sait dans quelle classe d'équivalence se trouvent x et y, le produit xy se trouve dans une classe bien déterminée. Par exemple, si x est dans $(+)$ et y dans (0), alors xy est dans (0). Formellement, on peut le noter $(+).(0) = (0)$. De même $(+).(-) = (-)$, ou encore $(+).(+) = (+)$, $(-).(-) = (+)$ etc. Ceci est un exemple simple de loi-quotient.
  Mais avec cet exemple on ne peut pas "faire passer au quotient" la loi $+$: que dire de la somme d'un élément de $(+)$ et d'un élément de $(-)$? Pour savoir si les lois et les propriétés de structure sont compatibles avec le passage au quotient, il est utile d'introduire le concept de surjection canonique.

Proposition 1.3.5 *Il existe une surjection canonique s de E dans l'ensemble quotient, qui à chaque élément de E associe sa classe d'équivalence :*

$$\begin{array}{rcl} s : E & \to & E/\mathcal{R} \\ x & \mapsto & cl(x) \end{array}$$

s est une application puisque tout élément de E appartient à une et une seule classe d'équivalence ; s est surjective puisqu'aucune classe d'équivalence n'est vide.
s n'est pas en général injective, mais on a :

$$\forall x \in E, \forall y \in E, [s(x) = s(y)] \Leftrightarrow [\mathcal{R}(x) = \mathcal{R}(y)] \Leftrightarrow [x\mathcal{R}y]$$

Cette surjection est ainsi une bijection ssi la relation d'équivalence concernée n'est autre que la relation d'égalité.

Grâce à la surjection s, si E est muni d'une structure, il est possible de transférer cette dernière à l'ensemble quotient, sous réserve que la structure soit compatible avec la relation d'équivalence, c'est-à-dire que deux éléments de E se comportent de la même manière vis-à-vis de la structure s'ils appartiennent à la même classe d'équivalence. L'ensemble quotient est alors muni de la structure quotient de la structure initiale par la relation d'équivalence.

Définition 1.3.19 *On dit qu'une relation d'équivalence, notée $\mathcal{R}$, définie dans une structure algébrique S (voir chapitre suivant), est* ***compatible*** *avec les lois de S lorsque les résultats des opérations effectuées sur des éléments équivalents demeurent équivalents. Plus précisément :*

- *Cas d'une loi interne comme l'addition : si $x\mathcal{R}x'$ et $y\mathcal{R}y'$, alors $(x+y)\mathcal{R}(x'+y')$*
- *Cas d'une loi externe (multiplication par un scalaire) : si $x\mathcal{R}x'$ et si a est un scalaire, alors $ax\mathcal{R}ax'$*

Exercice 27 On définit sur $\mathbb{R}$ la relation $x\mathcal{R}y$ si et seulement si $x^2 - y^2 = x - y$.

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Calculer la classe d'équivalence d'un élément x de $\mathbb{R}$. Combien y-a-t-il d'éléments dans cette classe ?

Correction :

1. Il suffit de remarquer que $x\mathcal{R}y \Leftrightarrow x^2 - x = y^2 - y \Leftrightarrow f(x) = f(y)$ avec $f : x \mapsto x^2 - x$. Il est alors aisé de vérifier en appliquant la définition que $\mathcal{R}$ est une relation d'équivalence.
2. Soit $x \in \mathbb{R}$. On cherche les éléments y de $\mathbb{R}$ tels que $x\mathcal{R}y$. On doit donc résoudre l'équation $x^2 - y^2 = x - y$. Elle se factorise en $(x-y)(x+y) - (x-y) = 0 \Leftrightarrow (x-y) \times (x+y-1) = 0$. La classe de x est donc égale à $\{x, 1-x\}$. Elle est constituée de deux éléments, sauf si $x = 1 - x \Leftrightarrow x = 1/2$. Dans ce cas, elle est égale à $\{1/2\}$.

Exercice 28 (*non corrigé*) Une relation binaire $\mathcal{R}$ dans un ensemble est dite **circulaire** si pour tout $(a, b, c) \in E^3$,

$$(a\mathcal{R}b \text{ et } b\mathcal{R}c) \Rightarrow c\mathcal{R}a$$

Montrer qu'une relation circulaire et réflexive est une relation d'équivalence.

1.3.4 Relations d'ordre

Définition 1.3.20 *On appelle **relation d'ordre sur un ensemble** E toute relation binaire sur E réflexive, transitive et antisymétrique.*

Exemple 1.3.8

- La relation "inférieur ou égal à" dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ est une relation d'ordre :
  . quel que soit x : $x \leq x$ (réflexivité)
  . si $x \leq y$ et $y \leq x$, alors $x = y$ (antisymétrie)
  . si $x \leq y$ et $y \leq z$, alors $x \leq z$ (transitivité)
- Dans l'ensemble des mots français par exemple (un mot est une suite finie de lettres de l'alphabet), l'ordre alphabétique ou lexicographique est une relation d'ordre. Cette relation existe dans de nombreux langages de programmation :

  "$ABBC \leq ABC$" est vrai
  "$ABCC \leq ABB$" est faux

La structure d'**ensemble ordonné** (ensemble muni d'une relation d'ordre) a été mise en place dans le cadre de la théorie des nombres par Cantor et Richard DEDEKIND (1831-1916).

Définition 1.3.21 *Soit $\mathcal{R}$ un ordre sur E. On dit que E est ordonné par $\mathcal{R}$. Deux éléments x et y de E tels que $x\mathcal{R}y$ ou $y\mathcal{R}x$ sont dits **comparables**.*
*Il se peut, en effet que l'on ait ni $x\mathcal{R}y$, ni $y\mathcal{R}x$: on parle alors d'**ordre partiel**. Sinon, l'**ordre** est **total**.*

Comme son nom l'indique, une relation d'ordre sert à établir une hiérarchie parmi les éléments de E. Si $x \leq y$, x sera le plus souvent considéré comme plus petit que y (la convention inverse aurait pu également être prise). $x\mathcal{R}y$ doit être compris comme une phrase du type "x est plus petit que y", ou bien "x est avant y" (et éventuellement, $x = y$). Du fait de l'antisymétrie et de la transitivité, il est impossible d'avoir un cycle d'éléments distincts vérifiant $x_1\mathcal{R}x_2$, $x_2\mathcal{R}x_3$,...,$x_{n-1}\mathcal{R}x_n$, $x_n\mathcal{R}x_1$.

Remarque 1.3.3 Si on définit une relation $\leq$ dans $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$, il n'en est pas de même dans $\mathbb{C}$. Pourquoi ? Les relations définies sur les ensembles de nombres présentent une certaine compatibilité avec les lois $+$ et $\times$ définies sur ces ensembles. En particulier, on a : $a \geq 0$ et $b \geq 0 \Rightarrow a + b \geq 0$ et $ab \geq 0$. Si l'on avait, sur $\mathbb{C}$, une relation du type $i \geq 0$, alors, en effectuant le produit de i par lui-même, on obtiendrait $-1 \geq 0$. De même si $i \leq 0$. Cela ne veut pas dire qu'il est impossible de définir une relation d'ordre sur $\mathbb{C}$, mais que cette relation ne présentera aucun caractère de compatibilité avec les lois $+$ et $\times$.

Exemple 1.3.9
- Si E possède au moins deux éléments, l'ensemble P des parties de E est partiellement ordonné par la relation d'inclusion $\subset$.
- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont totalement ordonnés par la relation usuelle $\leq$.
- La relation $<$, souvent dite d'ordre strict, n'est pas une relation d'ordre car non réflexive. L'antisymétrie n'est cependant pas en défaut puisque les inégalités $a < b$ et $b < a$ ne peuvent avoir lieu conjointement.

Exercice 29 (*non corrigé*) Vérifier que, dans $\mathbb{N}$, la relation "a divise b", souvent notée $|$, définie par $a|b$ ssi $b = ka$ avec $k \in \mathbb{N}$, est un ordre partiel.

Définition 1.3.22 *Dans un ensemble totalement ordonné $(E, \leq)$, on parle d'**intervalle** $[a, b]$ pour désigner l'ensemble des éléments x de E vérifiant la "double inégalité" : $a \leq x \leq b$. On parle aussi d'**encadrement** de x.*

Définition 1.3.23 *Si $\mathcal{R}$ est un ordre sur E et F une partie de E, la restriction à F de la relation $\mathcal{R}$ est un ordre sur F, dit **ordre induit** par $\mathcal{R}$ dans F.*

Définition 1.3.24 *On munit $\mathbb{Z}$ de la relation "a divise b " définie par : $a|b \Leftrightarrow b = k \times a$ avec $k \in \mathbb{Z}$. Restreinte à $\mathbb{N}$, cette relation est une relation d'ordre (partiel). Dans $\mathbb{Z}$, elle est réflexive et transitive mais n'est pas symétrique ni antisymétrique : on parle de **relation de préordre**.*

Exercice 30 (*non corrigé*) On munit $\mathbb{N}$ de l'ordre partiel "a divise b " défini par : $a|b \Leftrightarrow b$ est multiple de a. Montrer que la restriction de cet ordre à $F = \{n \in \mathbb{N}, n = 2p, p \in \mathbb{N}\}$ est un ordre total dans F.

Exercice 31 (*non corrigé*) On considère les relations suivantes sur $\mathbb{R}$:

1. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}$, $x\mathcal{R}y \Leftrightarrow x \leq y$
2. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}$, $x\mathcal{R}y \Leftrightarrow x^2 \leq y^2$
3. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}$, $x\mathcal{R}y \Leftrightarrow |x| \leq |y|$
4. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}$, $x\mathcal{R}y \Leftrightarrow \sin x \leq \sin y$
5. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}$, $x\mathcal{R}y \Leftrightarrow y - x \in \mathbb{N}$

Pour chacune de ces relations, a t-on une relation d'ordre ? Une relation d'équivalence ?

Exercice 32 (*non corrigé*) On définit la relation $\mathcal{R}$ sur $\mathbb{N}$ par :

$$\forall m, n \in \mathbb{N}^\star,\ m\mathcal{R}n \Leftrightarrow (\exists k \in \mathbb{N}^\star, m^k = n)$$

Démontrer que $\mathcal{R}$ est une relation d'ordre.

1.3.5 Majorant, minorant, bornes supérieure et inférieure, ensemble borné

Définition 1.3.25 *Soit $(E, \prec)$ un ensemble ordonné et F une partie de E. S'il existe un élément m de E tel que $x \prec m$ pour tout x de F, on dit que m est un* ***majorant*** *de F dans E ou encore que F est* ***majorée*** *par m. Si l'on a, au contraire, $m \prec x$ pour tout x de F, on parle de* ***minorant*** *et* ***partie minorée****. F sera dit* ***borné*** *s'il admet un majorant et un minorant.*

Propriété 1.3.1 *Si, dans l'ensemble ordonné $(E, \prec)$, un majorant (respectivement minorant) d'une partie F est élément de F, il est le seul à posséder cette propriété : on l'appelle le plus grand (respectivement plus petit) élément de F pour la relation.*

Preuve : En effet, supposons par exemple l'existence de deux majorants : on aurait, dans F, $x \prec m$ et $x \prec m'$ pour tout x de F et en choisissant $x = m$ puis $x = m'$, on obtient $m = m'$ par antisymétrie.
■

On peut aussi énoncer : s'il existe un élément m de E inférieur (respectivement supérieur) à tous les éléments de E (au sens de la relation $\prec$), on dit que m est le plus petit (respectivement plus grand) élément de E. De tels éléments sont uniques.

Exemple 1.3.10

- Dans $\mathbb{N}$, muni de la relation d'ordre usuel, l'intervalle $I = [1, 100]$ admet un plus petit élément 1 et un plus grand élément 100. De même si $I =]0, 101[$.
- Dans $\mathbb{R}$, l'intervalle $[0, 1[$ est borné. Son plus petit élément est 0, il n'y a pas de plus grand élément.
- Considérons l'ensemble $\mathbb{N}$ des entiers naturels muni de l'ordre partiel "a divise b" $(a|b)$, b est un multiple de a ($b = k \times a$ avec $k \in \mathbb{Z}$). Au sens de cette relation, 1 est le plus petit élément de $\mathbb{N}$ et 0 en est le plus grand. On remarque ainsi qu'il faut toujours préciser l'ordre auquel on se réfère.
- Soit F la partie de $\mathbb{N}$ définie par $F = \{2, 3, 5, 7, 8, 10\}$ muni de l'ordre ci-dessus. Au sens de cette relation, le plus petit des majorants de F est 840 (soit le PPMC de ses éléments) et F ne contient aucun de ses majorants. Le seul minorant de F est 1.
- Si on considère $G = \{3, 9, 27, 243\}$ muni de l'ordre précédent, 243 et ses multiples sont ses majorants. 243 est le plus petit : c'est le plus grand élément de G. Les minorants de G sont 1 et 3. Ce dernier est son plus petit élément.

Définition 1.3.26 *Lorsqu'une partie F est majorée (respectivement minorée), le plus petit des majorants (respectivement le plus grand des minorants), s'il existe, est appelé* ***borne supérieure*** *(respectivement* ***borne inférieure****) de F.*

Exemple 1.3.11 L'ensemble F des valeurs de la fonction numérique $f : x \mapsto \dfrac{x^2}{x^2+1}$ est majoré par 1 et par tout nombre supérieur à 1. Le nombre 1 est le plus petit des majorants : c'est la borne supérieure de F. On note $\sup(F) = 1$. On remarque que 1 n'est pas élément de F. On a $f(x) \geq 0$ et $f(0) = 0$: 0 est la borne inférieure de F (le plus grand des minorants) et puisque 0 est élément de F, on dit que 0 est le plus petit élément de F : on note $\inf(F) = 0$.

Proposition 1.3.6 *Un ensemble peut être borné sans pour autant admettre une borne supérieure ou une borne inférieure.*

Exemple 1.3.12 Dans l'ensemble $\mathbb{Q}$ des nombres rationnels (fractions $\frac{a}{b}$, a et b entiers, b non nul) muni de l'ordre usuel, la partie $F = \{x \in \mathbb{Q}, x \geq 0, x^2 \leq 2\}$ manifestement majorée (par 3/2, 2,...) n'admet pas de borne supérieure. En effet, supposons l'existence d'une borne supérieure m pour F. m est rationnel, il est le plus petit des majorants de F. On peut donc écrire :

1. $\forall x \in F$, $x \leq m$ et
2. $\forall M$ majorant de F, $m \leq M$

2. permet d'affirmer que $\forall \epsilon \in \mathbb{Q}$, $\epsilon > 0$, $\exists x_0 \in F / m - \epsilon < x_0 \leq m$. Il s'ensuit que pour tout rationnel ϵ vérifiant $0 < \epsilon \leq m$, on a $(m-\epsilon)^2 < 2$ et, par conséquent $\epsilon^2 - 2m\epsilon + m^2 - 2 < 0$ pour tout ϵ de l'intervalle rationnel $]0, m]$. Si nous résolvons cette équation dans $\mathbb{R}$, on voit qu'elle n'admet des solutions que si $m \leq \sqrt{2}$. Or on sait que $\sqrt{2}$ n'est pas rationnel, ainsi m est un rationnel vérifiant $m < \sqrt{2}$. En tant que partie de $\mathbb{R}$, les majorants M de F vérifient l'inégalité $M \geq \sqrt{2}$ et les majorants de F dans $\mathbb{Q}$ sont alors les rationnels vérifiant $M > \sqrt{2}$ et en particulier $m > \sqrt{2}$. Les inégalités $m < \sqrt{2}$ et $m > \sqrt{2}$ étant incompatibles, F n'admet pas de borne supérieure.

Définition 1.3.27 *Soit $(E, \prec)$ un ensemble ordonné. S'il existe dans E un élément m tel que tout x de E, comparable à m (et autre que m), lui soit inférieur (respectivement supérieur) au sens de la relation $\prec$, on dit que m est un* ***élément maximal*** *(respectivement* ***minimal****).*

Lorsque l'ordre de E n'est pas total, il peut exister plusieurs éléments maximaux ou minimaux.

Exemple 1.3.13 On munit l'intervalle $I = [1, 100]$ de $\mathbb{N}$ (nombres entiers de 1 à 100) de l'ordre partiel "a divise b" : $a|b$ ssi a est un diviseur de b (a inférieur à b), ssi b est multiple de a (b supérieur à a). Tout $n \geq 51$ est maximal et 1 est le seul élément minimal. C'est le plus petit élément. Si $I = [0, 100]$ alors 0, étant multiple de tout nombre, est le plus grand élément au sens de la relation "divise" et devient l'unique élément maximal.

Proposition 1.3.7 *Si $(E, \prec)$ admet un plus petit (respectivement grand) élément m, alors m est l'unique élément minimal (respectivement maximal) de E.*

1.3.6 Ordre produit et ordre réciproque

Définition 1.3.28 *Si $\mathcal{R}$ est un ordre sur E, la relation $\mathcal{R}'$ (souvent notée $\mathcal{R}^{-1}$) définie par :*

$$x\mathcal{R}'y \Leftrightarrow y\mathcal{R}x$$

est un ordre sur E, dit ***ordre réciproque*** *de $\mathcal{R}$.*

Exemple 1.3.14
- L'ordre réciproque de l'ordre usuel $\leq$ est l'ordre noté $\geq$.
- L'ordre réciproque de l'ordre "x divise y" dans $\mathbb{N}$ est l'ordre "x est multiple de y".

Remarque 1.3.4 On ne confondra pas l'ordre réciproque de $\mathcal{R}$ et la négation $\neg\mathcal{R}$ d'un ordre $\mathcal{R}$, laquelle serait définie par $x\neg\mathcal{R}y$ ssi non $(y\mathcal{R}x)$. La négation de la relation d'ordre usuel (inférieur ou égal) est la relation $>$ (supérieur et différent). C'est un ordre "strict".

Définition 1.3.29 *Si (E, O) et (F, O') sont deux ensembles ordonnés par les relations notées O et O', on peut ordonner le produit cartésien $E \times F$ par l'ordre T dit* ***ordre produit*** *de O et O' :*

$$(a, b)T(c, d) \Leftrightarrow (aOc \text{ et } bO'd)$$

Exemple 1.3.15 Si on applique cet ordre à $\mathbb{R}^2$ lorsque $\mathbb{R}$ est muni de l'ordre total usuel, $O = O' =$ " $\leq$", on obtient un ordre partiel. Par exemple, les couples $(1, 2)$ et $(2, -3)$ ne sont pas comparables.

1.3.7 Cardinal d'un ensemble

Définition 1.3.30 *Soient E et F deux ensembles.*
- *On dit que E et F ont même cardinal, et on note $Card(E) = Card(F)$, s'il existe une bijection de E sur F et on parle dans ce cas d'ensembles* ***équipotents****. Sinon on note $Card(E) \neq Card(F)$.*
- *On dit que le cardinal de E est inférieur ou égal au cardinal de F, et on note $Card(E) \leq Card(F)$, s'il existe une injection de E dans F. Si de plus $Card(E) \neq Card(F)$, on note $Card(E) < Card(F)$.*

– *On dit que le cardinal de E est supérieur ou égal au cardinal de F, et on note $Card(E) \geq Card(F)$, s'il existe une surjection de E dans F. Si de plus $Card(E) \neq Card(F)$, on note $Card(E) > Card(F)$.*

Remarque 1.3.5 On utilise parfois les notations $|E|$ et $\#E$ pour exprimer $Card(E)$.

Théorème 1.3.1 *(Cantor-Bernstein) Soient E et F deux ensembles.*

$$\boxed{Card(E) = Card(F) \Leftrightarrow (Card(E) \leq Card(F) \text{ et } Card(F) \leq Card(E))}$$

Remarque 1.3.6 Ces relations se comportent comme une relation d'ordre, mais cette "relation" n'est à priori pas définie sur un ensemble. Les résultats suivants vont nous en convaincre.

Théorème 1.3.2 *(Cantor) Soit E un ensemble non vide alors*

$$\boxed{card(E) < card(\mathcal{P}(E))}$$

Corollaire 1.3.2 *Il n'existe pas d'ensemble contenant tous les ensembles.*

Définition 1.3.31 *Soit E un ensemble. On dit que E est **fini** s'il n'est en bijection avec aucune de ses parties propres. Dans le cas contraire, on dit que E est **infini**.*
*Si E est un ensemble infini, on dit que E est **dénombrable** s'il existe une bijection de E sur l'ensemble $\mathbb{N}$ des entiers naturels. Dans le cas contraire, on dit que E est **indénombrable**.*

Remarque 1.3.7 Un ensemble fini est un ensemble dont le cardinal est un entier naturel. On retrouve là les cardinaux connus. Toutefois, cette notion n'est pas intuitive, en fait, elle a été utilisée par Cantor pour définir rigoureusement les nombres entiers naturels.

Proposition 1.3.8 *Tout ensemble infini contient un sous-ensemble dénombrable.*

Caractérisation : Un ensemble infini E est dénombrable si et seulement si E est l'ensemble-image d'une suite.

Si A et B sont des ensembles finis et si on désigne par $Card(A)$ le nombre d'éléments de A et par $Card(B)$ le nombre d'éléments de B, on aura

$$\boxed{Card(A \times B) = Card(A) \times Card(B)}$$

En effet le nombre de couples du type (a, b) avec $a \in A$ et $b \in B$ est obtenu en faisant correspondre à tout élément de $a \in A$ tous les éléments de B soit $Card(B)$ éléments. Ceci devra être répété autant de fois qu'il y a d'éléments dans A.

On vérifiera aisément que

$$\boxed{Card(A \cup B) = Card(A) + Card(B) - Card(A \cap B)}$$

$$\boxed{Card(A^n) = (Card(A))^n \text{ pour } n \in \mathbb{N}^\star}$$

$$\boxed{Card(\mathcal{P}(E)) = 2^{Card(E)}}$$

Exercice 33 (*non corrigé*) Dénombrer les parties d'un ensemble contenant n éléments.

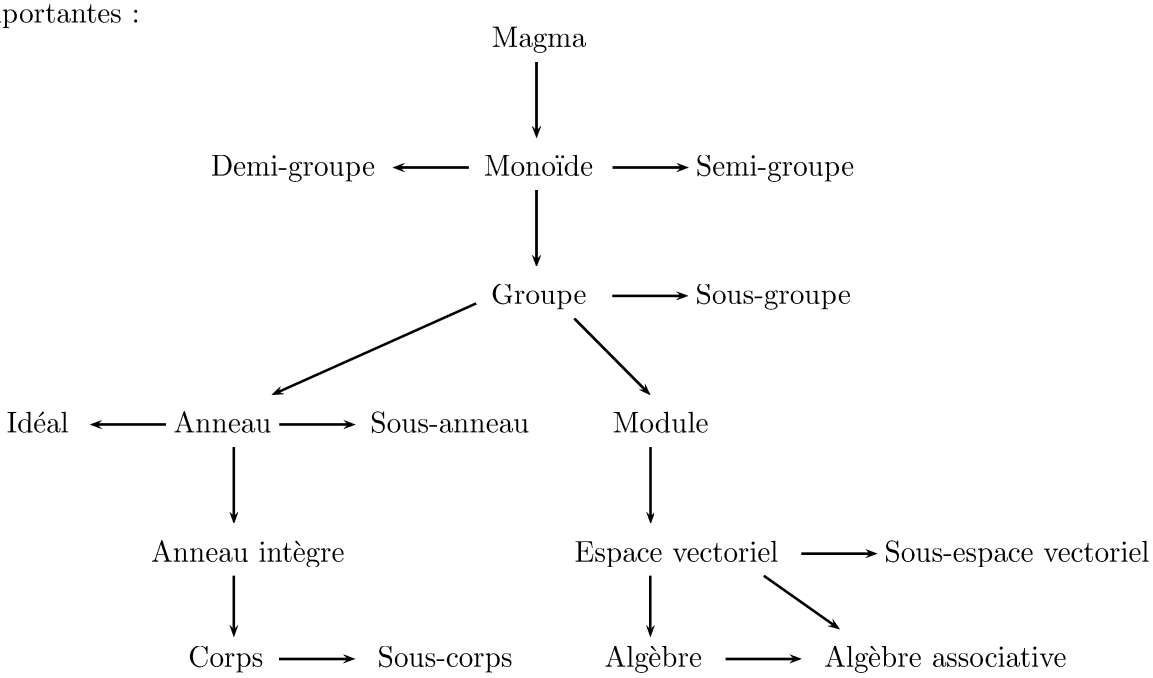
Exercice 34 (*non corrigé*) Soit l'ensemble E possédant n éléments. Quel est le nombre d'éléments de E^p ? Quel est le nombre de parties de E^p ?

Chapitre 2

Les structures algébriques

2.1 Introduction

Dans la théorie des ensembles, l'objet principal est un ensemble qui se dissimule parfois sous d'autres noms tels que classe, collection ou famille. Cependant, dans d'autres disciplines des mathématiques, un ensemble est toujours muni d'une structure. En algèbre tout particulièrement, un ensemble est combiné avec une ou plusieurs lois de composition et s'appelle une structure algébrique. Voici une liste des structures algébriques importantes :



Tout en haut du diagramme, on trouve les structures algébriques impliquant un nombre minimal de contraintes et en bas, celles qui en impliquent un maximum. Plus on descend, plus la structure est en quelque sorte spécialisée.
Les structures les plus communes sont les groupes, les anneaux et les corps.

2.2 Magmas et monoïdes

2.2.1 Les magmas

Introduisons dans un premier temps une structure algébrique élémentaire : le magma.

Définition 2.2.1 *Un ensemble E muni d'une loi de composition interne T est appelé* ***magma*** *et est noté (E,T).*

Un magma est donc une structure algébrique élémentaire. Il existe des structures plus subtiles dans lesquelles un ensemble est muni de plusieurs lois et de différentes propriétés.

Définition 2.2.2 *Soit A une partie non vide d'un magma (E,T). On dira que A est* ***stable*** *pour la loi T ou que A est une* ***partie stable*** *de E (lorsqu'il n'y a pas d'ambigüité sur la loi en cause) si la restriction à A de la loi T est une loi de composition interne dans A. Autrement dit :*

$$A \subset E,\ A \text{ stable pour la loi } T \Leftrightarrow \forall (a,b) \in A \times A,\ aTb \in A$$

On peut donc remarquer que dire qu'une loi T est une loi de composition interne dans un ensemble E équivaut à dire que E est stable pour cette loi. En revanche, si A est un sous-ensemble de E, il n'est pas certain que A soit stable pour la loi T. Ainsi $\mathbb{N}$ n'est pas stable pour la soustraction, mais $\mathbb{Z}$ l'est. De même, $\mathbb{Z}^\star$ n'est pas stable pour l'inverse, mais $\mathbb{Q}^\star$ l'est.

Définition 2.2.3 *Si, pour tout couple (x,y) d'éléments de E, on a $xTy = yTx$, la loi T est dite* ***commutative****. (E,T) est dit* ***commutatif****.*

Remarque 2.2.1

- Les magmas $(\mathbb{N},+)$, $(\mathbb{Z},+)$, $(\mathbb{Z},\times)$ sont commutatifs. Ce n'est pas le cas de $(\mathbb{Z},-)$: $3-2=1$ alors que $2-3=-1$. De même, $(\mathbb{Q}-\{0\},/)$, ensemble des nombres rationnels non nuls muni de la division usuelle n'est pas commutatif : $3/2 \neq 2/3$.
- Lorsqu'une loi n'est pas commutative, certains éléments peuvent cependant "commuter" : on parle d'éléments **permutables**. Il suffit pour s'en convaincre de considérer la loi "o" de composition des applications et les fonctions $f : x \mapsto 3x+2$ et $g : x \mapsto 2x+1$.
- Dans un magma associatif (E,T), un élément x permutable avec deux éléments a et b est permutable avec le composé aTb.
  Si la loi T n'est pas associative, le résultat peut ne plus être vrai : dans $(\mathbb{Z},T)$ avec $aTb = a^2 - 2b$, 3 et -5 commutent donc 3 commute avec 3 et -5 mais 3 ne commute pas avec $19 = 3T(-5)$; en effet $3T19 = -29$ et $19T3 = 355$.

Définition 2.2.4 *Un élément e de E vérifiant $xTe = eTx = x$ est dit* ***neutre*** *pour la loi T. Le magma (E,T) muni de cet élément neutre est dit* ***unifère*** *(ou parfois* ***unitaire****).*

Exemple 2.2.1

- Dans les magmas $(\mathbb{N},+)$ et $(\mathbb{Z},+)$, "0" est neutre, c'est-à-dire que pour tout entier naturel ou tout entier relatif n, $n+0=0+n=n$.
- Dans $(\mathbb{Z},-)$, 0 n'est neutre qu'à droite : $x-0=x$ mais $0-x=-x$.
- Dans $\mathbb{N}$ et $\mathbb{Z}$, "1 " est neutre pour la multiplication.
- Dans $\mathcal{M}_2(\mathbb{R})$, ensemble des matrices carrées d'ordre 2 à termes réels, la matrice $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est neutre pour la multiplication.

Remarque 2.2.2 Un magma peut admettre plusieurs éléments neutres d'un "même" côté (à droite : $aTe = a$, ou à gauche : $eTa = a$). Par exemple, dans $(\mathbb{Z},T)$ où T désigne la loi définie par $aTb = a + E(b/3)$ les entiers 0, 1 et 2 sont neutres à droite et il n'y a pas d'élément neutre à gauche.

Proposition 2.2.1 *Un élément neutre à gauche et à droite est unique : c'est l'élément neutre du magma (E,T).*

Preuve : Supposons que (E,T) admette deux éléments neutres distincts e_1 et e_2 à gauche et à droite respectivement. On a d'une part $\forall x \in E$, $e_1 T x = x$, cette relation est donc vraie pour $x = e_2$ ce qui nous permet d'affirmer que $e_1 T e_2 = e_2$. D'autre part $\forall x \in E$, $x T e_2 = x$, cette relation étant vraie pour $x = e_1$, on a $e_1 T e_2 = e_1$. Par conséquent, $e_1 = e_2$ ■

Définition 2.2.5 *Si un élément b de E vérifie $aTb = bTa = b$, $\forall a \in E$, alors b est dit* ***élément absorbant*** *pour la loi T.*

2.2.2 Les monoïdes

Définition 2.2.6 *Si, pour tout triplet (x,y,z) d'éléments de E, on a $(xTy)Tz = xT(yTz)$, la loi T est dite* ***associative****. Le magma (E,T) est dit* ***associatif****.*

Un monoïde est un magma associatif et unifère

Remarque 2.2.3
- Si la loi interne est en plus commutative, nous disons alors que la structure forme un **monoïde commutatif**.
- Un **demi-groupe** est un magma associatif. Le monoïde est donc un demi-groupe muni d'un élément neutre.

Exercice 35 Montrer que l'ensemble des entiers naturels est un monoïde commutatif totalement ordonné par rapport aux lois d'addition et de multiplication.
Correction :

1. La loi d'addition + est-elle une opération interne telle que $\forall a, b \in \mathbb{N}$ nous ayons $a + b = c \in \mathbb{N}$? Nous pouvons démontrer que c'est bien le cas en sachant que 1 appartient à $\mathbb{N}$ tel que $\sum_{i=1}^{a} 1 + \sum_{i=1}^{b} 1 = \sum_{i=1}^{a+b} 1$.
   Donc $c \in \mathbb{N}$ et l'addition est bien une loi interne (l'ensemble est stable par rapport à l'addition) et en même temps associative puisque 1 peut être additionné à lui-même par définition dans n'importe quel ordre sans que le résultat en soit altéré.
   La multiplication est une loi qui se construit sur l'addition donc la loi de multiplication $\times$ est aussi une loi interne et associative.
2. On admettra à partir d'ici qu'il est trivial que la loi d'addition est également commutative et que le "0" en est l'élément neutre e.
   La loi de multiplication est aussi commutative et il est trivial que "1" en est l'élément neutre e.
3. Pour conclure, on rappelle les résultats suivants :
   - $(\mathbb{N}, \leq, \geq)$ est totalement ordonné (attention cette notation est un peu abusive, il suffit qu'il y ait juste une des deux relations d'ordre $\mathcal{R}$ pour que l'ensemble soit totalement ordonné).
   - $(\mathbb{N}, +)$ et $(\mathbb{N}, \times)$ sont des monoïdes abéliens.

Conclusion, $\mathbb{N}$ est un monoïde abélien totalement ordonné par rapport aux lois d'addition et de multiplication.

Remarque 2.2.4 Il est rare d'utiliser les monoïdes car souvent, lorsque nous nous trouvons face à une structure trop pauvre pour pouvoir vraiment discuter, nous la prolongeons vers quelque chose de plus riche, comme un groupe, ou un anneau (voir plus loin).

Exemple 2.2.2

- Le magma $(\mathbb{Z}, +)$ est associatif et unifère (l'élément neutre étant dans ce cas 0) donc $(\mathbb{Z}, +)$ est un monoïde.
- Ce n'est pas le cas de $(\mathbb{Z}, -)$. En effet, $(\mathbb{Z}, -)$ est un magma non unifère et non associatif car, par exemple, $(3-2)-5 = -4$ alors que $3-(2-5) = 6$. Ce n'est pas le cas non plus de $(\mathbb{Q} - \{0\}, /)$, il suffit de considérer pour s'en convaincre l'exemple suivant : $(3/2)/5 = 3/10$ alors que $3/(2/5) = 15/2$.
- La loi de composition des applications est associative.
- Le produit vectoriel $\wedge$ (à ne pas confondre avec le "et " logique) n'est pas associatif : par exemple, si (i, j, k) est une base orthogonale $(i \wedge i) \wedge j = 0 \wedge k = 0$ alors que $i \wedge (i \wedge j) = i \wedge k = -j$.

Définition 2.2.7 *Dans un magma unifère (E, T) d'élément neutre e, un élément x est dit* ***symétrisable***
- *à droite : s'il existe x' dans E tel que $xTx' = e$,*
- *à gauche : s'il existe $x"$ dans E tel que $x"Tx = e$.*

Lorsque l'élément est symétrisable à gauche et à droite (bilatère) et si $x' = x"$, on a alors :

$$x'Tx = xTx' = e$$

Dans ce cas, x et x' sont dits ***symétriques*** *pour la loi T de E. On dit aussi que x' (respectivement x) est un symétrique de x (respectivement x'). Lorsque la loi T s'interprète comme une multiplication, on parle plutôt d'éléments* ***inversibles*** *et d'****inverses****.*

Remarque 2.2.5
- Dans $(\mathbb{Z}, -)$, 0 est neutre à droite et tout entier relatif est son propre et unique symétrique à droite.
- Dans $(\mathbb{Z}, +)$, tout entier relatif x possède un unique symétrique : son **opposé** $-x$.

Exercice 36 Montrer que les lois d'addition et de multiplication de l'ensemble des entiers naturels n'admettent pas de symétrique.

Correction : Existe-t-il pour la loi d'addition $+$ un symétrique $c \in \mathbb{N}$ tel que $\forall a \in \mathbb{N}$ nous ayons $a + c = \left(\sum_{i=1}^{a} 1\right) + c = e = 0$? Il est assez trivial que pour que cette égalité soit satisfaite on ait $\left(\sum_{i=1}^{a} 1\right) = -c \Leftrightarrow a = -c$ or les nombres négatifs n'existent pas dans $\mathbb{N}$. Ce qui nous amène aussi à la conclusion que la loi d'addition $+$ n'a pas de symétrique et que la loi de soustraction $-$ n'existe pas dans $\mathbb{N}$ (la soustraction étant rigoureusement l'addition d'un nombre négatif).
Existe t-il pour la loi de multiplication $\times$ un symétrique $a' \in \mathbb{N}$ tel que $\forall a \in \mathbb{N}$, on ait $a' \times a = e = 1$? D'abord il est évident que $a' = \dfrac{1}{a}$. Mais excepté pour $a = 1$, le quotient $1/a$ n'existe pas dans $\mathbb{N}$. Donc nous devons conclure qu'il n'existe pas pour tout élément de $\mathbb{N}$ de symétriques pour la loi de multiplication et ainsi que la loi de division n'existe pas dans $\mathbb{N}$.

Définition 2.2.8 *Dans un magma (E, T), un élément x est dit* ***régulier*** *(ou* ***simplifiable****)* ***à gauche*** *si pour tout couple (a, b) d'éléments de E tels que $xTa = xTb$, alors $a = b$. On définit de même un élément* ***régulier à droite****. Un élément est dit* ***régulier*** *s'il est régulier à droite et à gauche. Si T est commutative, les notions d'élément régulier à gauche et à droite coïncident.*

Exemple 2.2.3
- Dans $(\mathbb{N}, +)$, tout élément est régulier et dans $(\mathbb{N}, \times)$, tout élément non nul est régulier.
- Dans $(\mathbb{Z}, T)$, avec $aTb = |a| + b$, tout élément est régulier à gauche mais pas à droite.

Remarque 2.2.6
- Dans un magma associatif, le composé de deux éléments réguliers est régulier.
- Dans un magma associatif, tout élément symétrisable est régulier.
- Si le magma n'est pas associatif, rien n'est assuré.

Exercice 37 (*non corrigé*) On considère E l'ensemble des entiers naturels au plus égaux à 10 et la loi T définie dans E par $aTb = |a - b|$ (différence symétrique).
- Montrer que 0 est neutre et que tout élément est son propre symétrique.
- Montrer que seuls 0 et 10 sont réguliers.
- Montrer que T est non associative en considérant $(1T2)T3$ et $1T(2T3)$

Exercice 38 (*non corrigé*) On considère dans $\mathbb{Z}$ la loi T définie par $aTb = ab + 3$. Montrer que T n'est pas associative, que -1 et 3 sont réguliers mais que $-1T3 = 0$.

2.3 Les groupes

2.3.1 Les groupes

Le terme est de Évariste GALOIS (1811-1832), la structure est de Augustin Louis CAUCHY (1789-1857), l'axiomatisation de Arthur CAYLEY (1821-1895).

Définition 2.3.1 *Un groupe G est un ensemble muni d'une loi de composition interne T pour laquelle les axiomes suivants sont vérifiés :*
- $\boxed{g_1}$ *la loi T est associative : $(xTy)Tz = xT(yTz)$ pour tout x, y et z de G,*
- $\boxed{g_2}$ *la loi T possède un élément neutre e : $xTe = eTx = x$ pour tout x de G,*
- $\boxed{g_3}$ *tout élément x de G possède un symétrique x' pour la loi T : $xTx' = x'Tx = e$.*

Le groupe G muni de sa loi T est souvent noté (G, T).

Un groupe est un magma unifère associatif dans lequel tout élément admet un symétrique

Un groupe est un monoïde dans lequel tout élément admet un symétrique

Exercice 39 Soit G un ensemble muni d'une loi de composition interne "T" associative, qui possède un élément neutre à droite e (i.e. pour tout x de G, $xTe = x$) et tel que tout élément x possède un symétrique à droite x' (i.e. $xTx' = e$). Montrer que G est un groupe.
Correction : Soit $x \in G$, de symétrique à droite x'. Par conséquent $x'Tx$ est un élément de G (lci), il possède donc un symétrique à droite que l'on note z. On a donc $xT((x'Tx)Tz) = x \Rightarrow (xTx')TxTz = x \Rightarrow eTxTz = xTz = x$, par associativité de la loi. On compose ensuite à gauche par x', pour trouver $x'T(xTz) = (x'Tx)Tz = e = x'Tx$, ce qui permet d'affirmer que x' est également un symétrique à gauche de x. On en déduit ensuite que e est aussi neutre à gauche, car si x est dans G, $eTx = (xTx')Tx = xT(x'Tx) = xTe = x$ (on a utilisé à nouveau l'associativité de la loi et le fait que e est un symétrique à droite).

Exercice 40
1. $(\mathbb{N}, +)$ et $(\mathbb{N}, \times)$ sont-ils des groupes ?
2. $(\mathbb{Z}, +)$ et $(\mathbb{Z}, \times)$ sont-ils des groupes ?
3. $(\mathbb{R}, +)$ et $(\mathbb{R}, \times)$ sont-ils des groupes ?

Correction : On vérifie pour chacun des couples les propriétés du groupe $\boxed{g_1}$, $\boxed{g_2}$ et $\boxed{g_3}$.

2.a. Pour $(\mathbb{Z}, +)$:
- $\forall (x, y) \in \mathbb{Z}^2$, $x + y \in \mathbb{Z}$, la loi est donc interne (*magma*),
- $\forall x \in \mathbb{Z}$, $x + 0 = 0 + x = x$. "0" est l'élément neutre (*unifère*),
- $\forall (x, y, z) \in \mathbb{Z}^3$, $(x + y) + z = x + (y + z)$, la loi $+$ est associative dans $\mathbb{Z}$ (*associatif*),

– $\forall x \in \mathbb{Z}$, $\exists x' = -x$, $x + x' = 0$, *tous les éléments ont un symétrique.*
$(\mathbb{Z}, +)$ est donc un groupe.

3.a. On démontre de même que $(\mathbb{R}, +)$ est un groupe.

Par contre :

1.a. les éléments de $\mathbb{N}$ n'ont pas d'opposé (sauf 0),

1.b. les éléments de $\mathbb{N}$ n'ont pas d'inverse (sauf 1),

2.b. les éléments de $\mathbb{Z}$ n'ont pas d'inverse (sauf 1 et -1),

3.b. 0 n'a pas d'inverse,

donc $(\mathbb{N}, +)$, $(\mathbb{N}, \times)$, $(\mathbb{Z}, \times)$ et $(\mathbb{R}, \times)$ n'ont pas de structure de groupe, ce sont néanmoins des monoïdes.

Définition 2.3.2 *Un groupe dont la loi de composition possède des caractéristiques semblables à celle de l'addition (respectivement la multiplication) dans $\mathbb{Z}$ (respectivement dans $\mathbb{R}^\star$) est dit* ***additif*** *(respectivement* ***multiplicatif****).*

Définition 2.3.3 *Un groupe G est dit* ***abélien*** *(du nom de Niels Henrick ABEL, 1802-1829) ou* ***commutatif*** *si sa loi de composition interne T est commutative c'est-à-dire si $xTy = yTx$, $\forall x, y \in G$.*

Exemple 2.3.1

- L'addition dans $\mathbb{Z}$ et dans $\mathbb{R}$ est commutative. Ce n'est pas le cas de la soustraction : $2 - 5 \neq 5 - 2$. Dans $(\mathbb{Z}, -)$, 0 n'est neutre qu'à droite.
- $(\mathbb{Z}, +)$ est un groupe abélien, de même $(\mathbb{R} - \{0\}, \times)$. Par contre, $(\mathbb{R} - \{0\}, /)$ ne l'est pas car la division n'est pas associative ($(2/3)/4 = 1/6$ et $2/(3/4) = 8/3$) ni commutative ($5/4 = 1,25$ et $4/5 = 0,8$).
- $(\mathbb{Z}, -)$ n'est pas un groupe : la soustraction est une loi de composition interne dans $\mathbb{Z}$, mais elle n'est pas associative : $(2 - 3) - 5 \neq 2 - (3 - 5)$. C'est cependant un magma.
- Si $\mathcal{A}(\mathbb{R})$ désigne l'ensemble des fonctions affines bijectives de $\mathbb{R}$ sur $\mathbb{R}$ soit l'ensemble des fonctions de la forme $x \mapsto ax + b$ avec a non nul, $(\mathcal{A}(\mathbb{R}), \mathrm{o})$ est un groupe non abélien (o : loi de composition des applications). Si f désigne $x \mapsto 2x - 1$ et si g désigne $x \mapsto 3x$, on a $f_o g : x \mapsto 6x - 1$ et $g_o f : x \mapsto 6x - 3$.
- Si $\mathcal{M}_2(\mathbb{R})$ désigne l'ensemble des matrices carrées réelles d'ordre 2 de déterminant non nul, $(\mathcal{M}_2(\mathbb{R}), \times)$ est un groupe multiplicatif non abélien.
- L'ensemble constitué des homothéties de rapport non nul et des translations dans un plan P, muni de la loi de composition des applications, est un groupe non commutatif. Son élément neutre est l'application identique assimilé à la translation de vecteur nul ou à l'homothétie de rapport 1.
- Dans un plan P, considérons un carré $ABCD$ de centre O. Notons S_0 la symétrie centrale par rapport à O, S_1 la symétrie d'axe d_1 passant par les milieux des côtés $[AD]$ et $[BC]$, S_2 la symétrie d'axe d_2 passant par les milieux des côtés $[AB]$ et $[CD]$ et i l'application identique de P. Muni de la loi de composition des applications, l'ensemble $E = \{i, S_0, S_1, S_2\}$ est un groupe commutatif.

Exercice 41 Décrire tous les groupes possibles à 1, 2, 3 ou 4 éléments.

Correction :

1. Un groupe à un élément est un ensemble E constitué d'un seul élément e, et la loi $\star$ est nécessairement définie par $e \star e = e$. On vérifie sans difficulté que $(E, \star)$ est bien un groupe.
2. Si E contient deux éléments, l'un doit être le neutre pour $\star$, notons le e et notons l'autre x. On a donc $e \star e = e$ et $e \star x = x \star e = x$. Si l'on veut de plus que x soit inversible, on doit nécessairement avoir $x \star x = e$, et on vérifie que $(E, \star)$ est alors un groupe.
3. Ajoutons un troisième élément y à notre ensemble, on a nécessairement $e \star e = e$, $e \star x = x \star e = x$ et $e \star y = y \star e = y$. On ne peut avoir $x \star y = y$ $(x \neq e)$ ni $x \star y = x$ $(y \neq e)$ donc $x \star y = e$ (lci). On montre de la même manière que $y \star x = e$. On ne peut pas avoir $x \star x = x$ $(x \neq e)$ ni $x \star x = e$ (car l'inverse de x est unique dans un groupe et on sait qu'il vaut y). Par conséquent, $x \star x = y$ (lci) et on montre de la même manière que $y \star y = x$. On a donc les résultats suivants :

$\star$	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Cette loi est bien une loi de groupe.

4. Enfin, dans le cas de quatre éléments, on obtient en étudiant toutes les possibilités les quatre lois suivantes :

$\star$	e	x	y	z
e	e	x	y	z
x	x	y	z	e
y	y	z	e	x
z	z	e	x	y

$\star$	e	x	y	z
e	e	x	y	z
x	x	z	e	y
y	y	e	z	x
z	z	y	x	e

$\star$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

$\star$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	x	e
z	z	y	e	x

Théorème 2.3.1 *Tout élément d'un groupe (G,T) est régulier.*

Preuve : Vu que T est associative et que tout élément x admet un symétrique x', si e est l'élément neutre pour la loi T, $\forall (a,b) \in G^2$, $xTa = xTb \Rightarrow x'T(xTa) = x'T(xTb) \Rightarrow (x'Tx)Ta = (x'Tx)Tb \Rightarrow eTa = eTb \Rightarrow a = b$. (G,T) est régulier à gauche et on montre de la même façon que ce groupe est régulier à droite. ■

Théorème 2.3.2 *Dans un groupe (G,T), tout élément admet toujours un unique élément symétrique.*

Preuve : L'existence du symétrique est justifiée par la définition, il reste à prouver l'unicité. Supposons que $\forall x \in E,\ \exists x', x'' \in E,\ x' \neq x'',\ x'Tx = x''Tx (= e) \Leftrightarrow x' = x''$ pusique $x \in G$ est régulier (à droite). ■

Exercice 42 (*non corrigé*) Démontrer que si $(E,\star)$ est un groupe d'élément neutre e, dans lequel tout élément est **involutif** (c'est-à-dire $x \star x = e$), alors ce groupe est commutatif.
Généralement, l'unique élément symétrique de x est noté x^{-1}. On a

Propriété 2.3.1

- $e^{-1} = e$. *L'élément neutre est son propre symétrique, il est involutif.*
- $(x^{-1})^{-1} = x$.
- $(xTx')^{-1} = x'^{-1}Tx^{-1}$. *Le symétrique d'un produit est le produit inverse des symétriques.*
- *Plus généralement* $(x_1Tx_2T\dots Tx_n)^{-1} = x_n^{-1}Tx_{n-1}^{-1}T\dots Tx_1^{-1}$.

En particulier on a $(x^n)^{-1} = (x^{-1})^n$, $(n \in \mathbb{N}^\star)$. On note alors $x^{-n} := (x^n)^{-1}$ ce qui permet de définir x^m pour $m \in \mathbb{Z}$ en convenant $x^0 = e$. Dans ces conditions on a les relations.

$$(x^m)^{m'} = x^{mm'} \text{ et } x^mTx^{m'} = x^{m+m'},\ \forall m, m' \in \mathbb{Z}.$$

2.3.2 Les sous-groupes

Définition 2.3.4 *Un **sous-groupe** est une partie S d'un groupe (G,T) qui, munie de la loi T de G, est aussi un groupe.*

Proposition 2.3.1 *Un sous-ensemble H de (G,T) est un sous-groupe si et seulement si il contient e (élément neutre de (G,T)) et est stable par produit et passage à l'inverse.*

Preuve : Si un sous-ensemble de G vérifie ces trois propriétés, c'est bien un sous-groupe.
Réciproquement, si H est un sous-groupe, il possède un élément neutre e_0. Soit alors x un élément de H, on a $xTe_0 = x = xTe$ (la première loi est prise dans H, la deuxième dans G), donc $e_0 = e$ par simplification. De même, l'inverse de x dans H est nécessairement un inverse dans G également, donc il s'agit de l'unique inverse de x par T, et H est stable par inversion. Enfin, H doit clairement être stable par produit. ■

Proposition 2.3.2 *Une partie H non vide de G, contenant e, est un sous-groupe de (G,T) si et seulement si*

1. $\forall x, y \in H, xTy \in H$
2. $\forall x \in H, x^{-1} \in H$

Les deux conditions précédentes peuvent être remplacées par la suivante :

$$\forall x, y \in H, xTy^{-1} \in H$$

Remarque 2.3.1 La notation $H < G$ est employée pour dire H est sous-groupe de G. Lorsqu'on n'exclut pas la possibilité que H soit égal à G on écrit $H \leq G$.

Exercice 43 (*non corrigé*) Montrer que
- dans le groupe multiplicatif $(\mathbb{C}, \times)$ des nombres complexes, l'ensemble des nombres de module 1 est un sous-groupe de $\mathbb{C}$,
- dans le groupe additif $(F, +)$ des fonctions numériques, l'ensemble des fonctions linéaires $x \mapsto ax$ est un sous-groupe de F.

Exercice 44 Soit $n \in \mathbb{N}$. On note $n\mathbb{Z}$ l'ensemble des entiers relatifs de la forme nx, $x \in \mathbb{Z}$. Montrer que $n\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$.
Correction : Soit $n\mathbb{Z} = \{nk, k \in \mathbb{Z}\} = \{\ldots, -2n, n, 0, n, 2n, \ldots\}$.
- Soit $(x_1, x_2) \in (n\mathbb{Z})^2$, $\exists (k_1, k_2) \in \mathbb{Z}^2$, $x_1 = nk_1$, $x_2 = nk_2 \Rightarrow x_1 + x_2 = n(k_1 + k_2) \Rightarrow x_1 + x_2 \in n\mathbb{Z}$ donc la loi est interne.

(- Soit $(x_1, x_2, x_3) \in (n\mathbb{Z})^3$, $\exists (k_1, k_2, k_3) \in \mathbb{Z}^3$, $x_1 = nk_1$, $x_2 = nk_2$, $x_3 = nk_3$. Or $(x_1 + x_2) + x_3 = (nk_1 + nk_2) + nk_3 = nk_1 + (nk_2 + nk_3) = x_1 + (x_2 + x_3)$ donc la loi est associative.)

(- $0_{\mathbb{Z}} = 0_{n\mathbb{Z}} = 0$. En effet, si $x \in n\mathbb{Z}$, $x + 0 = 0 + x = x$.)
- Soit $x \in n\mathbb{Z}$, $\exists k \in \mathbb{Z}$, $x = nk$. $\exists x' = n(-k) \in n\mathbb{Z}$, $x \times x' = n(k - k) = 0$ donc tout élément possède un symétrique.

Conclusion, $n\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$.

Exercice 45 Montrer que l'ensemble des racines n-ièmes de l'unité forment un sous-groupe de $(\mathbb{U}, \times)$.
Correction : On constate dans un premier temps que l'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité est un sous-ensemble de $\mathbb{U}$. En effet, si $z^n = 1$, on a en particulier $|z|^n = 1$, donc $|z| = 1$ (dans $\mathbb{R}^+$, l'équation $x^n = 1$ a une seule solution). Ensuite, il reste à faire les vérifications élémentaires : $\mathbb{U}_n$ contient 1, $\mathbb{U}_n$ est

stable par produit (si $z^n = z'^n = 1$, alors $(zz')^n = z^n z'^n = 1$) et par inverse (si $z^n = 1$, $\frac{1}{z^n} = 1$), donc c'est bien un sous-groupe multiplicatif de $\mathbb{U}$.

Exercice 46 On considère l'ensemble constitué des six fonctions de $\mathbb{R} - \{0, 1\}$ dans lui-même suivantes :

$$f_1(x) = x, \quad f_2(x) = \frac{1}{1-x}, \quad f_3(x) = \frac{x}{x-1}, \quad f_4(x) = \frac{1}{x}, \quad f_5(x) = 1 - x, \quad f_6(x) = \frac{x-1}{x}.$$

Montrer qu'il s'agit d'un groupe pour la composition (écrire sa table). Déterminer tous ses sous-groupes.
Correction : Le plus simple est de faire un tableau de loi :

o	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_6	f_4	f_5	f_3	f_1
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_3	f_2	f_1	f_6	f_5
f_5	f_5	f_4	f_6	f_2	f_1	f_3
f_6	f_6	f_1	f_5	f_3	f_4	f_2

Pour obtenir tous les sous-groupes, le plus simple est de les construire petit à petit. On connaît les sous-groupes triviaux : le groupe G tout entier et le sous-groupe réduit à l'élément neutre. Par ailleurs, tout sous-groupe contient f_1 qui est le neutre. Si on cherche un sous-groupe contenant f_1 et f_2, on voit que pour être stable par "o" il doit aussi contenir $f_2 \circ f_2 = f_6$. On constate que $\{f_1, f_2, f_6\}$ est un troisième sous-groupe de G. Par contre si on ajoute f_3, f_4 ou f_5 à f_1 et f_2, on est obligé pour avoir stabilité d'ajouter toutes les autres fonctions. Remarquons ensuite que $\{f_1, f_3\}$ est un sous-groupe de G, mais que si on y ajoute une troisième fonction, on va à nouveau retomber sur le sous-groupe trivial G. De même, $\{f_1, f_4\}$ et $\{f_1, f_5\}$ sont des sous-groupes, et on n'en obtient pas d'autres. Le groupe G a donc un sous-groupe à un élément, trois sous-groupes à deux éléments et un à trois éléments, et lui-même est un sous-groupe à six éléments.

Proposition 2.3.3 *Si (G, T) est un groupe, si H et K sont deux sous-groupes de G, alors $H \cup K$ est un sous-groupe de G si et seulement si $H \subseteq K$ ou $K \subseteq H$.*

Preuve : Soient H et K deux sous-groupes de G tels que $H \cup K$ soit un sous-groupe de G. Nous devons prouver qu'un des deux sous-groupes H ou K est contenu dans l'autre. Supposons que H ne soit pas contenu dans K et prouvons que K est contenu dans H. Soit k un élément de K. Il s'agit de prouver que k appartient à H. Puisque H n'est pas contenu dans K, il existe $h \in H$ tel que $h \notin K$. Puisque $H \cup K$ est un sous-groupe de G, nous avons $hTk \in H \cup K$. D'autre part, puisque $h \notin K$ et $k \in K$, nous avons $hTk \notin K$, donc $hTk \in H$, d'où $k \in H$ ce qui prouve que $K \subseteq H$.
La réciproque est évidente : si par exemple, $H \subseteq K$, $H \cup K = K$ et $H \cup K$ est naturellement un sous-groupe.■

Remarque 2.3.2 $H \cup K$ n'est pas en général un sous-groupe de G. Par exemple, soient H la droite d'équation $y = 0$ et K la droite d'équation $x = 0$ dans $\mathbb{R}^2$, groupe additif. Alors H et K sont des sous-groupes de $(\mathbb{R}^2, +)$ mais pas $H \cup K$ car $(1, 0) + (0, 1) = (1, 1)$ n'appartient pas à $H \cup K$.

Proposition 2.3.4 *Soient (G, T) un groupe et F une famille non vide de sous-groupes de G (F peut contenir un nombre fini ou infini de sous-groupes). Si I est l'intersection de tous les éléments de F, autrement dit $I = \cap_{H \in F} H$ alors I est lui-même un sous-groupe de G.*

Preuve : Considérons sans perte de généralité l'intersection $I = H \cap K$ de deux sous-groupes H et K. $H \cap K$ n'est pas vide car e appartient à $H \cap K$. Soient x et y appartenant à $H \cap K$. Comme H et K sont des sous-groupes de G, xTy^{-1} appartient à H et à K donc à $H \cap K$. D'où, $H \cap K$ est un sous-groupe de G. La démonstration se généralise à un nombre fini ou infini de sous-groupes. ■

Définition 2.3.5 *Soit (G,T) un groupe et A un sous-ensemble non vide de G. On appelle* ***sous-groupe engendré*** *par A le sous-groupe $< A >= \cap_{H \in S} H$ où S est l'ensemble de tous les sous-groupes de G qui contiennent A. Si g appartient à G, on note $< g >$ à la place de G.*

Cet ensemble n'est pas vide car il contient A lui-même et la formule ci-dessus est par conséquent bien définie.

Exemple 2.3.2 $< m >= m\mathbb{Z}$, $< G >= G$, $< m, n >= pgcd(m,n)\mathbb{Z}$ sont des sous-groupes engendrés.

Théorème 2.3.3 *Le sous-groupe $< A >$ est le plus petit sous-groupe (au sens de l'inclusion) de G contenant A. Autrement dit, $< A >$ est caractérisé par les deux conditions suivantes :*

1. *$< A >$ est un sous-groupe de G contenant A.*
2. *Si K est un autre sous-groupe de G contenant A on a $< A > \subset K$.*

Preuve : Soit $< A >$ le sous-groupe engendré par A. $< A >= \cap H$ où l'intersection porte sur les sous-groupes H de G contenant A. $< A >$ est donc un sous-groupe de G contenant A d'après la proposition 2.3.4. Soit K un sous-groupe de G contenant A. Alors, K fait partie de l'ensemble des sous-groupes sur lequel porte l'intersection définissant $< A >$ donc, $< A >$ étant inclus dans tout sous-groupe de G contenant A, $< A >$ est inclus dans K. Par conséquent, $< A >$ est le plus petit sous-groupe de G contenant A. ■

Proposition 2.3.5 *Tout sous-groupe de $\mathbb{Z}$ est de la forme $< n >= n\mathbb{Z}$ où n est un entier positif.*

Preuve : Soit H un sous-groupe de $\mathbb{Z}$ distinct de $\mathbb{Z}$.

- Si $H = 0$ alors $H =< 0 >$.
- Si $H = \mathbb{Z}$, $H =< 1 >$.
- On suppose que H est un **sous-groupe propre** de $\mathbb{Z}$ (donc différent de $\mathbb{Z}$ et de $\{1\}$). Soit n le plus petit élément strictement positif de H, montrons alors que $< n >= H$.
  n appartient à H sous-groupe de $\mathbb{Z}$ donc $< n >$ est inclus dans H ($< n >$ plus petit sous-groupe de $\mathbb{Z}$ contenant n).
  Montrons que H est inclus dans $< n >$: soit x appartenant à H. D'après la division euclidienne, il existe un couple d'entiers (i,j) avec $0 \leq j < n$ tel que $x = in + j$.
  Si i est positif, $in = n + ... + n$ appartient à H car n appartient à H et H est un sous-groupe de $\mathbb{Z}$.
  Si i est négatif, $in = (-n) + ... + (-n)$ appartient à H car n appartient à H et H est un sous-groupe de $\mathbb{Z}$.
  Comme x appartient à H sous-groupe de $\mathbb{Z}$, $j = x - in$ appartient à H. Or j est positif et strictement inférieur à n et n est le plus petit entier strictement positif appartenant à H donc $j = 0$. D'où, $x = in$ et x appartient donc à $< n >$. H est inclus dans $< n >$. Conclusion, $H =< n >= n\mathbb{Z}$.

■

Exercice 47 (*non corrigé*)

1. Soient $m\mathbb{Z}$ et $n\mathbb{Z}$ deux sous-groupes de $\mathbb{Z}$. Montrer que

$$m\mathbb{Z} + n\mathbb{Z} = \{mu + nv \mid u, v \in \mathbb{Z}\}$$

   a) est un sous-groupe de $\mathbb{Z}$,

b) contient $m\mathbb{Z}$ et $n\mathbb{Z}$,

c) est contenu dans tout sous-groupe de $\mathbb{Z}$ qui contient $m\mathbb{Z}$ et $n\mathbb{Z}$.

d) Si $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, que peut-on dire de d ?

2. Déterminer les sous-groupes engendrés par : $14\mathbb{Z} \cup 35\mathbb{Z}$; $4\mathbb{Z} \cup 8\mathbb{Z} \cup 6\mathbb{Z} \cup 64\mathbb{Z}$; $2\mathbb{Z} \cup 3\mathbb{Z}$; $4\mathbb{Z} \cup 21\mathbb{Z}$; $5\mathbb{Z} \cup 25\mathbb{Z} \cup 7\mathbb{Z}$; $\{70, 4\}$.

On introduit ensuite la notion de sous-groupe distingué (utilisée initialement par Galois). Les sous-groupes distingués connaissent des applications en géométrie dans l'étude des actions de groupes, en topologie algébrique dans la classification des revêtements, en théorie de Galois dans la correspondance de Galois.

Définition 2.3.6 *Un sous-groupe H d'un groupe (G, T) est **distingué** (ou **normal** ou **invariant**) si pour tout x de G et pour tout h de H, le produit $xThTx^{-1}$ est élément de H. On note alors $H \triangleleft G$ et on lit "H est distingué dans G".*

Un sous-groupe distingué H d'un groupe G est un sous-groupe globalement stable par l'action de G sur lui-même par conjugaison. Les sous-groupes distingués interviennent naturellement dans la définition du quotient d'un groupe.

Définition 2.3.7 *Pour tout x de G on note :*
- *xH l'ensemble (**classe à gauche**) des éléments de G de la forme xTh avec h élément de H,*
- *Hx l'ensemble (**classe à droite**) des éléments de G de la forme hTx avec h élément de H,*
- *xHx^{-1} l'ensemble des éléments de G de la forme $xThTx^{-1}$ avec h élément de H.*

Une façon équivalente de définir un sous-groupe distingué est de dire que les classes à droite et à gauche de H dans G coïncident, c'est-à-dire :

Proposition 2.3.6

$$\boxed{H \triangleleft G \text{ si et seulement si } xHx^{-1} = H \Leftrightarrow xH = Hx}$$

Preuve : Par définition, $H \triangleleft G \Leftrightarrow xHx^{-1} \subset H$ pour tout x de G. Or, $H \subset xHx^{-1}$. En effet, si $h \in H$, on aura :

$$h \in xHx^{-1} \Leftrightarrow \exists h' \in H,\ h = xTh'Tx^{-1} \Leftrightarrow \exists h' \in H,\ h' = x^{-1}ThTx$$

Vu que $H \triangleleft G$, $h' = x^{-1}ThTx$ est effectivement élément de H. Ainsi, on peut également dire $H \triangleleft G$ si et seulement si $xHx^{-1} = H \Leftrightarrow xH = Hx$. ∎

Exemple 2.3.3 Les déplacements du plan, constitués des translations et des rotations, constituent un groupe (non commutatif) pour la loi de composition des applications. Les translations en constituent un sous-groupe distingué.

Remarque 2.3.3
- $\{e\}$ et G sont toujours des sous-groupes distingués.
- Un sous-groupe de G de la forme xHx^{-1} avec $x \in G$ est appelé un **conjugué** de H. Par conséquent, un sous-groupe est distingué si et seulement s'il est son seul conjugué.

Exercice 48 Soit $(G, \times)$ un groupe et $\simeq$ une relation d'équivalence sur G. On suppose que cette relation est compatible avec la loi de groupe, c'est-à-dire que si $\forall x, y, x', y' \in G$, $x \simeq x'$ et $y \simeq y'$ alors $xy \simeq x'y'$.

Montrer que la classe H de l'élément neutre 1 est un sous-groupe distingué de G et que $\forall x, x' \in G$, $x \simeq x'$ est équivalent à $x'x^{-1} \in H$.
Correction : Étant donnés $y, z \in H$, on a $y \simeq 1$ et $z \simeq 1$. La compatibilité de la loi donne d'une part $yz \simeq 1$, soit $yz \in H$, et d'autre part $yy^{-1} \simeq y^{-1}$ soit $y^{-1} \in H$. Cela montre que H est un sous-groupe de G. Pour tout $x \in G$, on a aussi $xyx^{-1} \simeq x1x^{-1} = 1$ et donc $xyx^{-1} \in H$. Le sous-groupe H est donc distingué. De plus, pour $x, x' \in G$, si $x \simeq x'$, alors par compatibilité de la loi, on a $x'x^{-1} \simeq xx^{-1} = 1$, c'est-à-dire $x'x^{-1} \in H$.
Réciproquement, si $x'x^{-1} \in H$, alors $x'x^{-1} \simeq 1$, et donc, par compatibilité de la loi, $x \simeq x'$.

Proposition 2.3.7 *Si G est commutatif (groupe abélien), alors tout sous-groupe de G est distingué dans G.*

Preuve : Soit H un sous-groupe de G. (G, T) est commutatif donc tous les éléments de G commutent entre-eux y compris ceux qui sont dans H ((H, T) est donc commutatif). Par conséquent, $\forall x \in G$ et $\forall h \in H$, $xTh = hTx \Leftrightarrow xThTx^{-1} = h$ en composant à droite par x^{-1} (l'inverse de x, qui existe puisque (G, T) est un groupe). Comme $h \in H$, on conclut que tout sous-groupe H de G est distingué dans G. ■

Exemple 2.3.4 $(\mathbb{Z}, +)$ est commutatif et $n\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$ donc $n\mathbb{Z} \triangleleft \mathbb{Z}$.

2.3.3 Construction du quotient d'un groupe

Les sous-groupes distingués sont importants dans l'étude des groupes quotients à cause du résultat suivant : on peut construire un groupe quotient G/H de loi compatible avec celle de G si et seulement si H est un sous-groupe distingué de G. Plus précisément, dans l'étude des groupes, le quotient d'un groupe est une opération classique permettant la construction de nouveaux groupes à partir d'anciens. À partir d'un groupe G, et d'un sous-groupe H, on peut définir une loi de groupe sur l'ensemble G/H des classes de G suivant H, à condition que les classes latérales droites soient égales aux classes latérales gauches ($xH = Hx$).

Soient (G, T) et (H, T) désignant respectivement un groupe et un sous groupe de G.

Proposition 2.3.8 *Soient $x, y \in G$. La relation $\mathcal{R}$ définie par $x\mathcal{R}y \Leftrightarrow xTy^{-1} \in H$ est une relation d'équivalence(à droite) sur G.*

Preuve :
- $\mathcal{R}$ est réflexive : $\forall x \in G$, $xTx^{-1} = e \in H \Leftrightarrow x\mathcal{R}x$.
- Ensuite, comme H est un sous-groupe de G, tout élément dans H admet un inverse (dans H) donc $(xTy^{-1})^{-1} = yTx^{-1} \in H \Leftrightarrow y\mathcal{R}x$ (H étant stable par inversion). Par conséquent, $\mathcal{R}$ est symétrique.
- Montrons enfin que $\mathcal{R}$ est transitive : soit $(x, y, z) \in G^3$, ($x\mathcal{R}y$ et $y\mathcal{R}z$) $\Leftrightarrow$ ($xTy^{-1} \in H$ et $yTz^{-1} \in H$). $(xTy^{-1})T(yTz^{-1}) = xT(y^{-1}Ty)Tz^{-1} = xTeTz^{-1} = xTz^{-1} \in H \Leftrightarrow x\mathcal{R}z$ (car H est stable pour la loi de composition).

■

Par conséquent, ($\forall x, y \in H$, $x\mathcal{R}y$) $\Leftrightarrow$ (H est un sous-groupe de G) d'après la proposition 2.3.2 .

Proposition 2.3.9 *Soit $x \in G$. La classe d'équivalence (à droite) de x pour la relation $\mathcal{R}$ est l'ensemble $Hx = \{hTx, h \in H\}$. Elle est notée $cl(x)$ ou $\overline{x}$.*

Preuve : Par définition, $cl(x) = \{y \in G, x\mathcal{R}y\}$. Soit $y \in G$ équivalent à x pour la relation $\mathcal{R}$. Alors il existe $k \in H$ (dont l'inverse $k^{-1} = h$ est aussi dans H) tel que $xTy^{-1} = k \Leftrightarrow y = hTx$. Et donc y est élément de Hx. Réciproquement, si y est élément de Hx, il est clair que $x\mathcal{R}y$. ■

Remarque 2.3.4 On aurait aussi pu définir la relation d'équivalence (à gauche) $\mathcal{R}$ par $x\mathcal{R}y \Leftrightarrow y^{-1}Tx \in H$. Dans ce cas, la classe d'équivalence d'un élément x de G aurait été donnée par l'ensemble xH (classe à gauche de x de H).

Supposons que H soit un sous-groupe distingué de G. On désire définir une loi $\boxed{\mathrm{T}}$ sur l'ensemble quotient $G/\mathcal{R}$ de la façon la plus naturelle possible c'est-à-dire en posant $cl(x)\boxed{\mathrm{T}}cl(y) = cl(xTy)$. La justification de ce choix est la suivante : si X et Y sont deux classes d'éléments de G suivant H, XY en est une aussi. Il existe des éléments x et y de G tels que X et Y soient repectivement les classes de x et y suivant H. Nous avons alors $XY = (xH)(yH) = (Hx)(yH) = H(xTy)H$; comme H est distingué, nous pouvons remplacer $H(xTy)$ par $(xTy)H$ et nous trouvons $XY = xTyHH$. Mais $HH = H$ (puisque H est un sous-groupe de G), donc la relation obtenue peut s'écrire $XY = xTyH$, ce qui montre bien que XY est une classe suivant H (et plus particulièrement, la classe de xTy). De ce qui précède, il résulte qu'en faisant correspondre à une classe X et une classe Y l'ensemble XY, nous définissons une loi de composition $\boxed{\mathrm{T}}$ dans l'ensemble des classes suivant H et que cette loi peut être caractérisée par la relation

$$xH\boxed{\mathrm{T}}yH = (xTy)H \Leftrightarrow cl(x)\boxed{\mathrm{T}}cl(y) = cl(xTy).$$

Cette définition a un sens si et seulement si la classe $cl(xTy)$ ne dépend pas du choix des représentants x et y des classes $cl(x)$ et $cl(y)$, autrement dit si : pour $x, y, x', y' \in G$,

$$\left.\begin{array}{l} x\mathcal{R}x' \\ y\mathcal{R}y' \end{array}\right\} \Rightarrow xTy\mathcal{R}x'Ty'. \tag{2.1}$$

Si l'implication (2.1) est vérifiée, on dit que la relation d'équivalence $\mathcal{R}$ est compatible avec la loi T (cf. chapitre 1). On ajoute la définition suivante :

Définition 2.3.8 *La relation $\mathcal{R}$ est dite* ***compatible à droite*** *(respectivement* ***à gauche****) avec la loi T si*

$$\forall x, y, z \in G,\ x\mathcal{R}y \Rightarrow xTz\mathcal{R}yTz \text{ (respectivement } x\mathcal{R}y \Rightarrow zTx\mathcal{R}zTy)$$

On a alors le

Théorème 2.3.4 *La relation $\mathcal{R}$ est compatible avec la loi de groupe si et seulement si elle est compatible à droite et à gauche.*

Preuve : Le sens non trivial se montre ainsi : $x\mathcal{R}x'$ et $y\mathcal{R}y' \Rightarrow xTy\mathcal{R}x'Ty$ et $x'Ty\mathcal{R}x'Ty' \Rightarrow xTy\mathcal{R}x'Ty'$. ■

On considère enfin le théorème intermédaire suivant :

Théorème 2.3.5 *Il y a équivalence entre*

1. *La relation d'équivalence $\mathcal{R}$ est compatible à droite.*
2. *Il existe un sous-groupe H tel que $x\mathcal{R}y \Leftrightarrow xTy^{-1} \in H \Leftrightarrow y \in Hx$*

Preuve : Si $\mathcal{R}$ est compatible à droite, $x\mathcal{R}y \Leftrightarrow xTy^{-1}\mathcal{R}e \Leftrightarrow xTy^{-1} \in cl(e)$ et on vérifie que $H = cl(e)$ est bien un sous-groupe de G. Réciproquement si on a 2., $xTy^{-1} \in H \Leftrightarrow (xTz)T(yTz)^{-1} \in H$, $\mathcal{R}$ est compatible à droite. ■

Des deux théorèmes précédents on déduit :

Théorème 2.3.6 *Soit (G, T) un groupe et $\mathcal{R}$ une relation d'équivalence dans G. Il y a équivalence entre :*

1. *$cl(x)\boxed{T}cl(y) = cl(xTy)$ définit une loi de groupe sur $G/\mathcal{R}$.*
2. *La relation $\mathcal{R}$ est compatible à droite et à gauche avec la loi de groupe.*
3. *Il existe un sous-groupe H tel que*
   (a) *$\forall x \in G,\ xH = Hx \Leftrightarrow H$ est distingué dans G.*
   (b) *$x\mathcal{R}y \Leftrightarrow xTy^{-1} \in H \Leftrightarrow x^{-1}Ty \in H$.*

Pour conclure on donne la

Définition 2.3.9 *Soit $H \triangleleft G$. La relation $\mathcal{R}$ définie par*

$$x\mathcal{R}y \Leftrightarrow xTy^{-1} \in H$$

est appelée ***relation d'équivalence*** *suivant le sous-groupe H. L'ensemble quotient $G/\mathcal{R}$ est alors un groupe pour la loi naturelle, appelé* ***groupe quotient****, et se note G/H.*

Exemple 2.3.5 Soit la relation $\mathcal{R}$ définie sur $\mathbb{Z}$ par $x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{Z}/x - y = kn$, $\mathcal{R}$ est une relation d'équivalence. Cette relation est appelée **relation de congruence modulo** n. Deux entiers x et y en relation sont dits congrus l'un à l'autre modulo n et on note alors $x \equiv y \mod n$ (ou $x \equiv y[n]$). On remarquera que $x \equiv 0 \mod n$ si et seulement si n divise x.
Soit x appartenant à $\mathbb{Z}$. On note par $\overline{x}$ la classe d'équivalence de x pour la relation de congruence modulo n. On note par $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences de la relation de congruence modulo n. On peut alors déduire des résultats précédents que $\mathbb{Z}/n\mathbb{Z}$ est un groupe (abélien) pour la loi $\overline{x} + \overline{y} = \overline{x+y}$.
Si on considère $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, cela nous permet d'affirmer par exemle que $\overline{9} = \overline{4+5} = \overline{4}+\overline{5} = \overline{4}+\overline{0} = \overline{4+0} = \overline{4}$.

Exercice 49 On définit sur $\mathbb{R}^2$ la relation ρ par

$$(x, y)\rho(x', y') \Leftrightarrow x + y = x' + y'$$

1. Montrer que ρ est une relation d'équivalence.
2. Trouver la classe d'équivalence du couple $(0, 0)$.
3. Soit f l'application de $\mathbb{R}^2$ dans $\mathbb{R}$ définie par :
$$f : (x, y) \to x + y$$
Montrer que deux éléments de $\mathbb{R}^2$ équivalents modulo ρ ont même image par f et que deux éléments non équivalents ont des images distinctes.
4. En déduire qu'entre l'ensemble quotient $\mathbb{R}^2/\rho$ et $\mathbb{R}$ il existe une bijection g que l'on précisera.

Correction :

1. On montre aisément que ρ est réflexive, symétrique et transitive donc ρ est bien une relation d'équivalence.
2. La classe d'équivalence du couple $(0, 0)$ est constituée par l'ensemble des couples $(x, y) \in \mathbb{R}^2$ vérifiant $x + y = 0$. C'est l'ensemble des points situés sur la deuxième bissectrice du plan $x0y$.
3. Soient $u, v \in \mathbb{R}^2$, alors $u\rho v \Leftrightarrow f(u) = f(v)$. On en déduit également que deux éléments non équivalents ont des images distinctes.
4. g est l'application qui à une classe fait correspondre la somme des composants d'un représentant quelconque de cette classe. g est injective d'après la question précédente. Par ailleurs, $\forall \alpha \in \mathbb{R}$, on peut considérer que α est l'image de $(\frac{\alpha}{2}, \frac{\alpha}{2}) \in \mathbb{R}^2$ donc g est surjective et par conséquent bijective.

2.3.4 Homomorphismes de groupes

On doit à Marie Ennemond Camille JORDAN (1838-1922) le concept d'**homomorphisme** entre deux structures :

Définition 2.3.10 *Un* ***morphisme de groupes*** *ou* ***homomorphisme de groupes*** *(du grec homoios = semblable et morphê = forme) est une application entre deux groupes qui respecte la structure des groupes.*

Plus précisément, si (G, T) et $(G', \star)$ sont deux groupes d'éléments neutres respectifs e et n, une application $f : G \to G'$ est un morphisme de groupes lorsque :

$$\boxed{\forall (a,b) \in G \times G,\ f(aTb) = f(a) \star f(b)}$$

Un morphisme de groupes transporte la loi de groupe, et va ainsi conserver toutes les propriétés liées à cette loi. Il est donc intéressant d'étudier comment se comportent les principaux objets de la théorie des groupes par les morphismes.

Définition 2.3.11 *Un **isomorphisme** f est un homomorphisme bijectif.*

Proposition 2.3.10 *Si (G,T) et $(G',\star)$ sont deux groupes quelconques, et si f est un isomorphisme de G sur G', alors f^{-1} est un isomorphisme de G' sur G.*

Preuve : Si f est un isomorphisme, alors f est une bijection, donc f^{-1} aussi. Il suffit de montrer que f^{-1} est un morphisme de groupes. Soient x et y deux éléments quelconques de G'. On a alors : $f(f^{-1}(x)Tf^{-1}(y)) = f(f^{-1}(x))\star f(f^{-1}(y)) = x\star y$. D'où $f^{-1}(x)Tf^{-1}(y) = f^{-1}(x\star y)$ et f^{-1} est donc un isomorphisme de groupes de G' sur G. ■

Définition 2.3.12 *Lorsque $G = G'$, un homomorphisme est appelé **endomorphisme** et s'il est bijectif, on parlera d'**automorphisme**.*

Exemple 2.3.6

- L'application $f : (\mathbb{Q}^\star, \times) \to (\mathbb{Q}^+, \times)$ définie par $f(x) = \|x\|$ est un morphisme de groupes :
$$f(x \times y) = \|x \times y\| = \|x\| \times \|y\| = f(x) \times f(y),\ \forall x, y \in \mathbb{Q}^\star$$
- L'application $f : (\mathbb{R}^{+\star}, \times) \to (\mathbb{R}, +)$ définie par $f(x) = \ln x$ est un isomorphisme de groupes :
$$f(x \times y) = \ln(x \times y) = \ln x + \ln y = f(x) + f(y),\ \forall x, y \in \mathbb{R}^{+\star}.$$
- Soit $a \in \mathbb{R}$. L'application $f_a : (\mathbb{R}, +) \to (\mathbb{R}^{+\star}, \times)$ définie par $f_a(x) = a^x$ est un isomorphisme de groupes : on a
$$f_a(x+y) = a^{x+y} = a^x \times a^y = f_a(x) \times f_a(y),\ \forall x, y \in \mathbb{R}.$$
- L'application $f : (\mathbb{R}^\star, \times) \to (\mathbb{R}^\star, \times)$ définie par $f(x) = x^2$ pour tout $x \in \mathbb{R}^\star$ est un homomorphisme ; en effet
$$f(x \times y) = (x \times y)^2 = x^2 \times y^2 = f(x) \times f(y),\ \forall x, y \in \mathbb{R}^\star.$$
- L'application $f : (\mathbb{C}^\star, \times) \to (\mathbb{R}^\star, \times)$ définie par $f(z) = |z|$ pour tout $x \in \mathbb{C}^\star$ est un homomorphisme, car
$$f(z \times w) = |z \times w| = |z| \times |w| = f(z) \times f(w),\ \forall z, w \in \mathbb{C}^\star.$$
- L'application $f : (\mathbb{R}, +) \to (\mathbb{R}^{+\star}, \times)$ définie par $f(x) = e^x$ pour tout $x \in \mathbb{R}$ est un isomorphisme, car elle est bijective et
$$f(x+y) = e^{x+y} = e^x \times e^y = f(x) \times f(y),\ \forall x, y \in \mathbb{R}.$$
- L'application $f : (\mathbb{R}, +) \to (\mathbb{C}^\star, \times)$ définie par $f(x) = e^{2i\pi x}$ pour tout $x \in \mathbb{R}$ est un homomorphisme, car
$$f(x+y) = e^{2i\pi(x+y)} = e^{2i\pi x} \times e^{2i\pi y} = f(x) \times f(y),\ \forall x, y \in \mathbb{R}.$$

Proposition 2.3.11 *Lorsque G possède un élément neutre e, l'image homomorphe $f(e) = n$ est neutre dans $f(G)$. Si la loi T de G est associative, alors celle de $f(G)$ l'est aussi. Si G est un groupe, son image homomorphe $f(G)$ en est aussi un et $f(x^{-1}) = [f(x)]^{-1}$: l'inverse de $f(x)$ dans $f(G)$ est l'image de l'inverse de x dans G.*

Preuve : Si e est neutre dans G, $f(e) \star f(x) = f(eTx) = f(x)$ et $f(x) \star f(e) = f(xTe) = f(x)$, donc $f(e)$ est neutre dans $f(G)$. Si la loi T est associative, la loi $\star$ l'est aussi : $f[aT(bTc)] = f[(aTb)Tc]$, donc

$f(a) \star f(bTc) = f(a) \star [f(b) \star f(c)]$ et c'est aussi $f(aTb) \star f(c) = [f(a) \star f(b)] \star f(c)$. Enfin si x admet un inverse x^{-1} dans G, $f(xTx^{-1}) = f(e) = f(x) \star f(x^{-1})$ et c'est aussi $f(x^{-1}) \star f(x)$: l'inverse dans $f(G)$ de $f(x)$ existe et c'est $f(x^{-1})$. En d'autres termes $[f(x)]^{-1} = f(x^{-1})$. ■

Exercice 50 On considère sur $]-1,1[$ la loi $xTy = \dfrac{x+y}{1+xy}$, montrer que $(]-1,1[,T)$ est un groupe commutatif. Montrer qu'il est isomorphe à $(\mathbb{R},+)$.
Correction : On montre sans grande difficulté que T est commutative (même si ce n'est pas indispensable), associative $\left(xT(yTz) = (xTy)Tz = \dfrac{x+y+z+xyz}{xy+xz+yz}\right)$, d'élément neutre 0, et tout élément x est inversible, d'inverse $-x$. Le plus difficile est en fait de prouver que la loi T est bien une lci (loi de composition interne), c'est-à-dire de prouver que $]-1,1[$ est stable par T. Si $x<1$ et $y<1$, $(x-1)(y-1) = xy-x-y-1 < 0$, donc $-(1+xy) < x+y$, et en divisant par $1+xy$ qui est positif, on obtient $-1 < \dfrac{x+y}{1+xy}$. De même, en partant de $-1<x$ et $-1<y$, on obtient $\dfrac{x+y}{1+xy} < 1$. Finalement, T est bien une loi de groupe. On peut également remarquer que $th : \mathbb{R} \to]-1,1[$ est une application bijective vérifiant $th(x+y) = th(x)Tth(y)$. On peut en déduire immédiatement qu'il s'agit d'un isomorphisme de groupes.

Définition 2.3.13 *Si G' admet un élément neutre n, l'ensemble N des éléments de G dont l'image par f est n s'appelle le* ***noyau*** *de f, noté $Kerf$. L'**image** de f est définie par $Imf = f(G)$.*

Exemple 2.3.7 Soient $G = \{\phi_0, \phi_1, \phi_2, \phi_3, \phi_4, \phi_5\}$, $G' = \{\phi_0, \phi_1\}$ d'élément neutre ϕ_0, et $f : G \to G'$ définie par $f(\phi_0) = \phi_0$, $f(\phi_1) = \phi_1$, $f(\phi_2) = \phi_0$, $f(\phi_3) = \phi_0$, $f(\phi_4) = \phi_1$ et $f(\phi_5) = \phi_1$. Alors, $\mathrm{Ker}f = \{\phi_0, \phi_2, \phi_3\}$ et $\mathrm{Im}f = G'$.

Exercice 51 Montrer que $x \mapsto \dfrac{x}{|x|}$ est un endomorphisme de groupes de $(\mathbb{R}^\star, \times)$. Déterminer son noyau et son image. Même question pour l'application $\theta \mapsto e^{i\theta}$ (de $(\mathbb{R},+)$ dans $(\mathbb{C}^\star,\times)$).
Correction : Il suffit de vérifier que $\forall x,y \in \mathbb{R}^\star$, $\dfrac{x}{|x|} \times \dfrac{y}{|y|} = \dfrac{xy}{|xy|}$, ce qui est vrai. L'image de ce morphisme est $\{-1,1\}$, et son noyau $\mathbb{R}^{\star+}$.
L'application $\theta \mapsto e^{i\theta}$ est un morphisme car $e^{i(\theta+\theta')} = e^{i\theta}e^{i\theta'}$. Son image est $\mathbb{U}$ ($\mathbb{U}$ est l'ensemble des nombres dont le module est égal à 1) et son noyau $2\pi\mathbb{Z} = \{2k\pi | k \in \mathbb{Z}\}$.

Proposition 2.3.12 *Le morphisme de groupe f est injectif si et seulement si le noyau de f n'est constitué que de l'élément neutre de G.*

Preuve : Soient $x,y \in G$ tels que $f(x) = f(y)$; alors $f(x) \star f(y)^{-1} = f(xTy^{-1}) = n$ c'est-à-dire que $xTy^{-1} \in \ker(f)$. Par conséquent $\ker(f) = \{e\}$ si et seulement si $xTy^{-1} = e$ c'est-à-dire que $x = y$. ■

Exercice 52 Soit G un groupe et $a \in G$. Montrer que l'application $x \mapsto axa^{-1}$ est un automorphisme de groupes de $(G,\times)$.
Correction : Comme $a(xy)a^{-1} = axa^{-1}aya^{-1}$, l'application est un endomorphisme de groupes. De plus, si $axa^{-1} = e$, alors $ax = a$, donc $x = e$, autrement dit le noyau de ce morphisme est réduit à l'élément neutre, l'application est donc injective. Comme de plus un élément y a toujours un antécédent, en l'occurence $a^{-1}ya$, elle est également surjective, donc bijective. C'est donc un automorphisme de groupes, dont la réciproque est d'ailleurs $y \mapsto a^{-1}ya$.

Théorème 2.3.7 *Lorsque G est un groupe, le noyau N de f est un sous-groupe distingué de G.*

Preuve : Notons e l'élément neutre de G. $n = f(e)$ est neutre dans $f(G)$. Soit u un élément de N et x dans G :

$$f(xTuTx^{-1}) = f(x) \star f(u) \star f(x^{-1}) = f(x) \star n \star f(x^{-1}) = [f(x) \star n] \star f(x^{-1}) = f(x) \star f(x^{-1}) = f(xTx^{-1}) = f(e) = n.$$

Par conséquent $xTuTx^{-1} \in N$ et donc $N \triangleleft G$. ■
Cela implique d'après la section sur la construction du quotient d'un groupe qu'on peut construire un groupe quotient $G/N = G/\mathrm{Ker}f$ de loi compatible avec celle de G.

On a également le résultat important ci-desssous qui permet de compléter le théorème 2.3.6 :

Théorème 2.3.8 *Soit (G,T) un groupe et $H \triangleleft G$. L'application s définie par*

$$\begin{array}{rcl} s : (G,T) & \to & (G/H, \boxed{T}) \\ x & \mapsto & cl(x) \end{array}$$

est un morphisme de groupes. Il est surjectif. Son noyau est égal à H. Le morphisme s s'appelle la ***surjection (ou projection) canonique*** *de G sur G/H. On note parfois $s = s_H$.*

Preuve : s est une application puisque tout élément de G appartient à une et une seule classe d'équivalence ; pour tout $x, y \in G$ on a $s(xTy) = HxTy = Hx\boxed{\mathrm{T}}Hy = s(x)\boxed{\mathrm{T}}s(y)$ c'est-à-dire que s est un morphisme. s est surjective puisqu'aucune classe d'équivalence n'est vide. ■

Le théorème suivant et qui utlise les résultats précédents est dû à Emmy NOETHER (1882-1935)

Théorème 2.3.9 *(Premier théorème d'isomorphisme ou théorème de décomposition canonique)*
Soient (G,T) et $(G',\star)$ deux groupes et φ un homomorphisme de G dans G'. Il existe alors un isomorphisme ν de $G/Ker(\varphi)$ sur $\varphi(G)$ tel que $\varphi = \nu_o s$ où s est la surjection canonique de G sur $G/Ker(\varphi)$. On a donc $G/Ker(\varphi) \simeq \varphi(G)$.

Preuve : Montrons que l'application $\nu : G/Ker(\varphi) \mapsto \varphi(G) = Im(G)$ est un homorphisme bijectif.

1. ν est bien définie. En effet, $\forall Hx, Hy \in G/H$ tels que $Hx = Hy$, il vient que $xTy^{-1} \in H = Ker(\varphi)$ donc $\varphi(xTy^{-1}) = \varphi(x) \star \varphi(y)^{-1} = n$ d'où $\varphi(x) = \varphi(y)$ soit $\nu(Hx) = \nu(Hy)$.
2. ν est un morphisme, pour tout $Hx, Hy \in G/H$ on a
$$\nu(Hx\boxed{\mathrm{T}}Hy) = \nu(HxTy) = \varphi(xTy) = \varphi(x) \star \varphi(y) = \nu(Hx) \star \nu(Hy).$$
3. ν est surjective par définition, il reste à prouver que ν est injective. Pour tout $Hx, Hy \in G/H$ tels que $\nu(Hx) = \nu(Hy)$ on a $\varphi(x) = \varphi(y)$. On en déduit que $\varphi(xTy^{-1}) = n$ d'où $xTy^{-1} \in Ker(\varphi)$ et $Hx = Hy$. ■

Corollaire 2.3.1 *Si φ est un homorphisme surjectif alors $G/Ker(\varphi) \simeq G'$ du fait que $Im(\varphi) = G'$.*

Exercice 53 *(non corrigé)* Soit $(A, +, 0)$ un groupe abélien (commutatif) et soit $H \subset A$ un sous-groupe de A. Pour tout $a \in A$, la classe de a modulo H est définie par le sous-ensemble de A suivant

$$a + H = \{a + h, h \in H\} \subset A$$

1. Donner une condition nécessaire et suffisante pour que deux classes soient égales $(a + H = b + H)$. On note A/H l'ensemble des classes modulo H :
$$A/H = \{a + H, a \in A\}$$

2. Montrer que l'ensemble des classes modulo H forme une partition de A. Si, en outre, A est fini, montrer que toutes les classes ont le même cardinal. Combien y a-t-il de classes différentes dans ce cas ?

On définit la loi de composition interne suivante entre deux classes :

$$(a+H)\oplus(b+H)=(a+b)+H=\{a+b+h, h\in H\}$$

3. Montrer que $(A/H, \oplus, 0+H)$ est un groupe abélien. Ce groupe est appelé le groupe quotient de A par H.

Exercice 54 *(non corrigé)*

1. Soit $n\in\mathbb{Z}$, montrer que $n\mathbb{Z}=\{nk, k\in\mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z},+,0)$.
2. Montrer que tous les sous-groupes de $\mathbb{Z}$ sont de cette forme.

On note $(\mathbb{Z}/n\mathbb{Z}, \oplus, 0+n\mathbb{Z})$ le groupe abélien des classes modulo n. Pour tout $k\in\mathbb{Z}$, on notera $\overline{k}$ la classe $k+n\mathbb{Z}$ de k modulo n.

3. Que vaut $\overline{137}\oplus\overline{212}$ dans $\mathbb{Z}/13\mathbb{Z}$?
4. "Arithmétique horlogère" [Gauss] : "Je dois partir demain pour San Francisco à 9 heures. Le train mettra 126 heures pour relier Nice à Vladivostok. Il faudra ensuite 358 heures au bateau pour franchir le Golden Gate Bridge. En arrivant vais-je pouvoir manger mes pancakes favoris dans un café du port dont les horaires d'ouverture sont 7 heures - 11 heures ?

2.3.5 Les groupes finis et l'exemple du groupe symétrique

Définition 2.3.14 *Un groupe (ou sous-groupe) est dit **fini** si le nombre de ses éléments, appelé alors **ordre** du groupe (ou sous-groupe), est fini. On notera $|G|$ l'ordre du groupe G.*

Définition 2.3.15 *L'**ordre d'un élément** (on dit parfois période) a d'un groupe est le plus petit nombre entier positif m tel que $a^m=e$ (où e désigne l'élément neutre ou identité du groupe, et a^m désigne le produit de m copies de a). Si aucun m de la sorte n'existe, on dit que a est d'ordre **infini**.*

Proposition 2.3.13 *Si H est un sous-groupe fini de G et si x et y sont deux éléments de G alors les classes d'équivalence (à gauche ou à droite) de x et y pour la relation $\mathcal{R}$ ont même nombre d'éléments et ce nombre est égal au cardinal de H.*

Preuve : Soit T la loi de composition interne de G et x un élément de G. Posons $f: H\to xH, h\mapsto f(h)=xTh$; l'application f est injective car si h et h' sont des éléments de H tels que $f(h)=f(h')$ alors on a l'égalité $xTh=xTh'\Leftrightarrow h=h'$ car x est régulier. f est aussi surjective car si y est un élément de xH, alors il existe $h\in H$ tel que $y=xTh$ et donc $y=f(h)$. f étant à la fois injective et surjective, est bijective. Ceci prouve que H et xH ont même nombre d'éléments. Mais si y est un élément de G, yH et H auront aussi même nombre d'éléments. Donc xH et yH ont même cardinal.
De même on montrerait que toutes les classes à droite pour une relation $\mathcal{R}$, issue d'un sous groupe H de cardinal fini dans G, ont même nombre d'éléments, ce nombre étant égal à $|H|$. ■

Le théorème qui vient maintenant et qui résulte en partie de la proposition précédente est fondamental en algèbre.

Théorème 2.3.10 *(Lagrange) Soit G un groupe fini. Si H est un sous-groupe de G, alors le cardinal de H divise celui de G. On notera $|G/H|$ où $[G:H]$ le nombre $|G|/|H|$. $[G:H]$ s'appelle l'**indice** de H dans G.*

Preuve : Soit donc H un sous-groupe de G. On considère la relation d'équivalence $\mathcal{R}$ associée à H. Elle nous permet de définir une partition de G par des sous-ensembles de la forme xH où $x \in G$. On peut donc trouver, G étant fini, un nombre $n \in \mathbb{N}$ et $x_1, \ldots, x_n \in G$ tels que $\{x_1H, \ldots, x_nH\}$ forme une partition de G. Mais les sous-ensembles x_iH ont tous, d'après la proposition précédente, le même nombre d'éléments. De plus, ce nombre est égal à $|H|$. Donc le cardinal de G s'écrit $|G| = n|H|$. ■

On donne maintenant un corollaire du théorème de Lagrange qui est absolument fondamental dans la théorie des groupes finis.

Corollaire 2.3.2 *Soit G un groupe. Soit g un élément de G d'ordre fini. Alors l'ordre de g divise l'ordre de G.*

Preuve : Soient G et g comme dans l'énoncé et soit n l'ordre de g. Alors $\{g, g^2, \ldots, g^n = e\}$ est un sous groupe de G. Cette affirmation est triviale à vérifier. De plus, par définition de l'ordre d'un élément dans un groupe, ce sous-groupe est de cardinal n. Par application du théorème de Lagrange, n est un diviseur du cardinal de G. ■

Remarque 2.3.5 On peut se poser le problème réciproque, à savoir : Si p est un diviseur de l'ordre du groupe alors existe-t-il un élément d'ordre p dans G ou encore, existe-t-il un sous groupe d'ordre p dans G ? La réponse est donnée par le théorème de Cauchy pour les éléments d'ordre p et sous certaines conditions sur p, et par le théorème de Ludwig SYLOW (1832-1918), pour les sous-groupes d'ordre p, sous certaines conditions sur p et sur G.

Définition 2.3.16 *Un groupe, noté ici multiplicativement, est dit* ***monogène*** *s'il contient un élément g tel que tout élément de G s'écrive sous la forme g^n. On dit que le groupe est* ***engendré par*** *g. Un groupe monogène* ***fini*** *(possédant un nombre fini d'éléments) est dit* ***cyclique****.*

Exemple 2.3.8 Dans $\mathbb{C}$, ensemble des nombres complexes contenant le célèbre nombre i tel que $i^2 = -1$, considérons $G = \{1, i, -1, -i\}$ muni de la multiplication usuelle des nombres complexes : $(G, \times)$ est un groupe commutatif ; on peut établir sa table de Pythagore (ci-dessous).

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Un tel groupe est monogène (il est engendré par les puissances d'un de ses éléments : i (ou bien -i)). Ce groupe monogène de 4 éléments est fini et donc cyclique.

Plus généralement un groupe (G, T) d'élément neutre e, non réduit à $\{e\}$ sera monogène s'il existe un élément a de G distinct de e tel que $G = \{e, a, aTa, aTaTa, \ldots, a^{(n)}, \ldots\}$ en désignant par $a^{(n)}$ le composé de n éléments égaux à a (n non nul). Un tel groupe sera cyclique, s'il existe un entier n non nul pour lequel $a^{(n)} = e$. Le plus petit entier non nul vérifiant cette égalité est alors l'ordre du groupe.

Proposition 2.3.14 *Soit $|G| = p$ premier. Alors G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (en particulier, G est commutatif).*

Preuve : Soit $x \neq 1$ dans G, et soit $H =< x >$ le sous-groupe engendré par x. Alors $|H||G/H| = p$, et comme $|H| > 1$, $|H| = p$, et $H = G$. Or $< x >$ est toujours un groupe cyclique ; en fait, si $< x >$ est fini, comme c'est le cas ici, $< x >= \mathbb{Z}/d\mathbb{Z}$, où $d > 0$ est le cardinal de $< x >$. Donc on a bien $G =< x >\simeq \mathbb{Z}/p\mathbb{Z}$. ■

Exemple 2.3.9

- Le groupe additif $(\mathbb{Z}, +)$ des entiers relatifs est monogène (engendré par 1) mais il est infini donc non cyclique.
- Dans $(\mathbb{Q}, \times)$, l'ensemble des puissances entières d'un nombre non nul a est un groupe monogène infini, isomorphe à $(\mathbb{Z}, +)$ vu que $a^{m+n} = a^m \times a^n$. Il suffit pour s'en convaincre de considérer l'ensemble des puissances de 2.
- Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est monogène (engendré par la classe de 1) et fini : c'est un groupe cyclique.
- Dans $\mathbb{C}$, les racines n-ièmes de l'unité constituent un groupe cyclique multiplicatif (pour la multiplication).

Remarque 2.3.6 Par définition, un groupe cyclique est fini mais un groupe fini n'est pas nécessairement cyclique : on pourra considérer le cas du groupe symétrique ci-après ou encore le groupe de Klein.

On peut énoncer que, à un isomorphisme près, $(\mathbb{Z}, +)$ est le seul groupe monogène infini. Et, à un isomorphisme près encore, $(\mathbb{Z}/n\mathbb{Z}, +)$ est le seul groupe monogène fini. Il suit que :

Proposition 2.3.15 *Tout groupe monogène (donc tout groupe cyclique) est abélien (commutatif)*

On introduit ensuite un théorème de Cauchy sur les groupes finis : ce théorème fut également énoncé auparavant par Euler et Lagrange dans une formulation équivalente sans le secours de la notion algébrique de groupe :

Théorème 2.3.11 *Dans un groupe fini E d'ordre n (c'est-à-dire ayant n éléments), si k est l'ordre d'un sous-groupe F de E, alors k divise n.*

Preuve : utilisons la notation additive pour simplifier les écritures. Soit $\mathcal{R}$ la relation définie dans E par : $a\mathcal{R}b \Rightarrow a - b \in F$. Il est clair que $\mathcal{R}$ est une relation d'équivalence dont les classes sont en nombre fini (puisque E est fini). Dans E, b est en relation avec a si et seulement si $b = a + u$, $u \in F$. Par suite, le cardinal de toute classe est le cardinal k de F. Et puisque les classes forment une partition de E, il s'ensuit que si p est le nombre de classes, alors $n = pk$. ■

On a en corollaire l'important résultat suivant :

Corollaire 2.3.3 *Si G est un groupe fini d'ordre n d'élément neutre e, alors pour tout élément a de G : $a^{(n)} = e$.*

Intéressons nous maintenant au **groupe symétrique** c'est-à-dire le groupe des permutations d'un ensemble fini. Muni de la loi de composition des applications (loi "o"), l'ensemble des bijections d'un ensemble E dans lui-même, est un groupe, non commutatif si E possède plus de 2 éléments. L'application identique i est l'élément neutre du groupe. Lorsque E est fini et possède n éléments, ces bijections s'appellent des permutations (autrefois appelées substitutions) et leur groupe en possède $n!$ (factorielle n) : c'est un groupe fini, appelé groupe symétrique de E souvent noté S_n (S comme substitution). Il n'est pas cyclique.

Exemple 2.3.10 Lorsque $E = \{a, b, c\}$, le groupe symétrique de E, soit S_3, possède donc 6 éléments. Désignons par xyz la permutation $a \to x$, $b \to y$, $c \to z$, on peut alors les écrire : $i = abc$, acb, bac, bca, cab, cba. Par exemple, par composition, on voit que bca est la permutation inverse de cab (symétrique de cab pour la loi o) :

. cab : $a \to c$, $b \to a$, $c \to b$

. $bca : a \to b,\ b \to c,\ c \to a$
. $bca_o cab : a \to a,\ b \to b,\ c \to c$

C'est dire que $bca_o cab = i$, soit $bca^{-1} = cab$. On a la table suivante

o	abc	cab	bca	cba	acb	bac
abc	abc	cab	bca	cba	acb	bac
cab	cab	bca	abc	bac	cba	acb
bca	bca	abc	cab	acb	bac	cba
cba	cba	acb	bac	abc	cab	bca
acb	acb	bac	cba	bca	abc	cab
bac	bac	cba	acb	cab	bca	abc

acb, bac et cba étant leur propre symétrique, ils ne peuvent engendrer le groupe. On vérifiera que $bca^{(3)} = cab^{(3)} = i$: le groupe n'est donc pas cyclique. Mais on peut noter que $H = \{abc, cab, bca\}$ est un sous-groupe cyclique de S_3. A un isomorphisme près, H est le seul groupe fini d'ordre 3 ; on peut l'identifier à $\mathbb{Z}/3\mathbb{Z}$.

Théorème 2.3.12 *(Arthur CAYLEY (1821-1895)) Tout groupe fini d'ordre n est isomorphe à un sous-groupe du groupe symétrique S_n (lequel possède $n! = 1 \times 2 \ldots (n-1) \times n$ éléments).*

Définition 2.3.17 *Une permutation opérant sur $(x, y, z, \ldots, t, u)$ est dite* ***circulaire*** *pour signifier que $(x, y, z, \ldots, t, u)$ est transformé en $(y, z, \ldots, u, x)$: tout est décalé d'un rang et le dernier terme prend la place du premier.*

2.4 Les anneaux

Le terme est de David HILBERT (1862-1943).

2.4.1 Les anneaux

L'étude des anneaux trouve sa source dans la théorie des polynômes et la théorie des entiers algébriques. Richard Dedekind fut le premier à introduire le concept d'anneau mais le terme "anneau" (ou plus précisément le terme allemand Zahlring) a été utilisé en premier par David Hilbert en 1897. La première définition axiomatique d'un anneau fut donnée par Abraham Adolf FRAENKEL (1891-1965) en 1914 et Emmy Noether donna quant-à elle la première fondation axiomatique de la théorie des anneaux commutatifs dans son remarquable article "Ideal Theory in Rings" en 1921.

Définition 2.4.1 *On appelle ainsi un groupe abélien $(A, +)$ muni d'une seconde loi, souvent appelée multiplication, notée ici "$\times$", associative et distributive sur ou par rapport à la loi de groupe (addition), c'est-à-dire que pour tout triplet (a, b, c) d'éléments de A :*

- $(a \times b) \times c = a \times (b \times c)$ *(associativité)*
- $a \times (b + c) = a \times b + a \times c$ *et* $(a + b) \times c = a \times c + b \times c$ *(distributivité)*

Par conséquent, un anneau est un triplet $(A, +, \times)$ tel que :

- A est un ensemble ;
- $+$ est une loi de composition interne telle que $(A, +)$ soit un groupe commutatif ; ce qui implique que
  - la loi $+$ est associative ;
  - A contient au moins un élément : l'élément neutre pour la loi $+$, noté 0 ;
  - tout élément a de A a un opposé, noté $-a$;

  - la loi $+$ est commutative ($a+b=b+a$) ;
- $\times$ est une loi de composition interne associative et distributive par rapport à $+$;

Remarque 2.4.1 Si seule est vérifiée l'égalité $a\times(b+c)=a\times b+a\times c$, on parle de distributivité à gauche. Si seule est vérifiée l'égalité $(a+b)\times c=a\times c+b\times c$, on parle de distributivité à droite. Mais pour un anneau, on doit avoir la distributivité à gauche et à droite : on parle d'ailleurs parfois de double distributivité.

Définition 2.4.2 *L'anneau est dit* ***unifère*** *(ou unitaire) si sa multiplication admet un élément neutre. Cet élément est dit* ***unité****. Il est dit* ***commutatif*** *si sa multiplication est commutative. L'élément neutre du groupe est dit* ***nul*** *et souvent appelé zéro par analogie avec l'anneau* $(\mathbb{Z},+,\times)$.

Exemple 2.4.1

- L'ensemble des entiers relatifs, $\mathbb{Z}$, muni de l'addition (la loi $+$) et de la multiplication (la loi $\times$) est un anneau.
- L'ensemble des entiers congruents modulo un nombre entier donné n est un anneau pour la loi provenant de la congruence ; il est noté $\mathbb{Z}/n\mathbb{Z}$.
  Ainsi $\mathbb{Z}/2\mathbb{Z}$ pour les lois $+$ et $\times$ est un anneau. 0 correspond aux nombres pairs et 1 aux nombres impairs. On retrouve alors les résultats suivants :
  - Un pair plus un pair est pair ($0+0=0$).
  - Un impair plus un pair est impair ($0+1=1+0=1$).
  - Un impair plus un impair est pair ($1+1=0$).
  - Un pair fois un entier quelconque est pair ($0\times x=0$).
  - Un impair fois un impair est impair ($1\times 1=1$).
- Un corps (voir plus loin) est un cas particulier d'anneau. En particulier, l'ensemble des nombres rationnels muni de l'addition et de la multiplication usuelles est un anneau.
- L'ensemble des réels s'écrivant $a+b\sqrt{2}$, où a et b sont des entiers relatifs, muni de l'addition et de la multiplication usuelles est un anneau.
- Les endomorphismes d'un espace vectoriel (applications linéaires de l'espace vers lui-même) forment un anneau, avec l'addition de fonction pour la loi $+$, et la composition pour la loi $\times$. L'identité est un élément neutre pour $\times$, donc c'est un anneau unifère. Il n'est pas commutatif en général. C'est une grande source de contre-exemples à des affirmations fausses sur les anneaux.
- Plus généralement les endomorphismes d'un groupe abélien forment un anneau.
- En particulier, l'ensemble des matrices 2×2 muni de l'addition et de la multiplication est aussi un anneau non commutatif unifère.
- L'ensemble des polynômes à coefficients dans un anneau est aussi un anneau.
- L'ensemble des fonctions d'un ensemble dans un anneau muni des lois héritées de l'anneau (c'est-à-dire $(f+g)(x)=f(x)+g(x)$ et $(f\times g)(x)=f(x)\times g(x)$) forme un anneau.

Exercice 55 (*non corrigé*) Soit $(A,+,\times)$ un anneau et h un homomorphisme de A vers un ensemble muni de deux lois de composition internes $(E,\oplus,\otimes)$. Prouver que l'image homomorphe $(h(A),\oplus,\otimes)$ est un anneau.

Exercice 56 Un élément x d'un anneau A est dit **nilpotent** s'il existe un entier $n\geq 1$ tel que $x^n=0$. On suppose que A est commutatif, et on fixe x, y deux éléments nilpotents.

1. Montrer que xy est nilpotent.
2. Montrer que $x+y$ est nilpotent.
3. Montrer que 1_A-x est inversible.
4. Soient u, $v\in A$ tels que uv est nilpotent. Montrer que vu est nilpotent.

Correction : Soient n,m tels que $x^n=0$ et $y^m=0$.

1. Puisque x et y commutent, on a $(xy)^n = x^n y^n = 0 \times y^n = 0$.
2. Remarquons d'abord que pour $p \geq n$, on a $x^p = x^{p-n}x^n = 0$. D'après la formule du binôme, $(x+y)^{n+m} = \sum_{k=0}^{n+m} \left(\begin{array}{c} n+m \\ k \end{array} \right) x^k y^{n+m-k}$. Mais, pour $k \geq n$, $x^k = 0 \Rightarrow x^k y^{n+m-k} = 0$. D'autre part, pour $k < n$, on a $n+m-k \geq m$ et donc $y^{n+m-k} = 0 \Rightarrow x^k y^{n+m-k} = 0$. Ainsi, $(x+y)^{n+m} = 0$. On pourrait même se contenter de prendre la puissance $n+m-1$.
3. L'idée est d'utiliser l'identité remarquable (toujours valable dans un anneau)
$$1 - x^p = (1-x)(1 + x + \ldots + x^{p-1}).$$
Si on l'applique pour $p = n$, alors on obtient $1 - x^n = 1 = (1-x)(1 + x + \ldots + x^{n-1})$ ce qui implique que $1 - x$ est inversible d'inverse $1 + x + \ldots + x^{n-1}$.
4. Soit $n \geq 1$ tel que $(uv)^n = 0$. Alors $(vu)^{n+1} = v(uv)^n u = v \times 0 \times u = 0$. Ainsi, vu est nilpotent.

Exercice 57 Soit A un anneau non nécessairement commutatif et soient $a, b \in A$ tels que $1 - ab$ soit inversible. Montrer qu'alors $1 - ba$ est également inversible.
Correction : Soit c l'inverse de $1 - ab$. On a

$$(1 + bca)(1 - ba) = 1 - ba + bca - bcaba = 1 - ba + bc(1 - ab)a = 1 - ba + ba = 1$$
$$(1 - ba)(1 + bca) = 1 - ba + bca - babca = 1 - ba + b(1 - ab)ca = 1 - ba + ba = 1$$

Ainsi $1 - ba$ est inversible d'inverse $1 + bca$.

Exercice 58 Soit A un anneau commutatif. On appelle **élément idempotent** tout élément $x \in A$ vérifiant $x^2 = x$.

1. Si A est le produit de deux anneaux B et C, montrer qu'il existe des éléments idempotents de A distincts de 0 et de 1.
2. Supposons qu'il existe un élément $b \in A$ idempotent distinct de 0 et de 1. On pose $c = 1 - b$, $B = bA$ et $C = cA$.
   (a) Montrer que c est idempotent et que $bc = 0$.
   (b) Montrer que B et C sont stables pour l'addition et la multiplication de A. En déduire que B et C sont des anneaux non nuls.
   (c) Montrer que l'application
   $$\begin{array}{rcl} \varphi : A & \to & B \times C \\ x & \mapsto & (bx, cx) \end{array}$$
   est un isomorphisme d'anneaux (qui permet d'identifier A avec $B \times C$).
   (d) Les anneaux B et C sont-ils des sous-anneaux de A ?

Correction :

1. Les éléments $0_A = (0_B, 0_C)$ et $1_A = (1_B, 1_C)$ sont des éléments idempotents, mais il en est de même des éléments $(0_B, 1_C)$ et $(1_B, 0_C)$.
2. (a) On a
$$c^2 = (1-b)^2 = 1 - 2b + b^2 = 1 - 2b + b = 1 - b = c$$
$$bc = b(1-b) = b - b^2 = b - b = 0$$
ainsi c est un élément idempotent de A et $bc = 0$.

(b) Soient $x, y \in B$, il existe $x', y' \in A$ tels que $x = bx'$ et $y = by'$. Alors $x+y = bx'+by' = b(x'+y') \in B$ et $xy = bx'by' = b(x'by') \in B$. Ainsi B est stable pour l'addition et la multiplication et donc leurs restrictions sont des lois de composition interne dans B. Comme ces lois sont commutatives, associatives et l'une distributive sur l'autre dans A, il en est de même de leurs restrictions à B. Et 0 étant l'élément neutre pour l'addition dans A et appartenant à B, c'est l'élément neutre pour l'addition dans B. Soit $x \in B$, il existe $b' \in A$ tel que $x = bx'$ et $bx = bbx' = bx' = x$ donc b est l'élément neutre pour la multiplication dans B. Ainsi B est un anneau commutatif non nul. De même C est un anneau commutatif non nul.

(c) Soient $x, y \in A$. On a

$$\varphi(x+y) = (b(x+y), c(x+y)) = (bx+by, cx+cy) = (bx, cx) + (by, cy) = \varphi(x) + \varphi(y)$$
$$\varphi(xy) = (bxy, cxy) = (bxby, cxcy) = (bx, cx)(by, cy) = \varphi(x)\varphi(y)$$

Et $\varphi(1) = (b, c)$, qui est l'élément neutre de $B \times C$. Ainsi φ est un morphisme d'anneaux.
Soit $x \in A$, on a

$$\varphi(x) = 0 \Rightarrow (bx, cx) = 0 \Rightarrow bx = cx = 0 \Rightarrow x = (b+c)x = 0$$

Donc φ est injective.
Soit $(x, y) \in B \times C$, il existe $x', y' \in A$ tels que $x = bx'$ et $y = cy'$. Alors

$$\varphi(x+y) = (b(bx'+cy'), c(bx'+cy')) = (b^2x' + bcy', cbx' + c^2y') = (bx', cy') = (x, y)$$

Donc φ est surjective. Ainsi φ est un isomorphisme d'anneaux de A sur $B \times C$.

(d) Les anneaux B et C ne sont pas des sous-anneaux de A car ils n'ont pas les mêmes éléments unités (voir section suivante).

2.4.2 Sous-anneau

Définition 2.4.3 *Une partie B de A est un **sous-anneau** de A si, muni des opérations de A, B est lui-même un anneau. Pour qu'il en soit ainsi il faut et il suffit que :*

- *B soit un sous-groupe de A,*
- *pour tout couple (u, v) d'éléments de B, $u \times v$ soit élément de B.*

Exemple 2.4.2

- $(\mathbb{Z}, +, \times)$, anneau des entiers relatifs, est un sous-anneau de $(\mathbb{Q}, +, \times)$, anneau des nombres rationnels.
- Tout sous-groupe de $\mathbb{Z}$ contenant 1 est $\mathbb{Z}$ lui-même. On en déduit que le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même.

Exercice 59 Montrer que l'ensemble $\mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2}/(a, b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$.
Correction : Tout est très simple, il ne faut juste oublier aucune vérification : $\mathbb{Z}[i\sqrt{2}]$ contient 0 et 1, est stable par somme et par produit, et par opposé, c'est un sous-anneau de $\mathbb{C}$.

Exercice 60 On considère $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau.
2. On note $N(a + b\sqrt{2}) = a^2 - 2b^2$. Montrer que, pour tous x, y de $\mathbb{Z}[\sqrt{2}]$, on a $N(xy) = N(x)N(y)$.
3. En déduire que les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont ceux s'écrivant $a + b\sqrt{2}$ avec $a^2 - 2b^2 = \pm 1$.

Correction :

1. Il suffit de prouver que $\mathbb{Z}[\sqrt{2}]$ un sous-anneau de $(\mathbb{R}, +, \times)$. $\mathbb{Z}[\sqrt{2}]$ est
   - stable par la loi $+$: $(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2}$.
   - stable par la loi $\times$: $(a + b\sqrt{2}) \times (a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2}$.
   - stable par passage à l'opposé $-(a + b\sqrt{2}) = -a + (-b)\sqrt{2}$.

De plus, 0 et $1 \in \mathbb{Z}[\sqrt{2}]$, ce qui achève la preuve.

2. Posons $x = a + b\sqrt{2}$ et $y = a' + b'\sqrt{2}$. En tenant compte de la formule pour le produit obtenue à la question précédente, on a $N(xy) = (aa' + 2bb')^2 - 2(ab' + a'b)^2 = (aa')^2 - 2(ab')^2 - 2(a'b)^2 + (4bb')^2$. D'autre part, $N(x) \times N(y) = (a^2 - 2b^2)(a'2 - 2b'^2) = (aa')^2 - 2(ab')^2 - 2(a'b)^2 + (4bb')^2$.
3. Soit $x = a + b\sqrt{2}$. Supposons d'abord que x est inversible, d'inverse y. Alors $N(xy) = N(1) = 1$, et donc $N(x)N(y) = 1$. Puisque $N(x)$ et $N(y)$ sont tous les deux des entiers, on a nécessairement $N(x) = \pm 1$. Réciproquement, si $N(x) = \pm 1$, alors, en utilisant la quantité conjuguée : $\dfrac{1}{a + b\sqrt{2}} = \dfrac{a - b\sqrt{2}}{a^2 - 2b^2} = \pm(a - b\sqrt{2})$ ce qui montre que $a + b\sqrt{2}$ est inversible, d'inverse $\pm(a - b\sqrt{2})$.

Exercice 61 Montrer que l'ensemble des suites réelles, muni de la somme et du produit terme par terme, est un anneau. Quels sont ses éléments inversibles (pour le produit) ? Parmi les ensembles suivants, lesquels en sont des sous-groupes ou des sous-anneaux :

1. suites bornées
2. suites monotones
3. suites convergentes
4. suites périodiques
5. suites divergeant vers $+\infty$

Correction : Le fait que l'ensemble des suites soit un anneau ne pose aucun problème. L'associativité et la commutativité des deux lois découlent de celles des opérations similaires sur les réels, puisqu'on fait les sommes et produits terme à terme. L'élément neutre pour la somme est la suite nulle, et celui pour le produit est la suite constante égale à 1. Enfin, l'opposé d'une suite (u_n) est la suite $(-u_n)$. Les suites inversibles sont celles qui ne s'annulent jamais, on peut alors inverser terme à terme.

1. Les suites bornées forment un sous-anneau de cet anneau : le sous-anneau contient les neutres, il est stable par opposition (si $m \leq u_n \leq M$) pour tout n, on a $(-M \leq u_n \leq -m)$, par somme (il suffit de prendre la somme des bornes) et même par produit (c'est un peu plus compliqué à cause des changements de signes, mais en prenant le plus gros produit parmi les valeurs absolues des quatre possibles, c'est un majorant du produit des deux suites).
2. Les suites monotones ne forment pas un sous-anneau, ce n'est pas stable par somme (une croissante plus une décroissante, cela peut donner n'importe quoi).
3. Pour les suites convergentes, aucun problème, les stabilités découlent des propriétés sur les limites de suites.
4. Les suites périodiques forment aussi un sous-anneau : il contient les neutres (une suite constante est périodique de période 1), stable par opposition (même période) et par somme et produit (le produit des deux périodes, par exemple, est alors une période).
5. Les suites divergeant vers $+\infty$ ne forment pas un sous-anneau, ce n'est pas stable par passage à l'opposé.

2.4.3 Anneau intègre, diviseur de zéro

Définition 2.4.4 *Un anneau est dit* ***intègre*** *si un produit nul nécessite que l'un des facteurs soit nul (égal à l'élément neutre pour l'addition). Lorsqu'un produit a.b est nul alors que ni a, ni b le sont, on dit que a et b sont des* ***diviseurs de zéro.***

Justifions cette appellation par un exemple fondamental :

Exemple 2.4.3 L'ensemble des matrices carrées d'ordre 2 à termes réels muni de l'addition et de la multiplication usuelles $(\mathcal{M}_2(\mathbb{R}), +, \times)$ est un anneau unitaire non commutatif et non intègre.
On a ce résultat étonnant puisqu'on est habitué à rencontrer un produit nul si et seulement si l'un des facteurs est nul :

$$\begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix} \times \begin{pmatrix} 2 & -1 \\ -4 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Le produit de deux matrices non nulles peut être nul !

Exemple 2.4.4
- L'ensemble $\mathbb{Z}$ des entiers relatifs est un anneau intègre.
- L'anneau des congruences modulo 6 noté $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre car on peut y écrire $\overline{3} \times \overline{2} = \overline{6} = \overline{0}$.
- L'anneau $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ n'est pas intègre, $(\overline{1}, \overline{0})$ et $(\overline{0}, \overline{1})$ sont deux éléments non nuls dont le produit est nul.

Ce dernier exemple découle de la proposition suivante :

Proposition 2.4.1 *L'anneau des congruences modulo n noté $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.*

Preuve : Cette proposition est une conséquence directe de l'identité de Bézout (Étienne BÉZOUT 1730-1783). Supposons n premier, alors si a est un entier premier avec n, c'est-à-dire non multiple de n, il existe deux entiers b et c tels que $ab + nc = 1$, ce qui signifie que la classe de a est inversible d'inverse la classe de b.
Réciproquement si n n'est pas premier, il existe deux entiers a et b différents de n et de 1 tels que leur produit est égal à n. La classe de a ainsi que la classe de b sont donc des diviseurs de zéro. ■

Exercice 62 Soit E un ensemble. Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau. En préciser les éléments neutres, les éléments inversibles (et leur inverse) pour chacune des deux lois. Cet anneau est-il intègre ? Si $F \subset E$, $(\mathcal{P}(F), \Delta, \cap)$ est-il un sous-anneau de $\mathcal{P}(E)$?
Correction : Les deux lois Δ et $\cap$ sont internes, commutatives, associatives et distributives l'une par rapport à l'autre. De plus, Δ possède un élément neutre qui est $\emptyset$, $\cap$ possède pour élément neutre E, et tout élément A de $\mathcal{P}(E)$ est inversible pour Δ, son inverse étant lui-même puisque $A\Delta A = (A \backslash A) \cup (A \backslash A) = \emptyset$. On est donc bien en présence d'un anneau.
Les éléments inversibles pour $\cap$ sont les parties A de E telles qu'il existe $B \subset E$ pour laquelle $A \cap B = E$. Ceci ne peut se produire que si $A = B = E$, donc le neutre est le seul élément inversible pour $\cap$. Pour que l'anneau soit intègre, il faudrait avoir $A \cap B = \emptyset \Rightarrow A = \emptyset$ ou $B = \emptyset$, ce qui n'est pas le cas (il suffit de prendre A non vide tel que A est non vide, ce qu'on peut toujours trouver dans un ensemble comportant au moins deux éléments). Enfin, $(\mathcal{P}(F), \Delta, \cap)$ n'est pas un sous-anneau de E car il ne contient pas l'élément neutre pour l'intersection, bien qu'il soit lui-même un anneau.

2.4.4 Idéal d'anneau

En mathématiques, un idéal est une structure algébrique définie dans un anneau. Les idéaux généralisent de façon féconde l'étude de la divisibilité pour les entiers. Il est ainsi possible d'énoncer des versions très générales de théorèmes d'arithmétique tels que le théorème des restes chinois ou le théorème fondamental de l'arithmétique, valables pour les idéaux. On peut aussi comparer cette notion à celle de sous-groupe distingué pour la structure algébrique de groupe en ce sens qu'elle permet de définir la notion d'anneau quotient.

Définition 2.4.5 *Un **idéal d'anneau** est un sous-groupe additif J d'un anneau A stable pour le produit par un élément de A (seconde loi).*

Par stabilité, on entend ici que pour tout a de A et tout x de J, les produits $a \times x$ et $x \times a$ sont éléments de J. Une telle partie est souvent qualifiée de bilatère. Un idéal à gauche (respectivement à droite) se limite à la condition $a \times x$ (respectivement $x \times a$) est élément de J.

Exemple 2.4.5 Un exemple élémentaire est donné par les sous-groupes additifs de $\mathbb{Z}$ de la forme $n\mathbb{Z}$, ensemble des multiples de l'entier relatif n.

Remarque 2.4.2 Un idéal joue, pour les anneaux, le même rôle que les sous-groupes distingués pour les groupes.

- Soient A et B deux anneaux et f un morphisme de A dans B, alors le noyau de f est un idéal bilatère.
- Soient A un anneau et I un idéal bilatère de A, alors le groupe quotient A/I peut être muni d'une unique structure d'anneau telle que la surjection canonique de A dans A/I soit un morphisme d'anneaux.
- Soient A et B deux anneaux, φ un morphisme d'anneau de A dans B. Notons s l'application canonique de A dans l'anneau quotient A/I et i le morphisme de $f(A)$ dans B qui à b associe b. Alors, i est une injection, s une surjection et il existe une bijection b telle que $\varphi = i_o b_o s$ (on a utilisé le théorème de décomposition canonique avec $\nu = i_o b$ où ν est un isomorphisme de A/I sur $\varphi(A)$).

Définition 2.4.6 *Soient A un anneau commutatif unitaire, a un élément de A et I un idéal de A. Un idéal I de A est dit **premier** si et seulement si le quotient de A par I est intègre et qu'il est différent de l'anneau réduit à l'élément nul.*

On peut exprimer cette définition à l'aide de la condition suivante :

Proposition 2.4.2 *Un idéal I de A est premier si et seulement si c'est un idéal propre (différent de A) et si :*

$$\forall x, y \in A,\ xy \in I \Rightarrow x \in I \text{ ou } y \in I$$

Cette proposition est l'équivalent du lemme d'Euclide : "si un nombre premier divise le produit ab alors il divise soit a soit b".

Exemple 2.4.6 Si n est un nombre premier, $I = n\mathbb{Z}$ est un idéal premier. En effet, d'après la proposition 2.4.1, $\mathbb{Z}/n\mathbb{Z}$ est intègre ssi n est premier.

Définition 2.4.7 *Soit A un anneau. Soit I un idéal de A.*

- *I est dit **principal à gauche** s'il existe un élément $a \in I$ tel que, pour tout $x \in I$, il existe un élément $y \in A$ tel que $x = y \times a$: $I = \{x \times a / x \in A\}$. On note $I = Aa$.*
- *I est dit **principal à droite** s'il existe un élément $a \in I$ tel que, pour tout $x \in I$, il existe un élément $y \in I$ tel que $x = a \times y$: $I = \{a \times x / x \in A\}$. On note $I = aA$.*
- *I est dit **principal** s'il est principal à la fois à gauche et à droite (ce qui est toujours le cas si A est commutatif). Dans ce cas, on peut noter $I = aA$ et I est forcément le plus petit idéal contenant a.*

Exemple 2.4.7

- Pour tout entier relatif k, $k\mathbb{Z} = \{kx / x \in \mathbb{Z}\}$ est un idéal principal de $\mathbb{Z}$.
- Un idéal n'est pas forcément principal. Par exemple, si $A = \mathbb{C}[X, Y]$, l'anneau commutatif des polynômes à deux indéterminées à coefficients complexes, l'ensemble des polynômes ayant un terme constant nul, noté (X, Y) car engendré par ces deux variables, est un idéal de $\mathbb{C}[X, Y]$, mais il n'est pas principal : si P engendrait (X, Y), X et Y seraient divisibles par P, ce qui est impossible, sauf si P est un polynôme constant non nul, ce qui est contradictoire.

Définition 2.4.8 *Un anneau intègre dont tous les idéaux sont principaux est dit **anneau principal**.*

Les anneaux principaux forment un type d'anneaux important dans la théorie mathématique de la divisibilité. Ce sont les anneaux intègres (commutatifs unitaires non nuls) auxquels on peut étendre deux théorèmes qui, au sens strict, concernent l'anneau des entiers relatifs : le théorème de Bachet-Bézout et le théorème fondamental de l'arithmétique qu'on rappelle :

Théorème de Bachet-Bézout : Si a et b sont deux éléments de A n'ayant pas d'autres diviseurs communs que les éléments du groupe des unités de l'anneau, alors il existe u et v éléments du groupe tel que $a \times u + b \times v = 1$.

Théorème fondamental de l'arithmétique : Un anneau principal est un anneau factoriel, c'est-à-dire que tout élément de l'anneau se décompose de manière unique en un produit de facteurs irréductibles et d'une unité (à un facteur inversible près).

Exemple 2.4.8 $\mathbb{Z}$ ou l'anneau $\mathbb{K}[X]$ des polynômes sur un corps $\mathbb{K}$ sont des anneaux principaux.

Définition 2.4.9 *Un **anneau euclidien** est un anneau disposant d'une division euclidienne. Un tel anneau est toujours principal.*

Exemple 2.4.9 Des exemples de cette nature sont donnés par
- l'ensemble des entiers relatifs $\mathbb{Z}$,
- l'ensemble des polynômes à coefficients dans un corps, par exemple celui des rationnels, réels ou complexes.

Remarque 2.4.3 Tous les anneaux principaux ne sont pas euclidiens

2.4.5 Intersection, somme et produit d'idéaux

Proposition 2.4.3 *Dans un anneau A, l'**intersection** de deux idéaux est un idéal. Et toute intersection d'idéaux de A est un idéal de A. Un idéal est dit **irréductible** s'il ne peut s'écrire comme intersection de deux idéaux de A.*

Définition 2.4.10 *Comme pour un sous-espace vectoriel, on définit la somme $K = I + J$ de deux idéaux I et J d'un anneau commutatif A comme étant l'ensemble des éléments z de A s'écrivant $x + y$ où x est élément de I et y élément de J.*

Définition 2.4.11 *Dans un anneau A, le **produit** de deux idéaux I et J est l'ensemble des sommes finies d'éléments de la forme $x_i y_i$ où x_i est dans I et y_i dans J.*

On vérifie facilement que l'ensemble IJ ainsi défini est un idéal de A.

Exercice 63 (*non corrigé*) Vérifier la chaîne d'inclusion : $IJ \subset (I \cap J) \subset (I \cup J) \subset I + J$.

Exercice 64 (*non corrigé*)

1. Justifier que l'intersection de deux idéaux est un idéal.
2. Montrer par un exemple que la réunion de deux idéaux n'en est pas toujours un !
3. Montrer que la somme de deux idéaux contient leur intersection. Étudier l'inclusion inverse.
4. Dans $\mathbb{Z}$, quel est l'idéal défini par $18\mathbb{Z} + 24\mathbb{Z}, 2\mathbb{Z} + 4\mathbb{Z}, 2\mathbb{Z} + 3\mathbb{Z}$? (mot clé : pgcd)

Exercice 65 *Le théorème chinois dans un anneau commutatif*
Soient I et J deux idéaux d'un anneau commutatif A tels que $I + J = A$.

1. Établir que $I \cap J = IJ$.

2. On considère l'application $\varphi : A \to A/I \times A/J$ qui à $x \in A$ associe le couple de ses classes modulo I et J. Montrer que φ est un morphisme d'anneaux et déterminer son noyau.
3. Montrer que les anneaux A/IJ et $A/I \times A/J$ sont isomorphes.

Correction :

1. Soient $x \in I$ et $y \in J$. Puisque I et J sont des idéaux, on a $xy \in I$ et $xy \in J$, d'où $xy \in I \cap J$. Puisque IJ est l'idéal engendré par les produits xy, $x \in I$ et $y \in J$, et puisque $I \cap J$ est un idéal, on a $IJ \subset (I \cap J)$.
   Réciproquement, puisque $I + J = A$, il existe $u \in I$ et $v \in J$ tels que $u + v = 1$ (élément neutre de A pour la seconde loi). Soit $x \in I \cap J$, on a alors $x = xu + xv \in IJ$ car $x \in J$, $u \in I$ et $x \in I$, $v \in J$. Donc $(I \cap J) \subset IJ$. Ainsi $I \cap J = IJ$.
2. Soient π_I et π_J les surjections canoniques de A sur A/I et A/J respectivement. Ce sont des morphismes d'anneaux et $\forall x \in A$,
$$\varphi(x) = (\pi_I(x), \pi_J(x)).$$
   On a $\varphi(1_A) = (\pi_I(1_A), \pi_J(1_A)) = (1_{A/I}, 1_{A/J}) = 1_{A/I \times A/J}$.
   Soient $x, y \in A$, on a
$$\varphi(x+y) = (\pi_I(x+y), \pi_J(x+y)) = (\pi_I(x) + \pi_I(y), \pi_J(x) + \pi_J(y)) = (\pi_I(x), \pi_J(x)) + (\pi_I(y), \pi_J(y)) = \varphi(x) + \varphi(y)$$
$$\varphi(xy) = (\pi_I(xy), \pi_J(xy)) = (\pi_I(x)\pi_I(y), \pi_J(x)\pi_J(y)) = (\pi_I(x), \pi_J(x))(\pi_I(y), \pi_J(y)) = \varphi(x)\varphi(y)$$
   Donc φ est un morphisme d'anneaux.
   Soit $x \in A$, on a
$$x \in Ker(\varphi) \Leftrightarrow \varphi(x) = 0 \Leftrightarrow (\pi_I(x), \pi_J(x)) = 0 \Leftrightarrow \begin{cases} \pi_I(x) = 0 \\ \pi_J(x) = 0 \end{cases} \Leftrightarrow \begin{cases} x \in I \\ x \in J \end{cases} \Leftrightarrow x \in I \cap J \Leftrightarrow x \in IJ.$$
   Ainsi le noyau de φ est l'idéal IJ.
3. Puisque $Ker(\varphi) = IJ$, φ induit par passage au quotient un morphisme injectif d'anneaux $\overline{\varphi} : A/IJ \to A/I \times A/J$ qui à $x \in A/IJ$ associe $(\pi_I(x'), \pi_J(x'))$ où x' est un représentant de x dans A. De plus $Im(\overline{\varphi}) = Im(\varphi)$, donc pour montrer que $\overline{\varphi}$ est surjectif, il suffit de montrer que φ est surjectif. Soit $(x, y) \in A/I \times A/J$. Soient x', $y' \in A$ tels que $x = \pi_I(x')$ et $y = \pi_J(y')$. Soient $u \in I$ et $v \in J$, on a
$$\varphi(x'v + y'u) = (\pi_I(x'v + y'u), \pi_J(x'v + y'u)) = (\pi_I(x')\pi_I(v) + \pi_I(y')\pi_I(u), \pi_J(x')\pi_J(v) + \pi_J(y')\pi_J(u)) = (\pi_I(x'), \pi_J(y')) = (x, y)$$
   car $\pi_I(u) = 0$ ($u \in I$), $\pi_J(v) = 0$ ($v \in J$), $\pi_I(v) = 1$ et $\pi_J(v) = 1$ ($u + v = 1$). Ainsi φ est surjectif.
   En conclusion φ est un isomorphisme d'anneaux et les anneaux A/IJ et $A/I \times A/J$ sont isomorphes.

Exercice 66 (*Théoème des restes chinois)* Soient deux nombres entiers p et q premiers entre eux.

1. Montrer que $\mathbb{Z}/pq\mathbb{Z}$ est isomorphe au produit $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.
2. Un général chinois est parti pour une bataille avec 386 soldats. À la fin du combat, il souhaite compter ses troupes. Il leur ordonne de se mettre en rang de p soldats et il note le nombre de soldats formant la dernière rangée incomplète. Puis il procède de même mais en les faisant se mettre en rang de q soldats. Quelles valeurs de p et q doit-il prendre ?
   Expliquer comment il s'y prend finalement pour compter précisement ses soldats.
3. Que peut-on dire si p n'est pas premier avec q ?

Correction : On rappelle que si p et q sont premiers entre-eux, $ppcm(p, q) = pq = n$ et $pgcd(p, q) = 1$.

1. On considère l'application
$$\begin{array}{rcl} \varphi : \mathbb{Z}/pq\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ \alpha & \mapsto & (\alpha[p], \alpha[q]) \end{array}$$

où $\alpha[r]$ est le reste de la division euclidienne de α par r. Par exemple, si $p = 2$ et $q = 3$, $\varphi(15) = (1, 0)$. Cette application est un isomorphisme de groupes (voir exercice précédent). On remarquera que les deux ensembles $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ ont le même nombre d'éléments. On le constate en considérant par exemple $p = 2$ et $q = 3$: $\mathbb{Z}/(2 \times 3)\mathbb{Z} = \mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{5}\}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}\} \times \{\overline{0}, \overline{1}, \overline{2}\}$.

2. D'après les données, si x désigne le nombre de soldats vivants à la fin du combat, on a :
   - $x \equiv p_1[p] \Leftrightarrow \exists k \in \mathbb{Z}, x = kp + p_1$ où k et p_1 désignent respectivement le nombre de rangées de p soldats et le nombre de soldats formant la dernière rangée incomplète,
   - $x \equiv q_1[q] \Leftrightarrow \exists k' \in \mathbb{Z}, x = k'q + q_1$ où k' et q_1 désignent respectivement le nombre de rangées de q soldats et le nombre de soldats formant la dernière rangée incomplète.

   On a alors $\varphi(x) = (p_1, q_1)$. φ étant un isomorphisme, on est assuré de l'existence et de l'unicité de la solution recherchée pour p et q donnés. p et q sont premiers entre-eux donc d'après le théorème de Bézout, on peut trouver $u, v \in \mathbb{Z}$ tels que $up+vq = 1$. Ainsi, $x = upx+vqx = up(q_1+k'q)+vq(p_1+kp) = upq_1 + vqp_1 + (upk'q + vqkp) = upq_1 + vqp_1 + Kn$ avec $K = uk' + vk \in \mathbb{Z}$. Modulo $n = pq$, une solution du problème est donnée par $x = upq_1 + vqp_1$.
3. Si p et q ne sont pas premiers entre-eux, le morphisme φ n'est qu'injectif. Il existe une solution au problème initial si et seulement si les données sont dans l'image, c'est-à-dire si et seulement si $p_1 \equiv q_1[pgcd(p, q)]$ (ou ssi $pgcd(p, q)$ divise $p_1 - q_1$).

2.5 Les Corps

C'est Richard Dedekind qui définit pour la première fois la structure de corps (Körper en allemand) et c'est la raison pour laquelle un corps quelconque est souvent nommé K ou $\mathbb{K}$. La structure de corps s'insère dans une hiérarchie comprenant le monoïde, le groupe, l'anneau, et donne lieu à la définition de l'espace vectoriel, et de l'algèbre.

De manière informelle, un corps est un ensemble dans lequel il est possible d'effectuer des additions, des soustractions, des multiplications et des divisions.

Définition 2.5.1 *Un anneau dans lequel tout élément non nul admet un symétrique pour la multiplication (souvent appelé inverse) est un* ***corps****. En particulier, un corps est un anneau intègre. Si la multiplication (seconde loi) est commutative, le corps est dit commutatif.*

Un corps est donc un ensemble $\mathbb{K}$ muni de deux lois internes notées en général $+$ et $\times$ vérifiant
- $(\mathbb{K}, +)$ forme un groupe commutatif dont l'élément neutre est noté 0,
- $(\mathbb{K}\backslash\{0\}, \times)$ forme un groupe multiplicatif,
- la multiplication est distributive pour l'addition (à gauche comme à droite) c'est-à-dire que
$$\forall a, b, c \in \mathbb{K},\ a \times (b + c) = a \times b + a \times c \text{ et } (b + c) \times a = b \times a + c \times a$$

On parle alors du corps $(\mathbb{K}, +, \times)$.

Définition 2.5.2 *Un* ***sous-corps*** *d'un corps $\mathbb{K}$ est un sous-anneau $\mathbb{K}'$ de $\mathbb{K}$ tel que pour tout x de $\mathbb{K}'$, son inverse soit élément de $\mathbb{K}'$. On dit inversement que $\mathbb{K}$ est un* ***sur-corps*** *de $\mathbb{K}'$.*

Exemple 2.5.1
- $\mathbb{R}$ et $\mathbb{C}$ munis de leurs opérations usuelles sont des corps commutatifs.
- $\mathbb{C}$ est un sur-corps de $\mathbb{R}$.
- $(\mathbb{Q}, +, x)$ est un corps commutatif, sous-corps de $(\mathbb{R}, +, x)$
- Le corps H de quaternions n'est pas commutatif (corps gauche).
- Les nombres constructibles constituent un sous-corps de $\mathbb{R}$.
- Si p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo p est un corps fini (ayant un nombre fini d'éléments).

- $(\mathbb{Z}, +, \times)$ est un anneau commutatif intègre mais ce n'est pas un corps : les seuls éléments inversibles (ayant un inverse) sont 1 et - 1.
- $(\mathcal{M}_2(\mathbb{R}), +, \times)$ n'est pas un corps (voir ci-dessus). La division, on le sait dans le calcul élémentaire, n'est autre que la multiplication par l'inverse : dans le cas des matrices, on ne parle pas de diviseur mais d'inverse. L'inverse (s'il existe) d'une matrice carrée A est une matrice notée A^{-1} vérifiant $A^{-1} \times A = A \times A^{-1} = I$, où I est la matrice unité.
- Soit D l'ensemble des nombres décimaux (l'ensemble des nombres admettant un représentant de la forme $a \times 10^n$ avec $(a, n) \in \mathbb{Z}^2$. Par exemple $3/5$, $-7/4$ et $1,237$ sont décimaux. $(D, +, \times)$ est un anneau intègre, sous-anneau de $(\mathbb{Q}, +, \times)$. Ce n'est pas un corps, 3 par exemple est décimal mais pas son inverse $1/3$.

Remarque 2.5.1 L'ensemble $(\mathbb{Z}, +\times)$ n'est pas un corps car la plupart des éléments de $\mathbb{Z}^\star$ ne sont pas inversibles : par exemple, il n'existe pas d'entier relatif n tel que $2n = 1$ donc 2 n'est pas inversible.

Proposition 2.5.1 *Les seuls idéaux d'un corps sont l'idéal nul et le corps tout entier. Réciproquement si A est un anneau n'ayant comme seuls idéaux que l'idéal nul et lui même alors A est un corps.*

Preuve :
- Supposons que $\mathbb{K}$ est un corps. Soit I un idéal non nul de A. Soit donc x un élément non nul de I. x est, par définition d'un corps, inversible dans $\mathbb{K}$. Soit x^{-1} l'inverse de x dans $\mathbb{K}$. $x^{-1}x$ est, par définition d'un idéal, élément de I. Mais $x^{-1}x$ est égal à l'élément unité de $\mathbb{K}$. Donc $1 \in I$ et $I = \mathbb{K}$.
- Réciproquement, supposons maintenant que les seuls idéaux de l'anneau A sont l'idéal nul et A tout entier. Il nous suffit de montrer que tout les éléments non nuls de A sont inversibles. Soit $x \neq 0$ un élément de A. Soit (x) l'idéal engendré par x. Comme x n'est pas nul, cet idéal n'est pas nul non plus. Il est alors égal à A tout entier. L'unité de A est donc élément de (x). Ceci signifie qu'il existe y dans A tel que $xy = 1$. x est donc inversible d'inverse y. ■

Définition 2.5.3 *Un **corps fini** est un corps (commutatif) dont le cardinal est fini. À un isomorphisme près, un corps fini est entièrement déterminé par son cardinal qui est toujours de la forme p^n, une puissance d'un nombre premier. Ce nombre premier n'est autre que sa **caractéristique** et le corps se présente comme l'unique extension simple du corps premier $\mathbb{Z}/p\mathbb{Z}$ de dimension n.*

Théorème 2.5.1 *Théorème de Wedderburn (Joseph WEDDERBURN 1882-1948) Tout corps fini est commutatif.*

Preuve : http ://www.math.mcgill.ca/chenever/PDF/Wedderburn.pdf ■

Exercice 67 Soit A un anneau intègre de cardinal fini. Montrer que A est un corps.
Correction : Soit $a \in A$ non nul. L'application

$$\begin{array}{rccc} \mu_a : & A & \to & A \\ & x & \mapsto & ax \end{array}$$

est injective. En effet, puisque A est un anneau intègre et a est non nul, pour tous $x, y \in A$, on a $\mu_a(x) = \mu_a(y) \Rightarrow ax = ay \Rightarrow ax - ay = 0 \Rightarrow a(x - y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y$.
Et comme A est un ensemble fini, toute injection de A dans A est une bijection. Ainsi μ_a est bijective. Soit $b \in A$ l'antécédent de 1 par μ_a. Alors $ab = \mu_a(b) = 1$. Et puisque A est un anneau commutatif, on a $ba = 1$ et b est l'inverse de a. Ainsi A est un corps.

Exercice 68 Soit $S\mathbb{K}$ un sous-corps d'un corps commutatif $\mathbb{K}$. Soient $P, Q \in S\mathbb{K}[X]$, P irréductible.

On suppose que P et Q, considérés comme éléments de $\mathbb{K}[X]$, ont une racine commune. Montrer que P divise Q.
Correction : Soit D un *pgcd* de P et Q dans $S\mathbb{K}[X]$. L'algorithme d'Euclide est identique que l'on considère les polynômes P et Q dans $S\mathbb{K}[X]$ ou dans $\mathbb{K}[X]$, donc D est un *pgcd* de P et Q dans $\mathbb{K}[X]$. Puisque P et Q ont une racine commune dans $\mathbb{K}$, ils ne sont pas premiers entre eux et ainsi D est distinct de 1. Or P est irréductible dans $S\mathbb{K}[X]$, donc il existe $\lambda \in S\mathbb{K}\backslash\{0\}$ tel que $D = \lambda P$. Ainsi P divise Q.
Autre méthode : puisque P et Q ont une racine commune dans $\mathbb{K}$, il existe un idéal I de $\mathbb{K}[X]$ distinct de $\mathbb{K}[X]$ contenant P et Q. On pose $J = I/S\mathbb{K}[X]$, c'est un idéal de $S\mathbb{K}[X]$, distinct de $S\mathbb{K}[X]$ (sinon 1 appartiendrait à J, donc à I et alors I serait égal à $\mathbb{K}[X]$) et contenant P et Q. Puisque $S\mathbb{K}[X]$ est principal et P est irréductible, J est l'idéal engendré par P, donc P divise Q.

Chapitre 3

Algèbre et arithmétique

3.1 Introduction

3.2 La division euclidienne et ses conséquences

Théorème 3.2.1 *(division euclidienne)*
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}/\{0\}$. Alors il existe $q \in \mathbb{Z}$ et $r \in \{0, 1, \ldots, |b| - 1\}$ tels que

$$a = bq + r.$$

En outre, q et r sont uniques. q est le dividende, b le diviseur, q le quotient et r le reste dans la division de a par b.

Preuve :On considère l'ensemble E formé des entiers $a - pb$, où $p \in \mathbb{Z}$. Puisque b est non nul, l'ensemble E contient des nombres positifs. Donc l'intersection $E \cap \mathbb{N}$ est non vide. Elle admet donc un élément minimal. Appelons r cet élément et définissons q par l'égalité $a - qb = r$. Montrons que $r < |b|$. Soit ϵ le signe de b ($\epsilon = 1$ si $b > 0$ et $\epsilon = -1$ si $b < 0$). Si nous avions $r > |b|$, nous pourrions enlever ϵb des deux côtés de l'égalité $a - qb = r$ pour trouver un nombre $r - \epsilon b = a - (q + \epsilon)b$ qui appartiendrait encore à $E \cap \mathbb{N}$ mais qui serait strictement inférieur à r, ce qui est une contradiction. On a donc bien $r \in \{0, 1, \ldots, |b| - 1\}$.
Montrons l'unicité. Si nous avons $qb + r = a = q'b + r'$, alors $(q - q')b = r - r'$. Puisque r et r' sont positifs et strictement inférieurs à $|b|$, il s'ensuit que $|q - q'||b| = |r - r'| < |b|$. Comme $|b| \neq 0$, nous avons $|q - q'| < 1$. Or, $|q - q'|$ est un entier positif et donc $|q - q'| = 0$ et $q = q'$. Par conséquent, nous avons aussi $r = a - qb = a - q'b = r'$. ■

Exercice 69 (non corrigé) Le 04 septembre 2002 est un mercredi, quel jour de la semaine sera le 04 septembre 2045 ?

Exemple 3.2.1
- On a $15 = 2 \times 7 + 1$ ce qui est une division euclidienne.
- On a aussi $-15 = (-2) \times 7 + (-1)$ ce qui n'est pas une division euclidienne, car le reste d'une division euclidienne est positif, par définition.
- Par contre, $-15 = (-3) \times 7 + 6$ est bien une division euclidienne.

Proposition 3.2.1 *Tout sous-groupe H de $(\mathbb{Z}, +)$ est de la forme $H = n\mathbb{Z}$ pour un $n \in \mathbb{Z}$ unique au signe près.*

Preuve : Si $H = \{0\}$, alors $H = 0\mathbb{Z}$ et il n'y a rien à démontrer. Supposons donc que $H \neq \{0\}$. Alors l'ensemble des normes $|x| > 0$ d'éléments de H est non-vide. Soit $n \in H$ tel que $|n|$ est non nul et minimal. On peut affirmer que $H = n\mathbb{Z}$. En effet, puisque H est un sous-groupe qui contient n, il contient $n\mathbb{Z}$.

Réciproquement, soit $a \in H$ et soit $a = qn + r$ la division euclidienne de a par n (rappelons que $n \neq 0$). Si on avait $r \neq 0$, alors $r = a - qn$ serait un élément de H non nul et de norme strictement inférieure à celle de n. Donc nous avons $r = 0$ et $a = qn \in n\mathbb{Z}$.
Montrons l'unicité. En effet, si $n\mathbb{Z} = n'\mathbb{Z}$, nous avons $n = xn'$ pour un $x \in \mathbb{Z}$ et $n' = x'n$ pour un $x' \in \mathbb{Z}$. Donc, $n = xx'n$. Nous avons soit $n = 0$, et alors $n\mathbb{Z} = \{0\}$ et $n' = 0$, soit $n \neq 0$ et alors $1 = xx'$ et donc $x = \pm 1$ et $n' = \pm n$. ■

Remarque 3.2.1 Si H et H' sont deux sous-groupes de $(\mathbb{Z}, +)$, on pose $H + H' = \{x + x', x \in H \text{ et } x' \in H'\}$. On vérifie aussitôt que $H + H'$ est encore un sous-groupe de $(\mathbb{Z}, +)$. D'après le théorème, si a et b sont deux entiers, il existe un entier c unique au signe près tel que $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$. Nous allons voir que c est en fait le plus grand commun diviseur de a et b.

Définition 3.2.1 *Soient $a, b \in \mathbb{Z}$. On dit que a est divisible par b s'il existe $q \in \mathbb{Z}$ tel que $a = qb$. Dans ce cas, on dit aussi que a est multiple de b, que b divise a ou que b est diviseur de a. On écrit $a|b$.*

Exemple 3.2.2
- Le nombre 15 est divisible par 1, 3, 5, 15, -1, -3, -5 et -15.
- Le nombre 0 est divisible par tout entier. Par contre le nombre 1 n'est divisible que par 1 et -1. En effet, si on a $1 = qb$, alors $1/|b|$ est un entier non nul et ≤ 1. Donc $b = \pm 1$.
- Supposons $b \neq 0$. Alors la division euclidienne de a par b est bien définie et a est divisible par b ssi le reste de la division euclidienne de a par b s'annule.

Définition 3.2.2 *Soient $a, b \in \mathbb{Z}$ tels que $(a, b) \neq (0, 0)$. Alors le module d'un diviseur commun à a et b est borné par $\max(|a|, |b|)$ et il existe donc un **plus grand diviseur commun** à a et b. On le note PGCD(a,b). Les nombres a et b sont premiers entre eux si $PGCD(a, b) = 1$. Si $a = b = 0$, on pose $PGCD(a, b) = 0$.*

Théorème 3.2.2 *(Bézout) Soient $a, b \in \mathbb{Z}$. Alors*

$$a\mathbb{Z} + b\mathbb{Z} = PGCD(a, b)\mathbb{Z}.$$

En particulier, on a équivalence entre

1. *Les entiers a et b sont premiers entre eux.*
2. *On a $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.*
3. *L'équation $ax + by = 1$ admet une solution $(x, y) \in \mathbb{Z}^2$.*

Preuve : Supposons que $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$ avec c positif. Comme $a \in c\mathbb{Z}$ et $b \in c\mathbb{Z}$, le nombre c est un diviseur commun de a et b. Donc $c \leq \text{PGCD}(a, b)$. De l'autre côté, $\text{PGCD}(a, b)$ divise a et b et donc tout élément de $a\mathbb{Z} + b\mathbb{Z}$. En particulier, $\text{PGCD}(a, b)$ divise c. Il s'ensuit que $c = \text{PGCD}(a, b)$. Il est ainsi clair que 1. est équivalent à 2. Il est aussi clair que 1. implique 3. Réciproquement, si 3. est vérifié et $z \in \mathbb{Z}$, il suffit de multiplier l'équation $ax + by = 1$ par z pour conclure que $z = a(zx) + b(zy)$ appartient à $a\mathbb{Z} + b\mathbb{Z}$ et donc que $\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. ■

Exemple 3.2.3 L'équation $ax + by = 1$ est dite équation de Bézout. Si $(a, b) \neq (0, 0)$, elle admet toujours des solutions $(x, y) \in \mathbb{Q}^2$ mais pas nécessairement dans $\mathbb{Z}^2$. Il s'ensuit du théorème que tout diviseur commun c de a et b divise $\text{PGCD}(a, b)$ (car il divise $ax + by$ quels que soient x, $y \in \mathbb{Z}$).

Exercice 70 (non corrigé) Trouver u et v tels que $17u + 48v = 1$.

Lemme 3.2.1 *(Gauss)*
Soient a, b, $c \in \mathbb{Z}$. Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

Preuve : D'après le lemme de Bézout, il existe x, $y \in \mathbb{Z}$ tels que $ax + by = 1$. Nous multiplions cette égalité par c pour obtenir $acx + bcy = c$. Puique a divise acx et bcy, il doit diviser $axc + bcy = c$. ■

Définition 3.2.3 *Un **nombre premier** est un entier > 1 dont les seuls diviseurs positifs sont 1 et lui-même.*

Exemple 3.2.4
- Le nombre 1 n'est pas premier.
- Les nombres 2, 3, 5 ... sont premiers.
- Un nombre premier est un entier positif qui admet exactement deux diviseurs positifs.

Lemme 3.2.2 *(Euclide)*
Soit p un nombre premier et a, $b \in \mathbb{Z}$. Si p divise ab alors p divise a ou p divise b.

Preuve : Si p ne divise pas a, alors a et p sont premiers entre eux, car les seuls diviseurs de p sont 1 et lui-même. D'après le lemme de Gauss, p doit alors diviser b. De même, si p ne divise pas b, il doit diviser a.■

Exemple 3.2.5 L'affirmation de ce lemme est fausse si on omet l'hypothèse que p est premier. Par exemple le nombre 3×5 divise le produit $(2 \times 3) \times (5 \times 7)$ mais il ne divise ni 2×3 ni 5×7. Soient p et p_1,..., p_r des nombres premiers.

Montrons que si p divise $p_1 \dots p_r$, alors $p = p_i$ pour un i. Si $r = 1$, il n'y a rien à démontrer. Si $r > 1$, et que p divise le produit $p_1 \times (p_2 \dots p_r)$, alors d'après le lemme d'Euclide, p divise p_1 ou p divise $p_2 \dots p_r$. Dans le premier cas, nous avons $p = p_1$ et dans le second $p = p_i$ pour un $i \geq 2$, d'après l'hypothèse de récurrence.

Théorème 3.2.3 *(Décomposition en facteurs premiers)*
Soit $n \geq 1$ un entier et soit p_1, $p_2 \dots$ la liste des nombres premiers (exhaustive et sans répétitions). Alors il existe des entiers $m_i \in \mathbb{N}$ uniques et nuls sauf pour un nombre fini d'entre eux tels que

$$n = p_1^{m_1} p_2^{m_2} p_3^{m_3} \dots$$

Preuve : Montrons l'existence de l'écriture par un raisonnement récursif : Si $n = 1$, on pose $m_i = 0$ pour tous les i. Si $n > 1$ alors soit n est premier, soit $n = n'n''$ pour deux nombres strictement inférieurs à n. Dans le premier cas, il existe un nombre premier p_j dans la liste et un seul tel que $n = p_j$. On pose $m_i = 0$ pour $i \neq j$ et $m_j = 1$. Dans le second cas, l'hypothèse de récurrence nous donne les écritures

$$n' = p_1^{m'_1} p_2^{m'_2} \dots$$
$$n'' = p_1^{m''_1} p_2^{m''_2} \dots$$

En multipliant nous trouvons

$$n = p_1^{m'_1 + m''_1} p_2^{m'_2 + m''_2} \dots.$$

Montrons l'unicité de l'écriture. Supposons donc que

$$n = p_1^{m_1} p_2^{m_2} \dots = p_1^{m'_1} p_2^{m'_2} \dots$$

Montrons que $m_1 = m'_1$ (la démonstration pour les autres m_i est la même). Nous procédons par récurrence. Si $m_1 = 0$, alors p ne divise pas n (sinon il serait égal à l'un des p_i). Donc $m'_1 = 0$. Si $m_1 > 0$, alors p_1 divise n. D'après la remarque ci-dessus, p_1 doit apparaître dans l'écriture

$$p_1^{m'_1} p_2^{m'_2} \dots$$

Donc $m'_1 > 0$. En divisant par p_1 nous trouvons

$$p_1^{m_1-1} p_2^{m_2} \dots = p_1^{m'_1-1} p_2^{m'_2} \dots$$

et par l'hypothèse de récurrence, il s'ensuit que $m_1 - 1 = m'_1 - 1$. Donc $m_1 = m'_1$. ■

Remarque 3.2.2 Ce théorème a des conséquences étonnantes. Par exemple, d'après l'unicité, l'application

$$\begin{array}{rcl} \mathbb{N} \times \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \\ (m_1, m_2, m_3) & \mapsto & 2^{m_1} \times 3^{m_2} \times 5^{m_3} \end{array}$$

est injective. Donc le cardinal de $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ est inférieur à celui de $\mathbb{N}$. (Bien sûr, on sait par ailleurs que ces deux cardinaux sont égaux).

Remarque 3.2.3 Si nous avons

$$n = p_1^{m_1} p_2^{m_2} p_3^{m_3} \dots$$

comme dans le théorème, alors les diviseurs positifs de n sont exactement les nombres

$$n' = p_1^{m'_1} p_2^{m'_2} p_3^{m'_3} \dots$$

où $m'_i \leq m_i$ pour tout i. En effet, il est clair que ces nombres divisent n. Réciproquement supposons que $n = n'n''$ et que nous ayons les décompositions

$$\begin{array}{l} n' = p_1^{m'_1} p_2^{m'_2} \dots \\ n'' = p_1^{m''_1} p_2^{m''_2} \dots \end{array}$$

En multipliant n' par n'' nous trouvons

$$n = p_1^{m_1} p_2^{m_2} p_3^{m_3} \dots = p_1^{m'_1+m''_1} p_2^{m'_2+m''_2} p_3^{m'_3+m''_3} \dots$$

Par unicité, il s'ensuit que $m_i = m'_i + m''_i$ pour tout i. Donc on a bien $m_i \geq m'_i$. On en déduit que le nombre de diviseurs de n est égal à $(m_1 + 1)(m_2 + 1) \dots$ Supposons que nous ayons les décompositions

$$\begin{array}{l} n = p_1^{m_1} p_2^{m_2} p_3^{m_3} \dots \\ n' = p_1^{m'_1} p_2^{m'_2} p_3^{m'_3} \dots \end{array}$$

Alors il s'ensuit que

$$\begin{array}{l} \mathrm{PGCD}(n, n') = p_1^{\min(m_1, m'_1)} p_2^{\min(m_2, m'_2)} \dots \\ \mathrm{PPCM}(n, n') = p_1^{\max(m_1, m'_1)} p_2^{\max(m_2, m'_2)} \dots \end{array}$$

où $\mathrm{PPCM}(n, n')$ désigne le **plus petit commun multiple** de n et n'. On en déduit que

$$\boxed{n \times n' = \mathrm{PPCM}(n, n') \times PGCD(n, n')}.$$

3.3 Congruences

Définition 3.3.1 *Soient $n \geq 1$ un entier et $a, b \in \mathbb{Z}$. On dit que a est* ***congru à*** *b* ***modulo*** *n s'il existe un $k \in \mathbb{Z}$ tel que $a = b + kn$. On écrit alors*

$$a \equiv b(n) \text{ ou } a \equiv_n b \text{ ou } a = b \text{ mod } n.$$

Remarque 3.3.1 On a $a \equiv b(n)$ si et seulement si a et b ont le même reste dans la division euclidienne par n. En effet, si nous avons $a = qn + r$ et $b = q'n + r$, alors $a = b + (q - q')n$ et $a \equiv b(n)$. Réciproquement, si $a = qn + r$ et $b = q'n + r'$ et que $a = b + kn$, alors $a = b + kn = q'n + r' + kn = (q' + k)n + r' = qn + r$ et par l'unicité de la division euclidienne, il s'ensuit que $r = r'$ (et $q = q' + k$).

Exemple 3.3.1 Nous avons $6 \equiv -15(7)$ car $6 = -15 + 3 \times 7$. Notons que -15 a effectivement le même reste que 6 pour la division euclidienne par 7 car $-15 = (-3) \times 7 + 6$.

Exercice 71 (non corrigé) 1517 et 2428 sont-ils congrus modulo 7 ?

Lemme 3.3.1

1. *La relation $\equiv_n$ est une relation d'équivalence.*
2. *Si $a \equiv a'(n)$ et $b \equiv b'(n)$, alors $a + b \equiv a' + b'(n)$ et $ab \equiv a'b'(n)$. Dans ce cas, on a aussi $a^m \equiv a'^m(n)$ pour tout $m \in \mathbb{N}$.*
3. *Les nombres $0, 1, \ldots, n-1$ forment un système de représentants des classes par rapport à $\equiv_n$.*

Preuve :

1. La relation est réflexive car nous avons $a = a + 0 \times n$ pour tout $a \in \mathbb{Z}$. Elle est symétrique car si nous avons $a = b + kn$ alors nous avons $b = a + (-k)n$. Elle est transitive, car si nous avons $a = b + kn$ et $b = c + ln$, alors nous avons $a = (c + ln) + kn = c + (l + k)n$.
2. Supposons que $a = a' + kn$ et que $b = b' + ln$. Alors $a + b = a' + b' + (k + l)n$ et $ab = (a' + kn)(b' + ln) = a'b' + a'ln + knb' + klnn = a'b' + (a'l + kb' + kln)n$. La dernière affirmation s'ensuit par récurrence sur m.
3. Tout $a \in \mathbb{Z}$ est équivalent par $\equiv_n$ à un et un seul des nombres $0, 1, \ldots, n-1$. En effet, cette affirmation est une reformulation de l'existence et de l'unicité du reste dans la division euclidienne de a par n.

■

Définition 3.3.2 *On pose $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\equiv_n$. On note ${}^n\overline{a}$ ou $\overline{a}$ (ou même a) la classe de $a \in \mathbb{Z}$. Les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont donc les $\overline{a}$, $a \in \mathbb{Z}$. On munit $\mathbb{Z}/n\mathbb{Z}$ des deux lois*

$$\begin{array}{rcl} + : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ (\overline{a}, \overline{b}) & \mapsto & \overline{a} + \overline{b} = \overline{a+b} \\ . : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ (\overline{a}, \overline{b}) & \mapsto & \overline{a}.\overline{b} = \overline{a.b} \end{array}$$

Exemple 3.3.2 Grâce au lemme ci-dessus les deux lois sont bien définies. Par définition de la notion de "classe d'équivalence", nous avons ${}^n\overline{a} = {}^n\overline{b}$ si et seulement si $a \equiv b(n)$. Par conséquent, deux classes $\overline{a}$ et $\overline{b}$ sont égales ssi les restes de a et b par la division euclidienne par n sont égaux. D'après le lemme ci-dessus, les classes $\overline{0}$, $\overline{1}$,…,$\overline{n-1}$ sont distinctes deux à deux et toute classe est égale à une d'entre-elles. Ces classes constituent donc la liste (exhaustive et sans répétitions) des éléments de $\mathbb{Z}/n\mathbb{Z}$. En particulier, $\mathbb{Z}/n\mathbb{Z}$ est de cardinal n.

3.4 Critères de divisibilité

3.4.1 En base décimale

Soit $N = 1001001001001001001001001$. Le nombre N est-il premier ?
Non. Il est divisible par 3 car la somme de ses chiffres est divisible par 3. De façon générale, on sait qu'un nombre est divisible par 3 ssi la somme de ses chiffres l'est. De même pour 9 au lieu de 3. On sait aussi qu'un nombre est divisible par 11 ssi la somme alternée $c_0 - c_1 + c_2 - \dots$ de ses chiffres l'est (c_0 est le chiffre des unités, c_1 celui des dizaines,...). La divisibilité par 7, par contre, ne semble être reliée ni à la divisibilité par 7 de la somme ni à celle de la somme alternée de ses chiffres comme le montrent les exemples 7, 14, 21,... En fait, nous allons voir qu'un nombre est divisible par 7 si et seulement si c'est le cas pour le nombre

$$c_0 + 3c_1 + 2c_2 - c_3 - 3c_4 - 2c_5 + c_6 + 3c_7 + 2c_8 - c_9 - 3c_{10} - \dots$$

Par exemple, le nombre 100100100100 est divisible par 7. Plus généralement, tout nombre dont l'écriture décimale est 3-périodique et comporte un nombre de chiffres divisible par 6 est divisible par 7.

Ces faits trouvent leur explication à l'aide de deux outils suivants :

1. le calcul des congruences et
2. le calcul des restes de puissances.

Le lemme suivant élucide le rôle que joue le calcul des congruences.

Lemme 3.4.1 *Soit $n \geq 2$ un entier et a_i, $i \in \mathbb{N}$ une suite d'entiers telle que*

$$a_i \equiv 10^i(n) \text{ pour tout } i \in \mathbb{N}.$$

Soit $N \in \mathbb{N}$ et soient $c_0, c_1, \dots, c_s \in \{0, \dots, 9\}$ les chiffres de son écriture décimale (c_0 =unités,...). Alors nous avons $N \equiv a_0c_0 + a_1c_1 + a_2c_2 + \dots + a_sc_s(n)$. En particulier, N est divisible par n si et seulement si $a_0c_0 + a_1c_1 + \dots + a_sc_s$ est divisible par n.

Preuve : Par définition de l'écriture décimale, on a

$$N = c_0 + c_1 \times 10 + c_2 \times 10^2 + c_3 \times 10^3 + \dots + c_s \times 10^s.$$

Puisque $10^i \equiv a_i(n)$, les règles du calcul des congruences nous permettent de conclure que

$$N \equiv c_0a_0 + c_1a_1 + c_2a_2 + c_3a_3 + \dots + c_sa_s(n).$$

■

Exemple 3.4.1 Déduisons le critère de divisibilité par 7 que nous avons évoqué plus haut. Pour pouvoir appliquer le lemme, il nous faut calculer une suite d'entiers a_i tels que $a_i \equiv 10^i(7)$. La suite des a_i vérifie donc les congruences

$$a_0 \equiv 1(7)$$
$$a_{i+1} \equiv 10a_i(7) \equiv 3a_i(7)$$

(car $10 \equiv 3(7)$). Pour $a_0, \dots, a_6$, nous trouvons

$$1, 3, 2, -1, -3, -2, 1.$$

Donc $a_6 \equiv a_0(7)$ et par récurrence, on trouve que $a_i \equiv a_{i+6}(7)$ pour tout $i \in \mathbb{N}$. Pour la suite des a_i, on peut donc choisir la suite 6-périodique suivante

$$1, 3, 2, -1, -3, -2, 1, 3, 2, -1, -3, -2, 1, 3, 2, -1, -3, -2, \dots$$

D'aprs le lemme, il s'ensuit que N est divisible par 7 ssi c'est le cas pour le nombre

$$c_0 + 3c_1 + 2c_2 - c_3 - 3c_4 - 2c_5 + c_6 + 3c_7 + 2c_8 - c_9 - 3c_{10} - \dots$$

où les c_i sont les chiffres de l'écriture décimale de N (c_0 =unités, c_1 =dizaines,...).

3.4.2 Généralisation à d'autres systèmes de numération

Le fondement mathématique des systèmes de numération est le lemme suivant :

Lemme 3.4.2 *Soit $b \geq 2$ un entier. Pour tout entier $N \in \mathbb{N}$, il existe des entiers uniques $c_i \in \{0, \ldots, b-1\}$, $i \in \mathbb{N}$, nuls sauf pour un nombre fini d'entre eux, tels que*

$$N = c_0 + c_1 b + c_2 b^2 + \ldots c_i b^i + \ldots$$

Remarque 3.4.1 Dans la situation du lemme, si $N \neq 0$ et que c_s est le dernier coefficient non nul, nous écrivons

$$N = [c_s, c_{s-1}, \ldots, c_1, c_0]_b$$

et nous appelons l'expression à droite **l'écriture de N en base b**. Il nous arrivera d'omettre les crochets et les virgules comme dans l'exemple suivant :

$$1995_{10} = 11111001011_2 = 133023_8.$$

Dans les cas $b = 2, 8$ et 16, on parle respectivement des écritures binaire, octale et hexadécimale. Si b excède 10, les "chiffres" de 10 à b sont représentés par les premières lettres de l'alphabet. Par exemple, les chiffres du système hexadécimal sont $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$. Ainsi on a

$$1995_{10} = 7CB_{16}.$$

Preuve du lemme : On prouve d'abord l'existence par récurrence sur n. Pour $n = 0$ on pose $c_i = 0$ pour tout $i \in \mathbb{N}$. Supposons $n > 0$. Effectuons la division euclidienne de n par b

$$n = qb + r.$$

D'après l'hypothèse de récurrence, le nombre q s'écrit

$$q = c'_0 + c'_1 b + \ldots + c'_t b^t$$

et donc

$$n = r + c'_0 b + c'_1 b^2 + \ldots + c'_t b^{t+1}.$$

On pose donc $c_0 = r$ et $c_i = c'_{i-1}$ pour $i > 0$.
Montrons ensuite l'unicité. Si nous avons

$$n = c_0 + c_1 b + c_2 b^2 + \ldots = d_0 + d_1 b + d_2 b^2 + \ldots$$

alors $c_0 = d_0$ car les deux apparaissent comme le reste de la division euclidienne de n par b. Nous enlevons $c_0 = d_0$ des deux côtés et nous divisons par b pour obtenir

$$(n - c_0)/b = c_1 + c_2 b + \ldots = d_1 + d_2 b + \ldots.$$

L'unicité s'ensuit par récurrence sur n. ■

Lemme 3.4.3 *Soit $n \geq 2$ un entier et a_i, $i \in \mathbb{N}$, une suite d'entiers tels que $b_i \equiv a_i(n)$. Soit $N \in \mathbb{N}$ et c_i, $i \in \mathbb{N}$, les chiffres de son écriture en base b (c_0 =unités,...). Alors on a*

$$N \equiv a_0 c_0 + a_1 c_1 + a_2 c_2 + \ldots (n)$$

En particulier, N est divisible par n si c'est le cas pour $a_0 c_0 + a_1 c_1 + a_2 c_2 + \ldots$.

Preuve : La démonstration est analogue à celle du cas $b = 10$. ■

Exemple 3.4.2

- Nous avons $8^i \equiv 1(7)$. Donc un nombre est divisible par 7 ssi la somme des chiffres de son écriture octale est divisible par 7.
- Nous avons $16^i \equiv (-1)^i(16)$. Donc un nombre est divisible par 17 ssi la somme alternée des chiffres de son écriture hexadécimale est divisible par 17.

3.5 Le lemme chinois en termes de congruence

Lemme 3.5.1 *(lemme chinois)*
Soient n_1, $n_2 \geq 2$ deux entiers premiers entre eux et $u_1n_1 + u_2n_2 = 1$ une équation de Bézout. Soient $a, a_1, a_2 \in \mathbb{Z}$ tels que $a \equiv a_1u_2n_2 + a_2u_1n_1(n_1n_2)$. Alors pour $x \in \mathbb{Z}$ on a l'équivalence

$$\left.\begin{array}{lll} x & \equiv a_1 & (n_1) \\ x & \equiv a_2 & (n_2) \end{array}\right\} \Leftrightarrow x \equiv a(n_1n_2).$$

Remarque 3.5.1 On peut réinterpréter le lemme en disant que la solution générale $x \in \mathbb{Z}$ du système de congruences à gauche est donnée par

$$x = a + kn_1n_2,\ k \in \mathbb{Z}.$$

Preuve du lemme : Vérifions d'abord que a est bien une solution du système de congruences. En effet, d'après l'hypothèse, nous avons

$$a = a_1u_2n_2 + a_2u_1n_1 + kn_1n_2$$

pour un $k \in \mathbb{Z}$ et donc

$$a \equiv a_1u_2n_2 \equiv a_1(u_2n_2 + u_1n_1) \equiv a_1(n_1)$$

et de même

$$a \equiv a_2u_1n_1 \equiv a_2(u_1n_1 + u_2n_2) \equiv a_2(n_2).$$

Montrons maintenant l'équivalence. Supposons que $x \equiv a(n_1n_2)$. Alors $x = a + kn_1n_2$ pour un $k \in \mathbb{Z}$ et donc $x \equiv a \equiv a_1(n_1)$ et $x \equiv a \equiv a_2(n_2)$. Réciproquement, supposons que x vérifie $x \equiv a_1(n_1)$ et $x \equiv a_2(n_2)$. Alors nous avons $(x - a) \equiv 0(n_1)$ et $(x - a) \equiv 0(n_2)$. Donc $x - a$ est divisible par n_1 et par n_2. Puisque les deux sont premiers entre eux, il s'ensuit (lemme de Gauss) que $x - a$ est divisible par n_1n_2, c'est-à-dire que $x \equiv a(n_1n_2)$. ■

Exemple 3.5.1 Considérons le système

$$\left\{\begin{array}{lll} x & \equiv 1 & (17) \\ x & \equiv 2 & (28) \\ x & \equiv 3 & (31) \end{array}\right.$$

Nous avons l'équation de Bézout $5 \times 17 - 3 \times 28 = 1$. Le système formé des deux premières équations est donc équivalent à la congruence $x \equiv a(17 \times 28)$ où $a = 1 \times (-3 \times 28) + 2 \times (5 \times 17) = 86$. Le système des trois équations se réduit donc à

$$\left\{\begin{array}{lll} x & \equiv 86 & (476) \\ x & \equiv 3 & (31) \end{array}\right.$$

Nous avons l'équation de Bézout $(-14) \times 476 + 215 \times 31 = 1$. Donc le système est équivalent à la congruence $x \equiv b\ (476 \times 31)$ où $b = 86 \times (215 \times 31) + 3 \times (-14 \times 476) = 553198$. Si nous réduisons b modulo $476 \times 31 = 14756$, nous trouvons que le système des trois équations est équivalent à la congruence

$$x \equiv 7226\ (14756).$$

On vérifiera que 7226 donne les restes 1, 2 et 3 dans la division par 17, 28 et 31.

3.6 Systèmes de congruence

Soient r et $n_1, \ldots, n_r$ des entiers ≥ 2 et $a_1, \ldots, a_r$ des entiers quelconques. Considérons le système

$$\begin{cases} x & \equiv a_1 \quad (n_1) \\ x & \equiv a_2 \quad (n_2) \\ & \cdots \\ x & \equiv a_r \quad (n_r) \end{cases}$$

Supposons que $x = a$ et $x = a'$ sont deux solutions. Alors la différence $a - a'$ est divisible par tous les n_i et donc par leur plus petit commun multiple $n = \text{PPCM}(n_1, \ldots, n_r)$. Donc s'il existe une solution, sa classe modulo n est unique. Il peut ne pas exister de solution comme le montre l'exemple du système

$$\begin{cases} x & \equiv 1 \quad (6) \\ x & \equiv 2 \quad (8) \end{cases}$$

ou encore celui du système

$$\begin{cases} x & \equiv 1 \quad (2) \\ x & \equiv 0 \quad (2) \end{cases}$$

Notons que nous n'avons pas exclu ce genre de contradiction banale. L'application systématique du lemme chinois nous permettra de réduire tout système de congruences soit à un système contradictoire soit à une seule congruence modulo le plus petit commun multiple des modules. Nous ne développons pas ici la méthode dans le cas général mais nous limitons à la décrire dans un exemple simple. Considérons le système

$$\begin{cases} x & \equiv 3 \quad (18) \\ x & \equiv c \quad (12) \end{cases}$$

Il s'agit de déterminer tous les entiers c pour lesquels le sytème admet des solutions et de calculer les solutions dans ce cas. Constatons tout d'abord que les nombres 18 et 12 ne sont pas premiers entre eux de façon que le lemme chinois ne s'applique pas immédiatement. Pour résoudre le problème, nous allons dans une première étape augmenter le nombre d'équations pour obtenir des modules qui sont des puissances de nombres premiers. Nous avons ainsi $18 = 2 \times 3^2$ et d'après le lemme chinois la première congruence est équivalente au système

$$\begin{cases} x & \equiv 1 \quad (2) \\ x & \equiv 3 \quad (9) \end{cases}$$

De même, puisque nous avons $12 = 3 \times 4$, la seconde congruence est équivalente au système

$$\begin{cases} x & \equiv c \quad (3) \\ x & \equiv c \quad (4) \end{cases}$$

Nous avons ainsi trouvé un système de quatre congruences qui est équivalent au système de départ. Nous le réécrivons dans un ordre où les puissances de chaque nombre premier sont regroupées ensemble et les puissances les plus élevées apparaissent en premier lieu :

$$\begin{cases} x & \equiv c \quad (4) \quad (3.5.1) \\ x & \equiv 1 \quad (2) \quad (3.5.2) \\ x & \equiv 3 \quad (9) \quad (3.5.3) \\ x & \equiv c \quad (3) \quad (3.5.4) \end{cases}$$

Rappelons-nous que si nous avons $a \equiv b(n)$ alors nous avons aussi $a \equiv b(d)$ pour tout diviseur d de n (en effet, si $n = qd$ et $a = b + kn$ alors $a = b + (kq)d$). L'équation (3.5.1) implique donc que $x \equiv c(2)$ de façon que les équations (3.5.1) et (3.5.2) sont contradictoires sauf si $c \equiv 1(2)$. De même, les équations (3.5.3) et (3.5.4) sont contradictoires sauf si $c \equiv 0(3)$. Nous avons donc les conditions

$$\begin{cases} c & \equiv 1 \quad (2) \\ c & \equiv 0 \quad (3) \end{cases}$$

qui sont nécessaires pour qu'une résolution existe. Réciproquement, ces conditions sont aussi suffisantes car si elles sont vérifiées, la congruence (3.5.2) est une conséquence de (3.5.1), et (3.5.4) est une conséquence de (3.5.3) de façon que le système tout entier est équivalent à un système de deux congruences

$$\begin{cases} x & \equiv c \quad (4) \\ x & \equiv 3 \quad (9) \end{cases}$$

Nous avons l'équation de Bézout $-2 \times 4 + 9 = 1$. Donc, d'après le lemme chinois, ce système est équivalent à la congruence $x \equiv c \times 9 + 3 \times (-8)(36)$ ou encore $x \equiv 3c + 12(36)$. En conclusion, le système de départ admet une solution si et seulement si $c \equiv 3(6)$ et dans ce cas l'ensemble des solutions est l'ensemble des entiers x tels que $x \equiv 3c + 12(36)$.

3.7 Classes de congruence inversibles

Définition 3.7.1 *Soit $n \geq 2$ un entier. Une classe de congruence $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est **inversible** s'il existe une classe $\overline{b}$ telle que $\overline{a}.\overline{b} = \overline{1}$. On note $(\mathbb{Z}/n\mathbb{Z})^\star$ l'ensemble des classes inversibles.*

Lemme 3.7.1 *Muni de la multiplication naturelle, l'ensemble des classes inversibles est un groupe d'élément neutre $\overline{1}$.*

Preuve : Il s'agit d'abord de vérifier que la loi de multiplication est bien définie, c'est-à-dire que le produit de deux classes inversibles est encore inversible. En effet, si $\overline{a}\overline{b} = \overline{1}$ et $\overline{a'b'} = \overline{1}$, alors $(\overline{aa'})(\overline{b'b}) = \overline{1}$. La loi est associative car la multiplication de $\mathbb{Z}/n\mathbb{Z}$ est associative. Elle admet l'élément 1 pour élément neutre. Finalement, par définition, tout élément de $(\mathbb{Z}/n\mathbb{Z})^\star$ admet un inverse. ■

Remarque 3.7.1 Le lemme implique que si la classe $\overline{a}$ est inversible, alors la classe $\overline{b}$ telle que $\overline{a}\overline{b} = \overline{1}$ est unique. On l'appelle la classe inverse de $\overline{a}$.

Lemme 3.7.2 *Une classe $\overline{a}$ est inversible ssi a et n sont premiers entre eux.*

Preuve : En effet, la classe $\overline{a}$ est inversible, ssi l'équation $ab = 1 + kn$ admet des solutions $b, k \in \mathbb{Z}$. Or cette équation est une variante de l'équation de Bézout $ab + (-n)k = 1$ aux inconnues b, k. L'affirmation en résulte. ■

Lemme 3.7.3 *Supposons que la classe $\overline{x}$ est inversible. Alors la congruence $a \equiv b(n)$ est équivalente à $ax \equiv bx(n)$.*

Preuve : Supposons que $\overline{xy} = 1$. Alors $xy \equiv 1(n)$ et donc la congruence $axy \equiv bxy(n)$ implique $a \equiv b(n)$. ■

Remarque 3.7.2 L'affirmation du lemme est fausse si la classe $\overline{x}$ n'est pas inversible.

3.8 Anneaux, groupes et lemmes chinois

Lemme 3.8.1 *Soient $(A_1, +, \cdot)$ et $(A_2, +, \cdot)$ deux anneaux. L'ensemble $A_1 \times A_2$ muni des lois définies par*

$$(a_1, a_2) + (a'_1, a'_2) = (a_1 + a'_1, a_2 + a'_2)$$
$$(a_1, a_2) \cdot (a'_1, a'_2) = (a_1 a'_1, a_2 a'_2)$$

*est un anneau appelé l'**anneau produit** de A_1 par A_2. L'élément neutre pour l'addition de $A_1 \times A_2$ est le couple $(0,0)$ et celui pour la multiplication le couple $(1,1)$.*

Remarque 3.8.1 En appliquant plusieurs fois ce résultat nous obtenons un grand nombre de nouveaux exemples d'anneaux. Par exemple, tous les anneaux suivants sont de cardinal 24

$$\mathbb{Z}/24\mathbb{Z}\ ,\ \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}\ ,\ \mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\ ,\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}.$$

Nous allons voir que certains de ces anneaux sont "isomorphes", c'est-à-dire qu'ils ne se distinguent pas de façon essentielle.

Preuve du lemme : Il s'agit de vérifier les trois groupes d'axiomes pour les lois définies sur $A_1 \times A_2$. À titre d'exemple, vérifions que la multiplication est associative. En effet, en utilisant la définition de la multiplication sur $A_1 \times A_2$ et l'associativité de la multiplication dans A_1 et A_2, nous avons

$$((a_1,a_2)(a_1',a_2'))(a_1'',a_2'') = (a_1a_1',a_2a_2')(a_1'',a_2'') = ((a_1a_1')a_1'',(a_2a_2')a_2'') = (a_1(a_1'a_1''),a_2(a_2'a_2'')) = (a_1,a_2)(a_1'a_1'',a_2'a_2'') = (a_1,a_2)((a_1',a_2')(a_1'',a_2'')).$$

On démontre facilement les autres propriétés. ■

Lemme 3.8.2 *Soient $(G_1,\star)$ et $(G_2,\star)$ deux groupes. L'ensemble $G_1 \times G_2$ muni de la loi*

$$(g_1,g_2)\star(g_1',g_2') = (g_1\star g_1', g_2\star g_2')$$

est un groupe d'élément neutre le couple (e,e).

Preuve : La démonstration est analogue à celle du lemme précédent. ■

Lemme 3.8.3 *Soient $(A_1,+,\cdot)$ et $(A_2,+,\cdot)$ deux anneaux. Alors nous avons l'égalité*

$$(A_1\times A_2)^\star = A_1^\star \times A_2^\star$$

En outre la loi de groupe sur $(A_1\times A_2)^\star$ est celle du groupe produit $A_1^\star \times A_2^\star$

Preuve : Soit (a_1,a_2) un couple d'éléments inversibles. Soient a_1' et a_2' les inverses respectifs de a_1 et a_2. Alors nous avons $(a_1',a_2')(a_1,a_2) = (1,1) = (a_1,a_2)(a_1',a_2')$ ce qui signifie que (a_1,a_2) est inversible dans $A_1\times A_2$ d'inverse (a_1',a_2'). Ainsi l'ensemble $A_1^\star \times A_2^\star$ est inclus dans $(A_1\times A_2)^\star$. Réciproquement, soit (a_1,a_2) un élément inversible de $A_1\times A_2$ et soit (a_1',a_2') son inverse. Alors on vérifie aussitôt que a_1' est l'inverse de a_1 dans A_1 et que a_2' est l'inverse de a_2 dans A_2. La dernière affirmation est une conséquence immédiate des définitions. ■

Définition 3.8.1 *Soient $(A,+,)$ et $(B,+,)$ deux anneaux. Une application $f: A\to B$ est un **homomorphisme d'anneaux** si elle vérifie*

$$f(a+a') = f(a)+f(a')$$
$$f(a.a') = f(a).f(a')$$
$$f(1_A) = 1_B$$

*quels que soient $a,a'\in A$. C'est un **isomorphisme d'anneaux** si en plus elle est bijective. Les anneaux A et B sont isomorphes s'il existe un isomorphisme de A vers B.*

Exemple 3.8.1 Soient A_1 et A_2 deux anneaux. Considérons l'application

$$\begin{array}{rcl} f : A_1 \times A_2 & \to & A_2 \times A_1 \\ (a_1, a_2) & \mapsto & (a_2, a_2). \end{array}$$

Alors on vérifie que f est un isomorphisme.

Lemme 3.8.4 *Soient A et B deux anneaux et $f : A \to B$ un isomorphisme. Soit $g : B \to A$ l'application réciproque de f. Alors g est un homomorphisme et même un isomorphisme.*

Preuve : En effet, soient b, b' des éléments de B. Pour vérifier qu'on a égalité entre $g(bb')$ et $g(b)g(b')$ il suffit de voir que les images par f de ces deux éléments coïncident. Or nous avons

$$f(g(bb')) = bb' = f(g(b))f(g(b')) = f(g(b)g(b')).$$

De même on vérifie que $g(b+b') = g(b) + g(b')$. Finalement, l'égalité $f(1_A) = 1_B$ entraîne que $1_A = g(1_B)$.■

Définition 3.8.2 *Soient G et H deux groupes. Une application $f : G \to H$ est un homomorphisme de groupes si elle vérifie*

$$f(g_1 \star g_2) = f(g_1) \star f(g_2)$$

quels que soient $g_1, g_2 \in G$. C'est un isomorphisme si en plus elle est bijective. Les groupes G et H sont isomorphes s'il existe un isomorphisme de G vers H.

Exemple 3.8.2 On peut s'étonner de ne pas trouver l'axiome $f(e_G) = e_H$ dans cette définition. Or cet axiome est une conséquence de la définition. En effet, nous avons

$$f(e_G) = f(e_G \times e_G) = f(e_G) \times f(e_G).$$

Si nous multiplions cette égalité des deux côtés à gauche par l'inverse de $f(e_G)$ dans H, nous trouvons $e_H = f(e_G)$. Notons que cette démonstration utilise l'existence des inverses et qu'elle n'a donc pas d'analogue pour les lois de multiplication des anneaux. Si $f : G \to H$ est un isomorphisme de groupes et que $g : H \to G$ est l'application réciproque à f, alors g est un homomorphisme de groupes et même un isomorphisme. On adapte au cadre des groupes la démonstration donnée ci-dessus pour les anneaux.

Lemme 3.8.5 *Soient A et B deux anneaux et $f : A \to B$ un homomorphime d'anneaux. Alors nous avons $f(A^\star) \subset B^\star$ et l'application*

$$\begin{array}{rcl} f^\star : A^\star & \to & B^\star \\ a & \mapsto & f(a) \end{array}$$

est un homomorphisme de groupes. C'est un isomorphisme de groupes si f est un isomorphisme d'anneaux.

Preuve : Supposons que $a \in A$ est inversible d'inverse a'. Alors $f(a')$ est l'inverse de $f(a)$. En effet, nous avons

$$f(a)f(a') = f(aa') = f(1_A) = 1_B = f(a')f(a).$$

Ainsi, l'application f nous fournit bien une application entre les groupes des éléments inversibles

$$\begin{array}{rcl} f^\star : A^\star & \to & B^\star \\ a & \mapsto & f(a) \end{array}$$

Il est immédiat de constater que cette application est un homomorphisme de groupes. Supposons maintenant que f est un isomorphisme d'anneaux et soit $g : B \to A$ son application réciproque. Alors g est un homomorphisme et donc $g(B^\star)$ est contenu dans $A^\star$. Ceci montre que $a \in A$ est inversible si et seulement si $f(a)$ est inversible dans B. Donc dans ce cas $f^\star$ est bijective et c'est donc un isomorphisme de groupes. ■

Lemme 3.8.6 *(Lemme chinois en termes d'anneaux résiduels)*
Soient r et s deux entiers ≥ 2 et premiers entre eux. Alors l'application

$$\begin{array}{rcl} \phi : \mathbb{Z}/rs\mathbb{Z} & \to & \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z} \\ {}^{rs}\overline{a} & \mapsto & ({}^{r}\overline{a}, {}^{s}\overline{a}) \end{array}$$

est un isomorphisme d'anneaux.

Remarque 3.8.2 Ainsi nous voyons que tous les anneaux suivants sont isomorphes

$$\mathbb{Z}/24\mathbb{Z} \ , \ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, \ \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Nous verrons plus tard que ces anneaux ne sont pas isomorphes à $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Preuve du lemme : Vérifions que ϕ est un homomorphisme. En effet pour $a, b \in \mathbb{Z}$, nous avons

$$\phi({}^{rs}\overline{a} + {}^{rs}\,\overline{b}) = \phi({}^{rs}\overline{a+b}) = ({}^{r}\overline{a+b}, {}^{s}\,\overline{a+b}) = ({}^{r}\overline{a} + {}^{r}\,\overline{b}, {}^{s}\,\overline{a} + {}^{s}\,\overline{b}) = ({}^{r}\overline{a}, {}^{s}\,\overline{a}) + ({}^{r}\overline{b}, {}^{s}\,\overline{b}).$$

De même, on vérifie que ϕ est compatible pour la multiplication. Vérifions que ϕ est injective. En effet, si $\phi({}^{rs}\overline{a}) = \phi({}^{rs}\overline{b})$, alors nous avons $({}^{r}\overline{a}, {}^{s}\,\overline{a}) = ({}^{r}\overline{b}, {}^{s}\,\overline{b})$ et donc

$$\left\{ \begin{array}{rcl} a & \equiv b & (r) \\ a & \equiv b & (s) \end{array} \right.$$

Ainsi la différence $a - b$ est divisible par r et s et donc par le produit rs, puisque r et s sont premiers entre eux. Donc les classes ${}^{rs}\overline{a}$ et ${}^{rs}\overline{b}$ sont égales. Vérifions que ϕ est surjective. En effet, soient $a_1, a_2 \in \mathbb{Z}$. Alors nous cherchons $a \in \mathbb{Z}$ tel que $({}^{r}\overline{a}, {}^{s}\,\overline{a}) = ({}^{r}\overline{a_1}, {}^{s}\,\overline{a_2})$. De façon équivalente, nous cherchons $a \in \mathbb{Z}$ solution du système

$$\left\{ \begin{array}{rcl} a & \equiv a_1 & (r) \\ a & \equiv a_2 & (s) \end{array} \right.$$

Or, puisque r et s sont premiers entre eux, d'après le lemme chinois pour les congruences, il existe une solution $a \in \mathbb{Z}$. ■

Remarque 3.8.3 Les anneaux $\mathbb{Z}/rs\mathbb{Z}$ et $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$ ont même cardinal (égal à rs). Dans la démonstration, il aurait donc suffi de montrer soit la surjectivité soit l'injectivité de l'application ϕ pour conclure qu'elle est en fait bijective.

Corollaire 3.8.1 *Soient r, s des entier ≥ 2 et premiers entre eux. Alors l'application*

$$\begin{array}{rcl} \phi^\star : (\mathbb{Z}/rs\mathbb{Z})^\star & \to & (\mathbb{Z}/r\mathbb{Z})^\star \times (\mathbb{Z}/s\mathbb{Z})^\star \\ {}^{rs}\overline{a} & \mapsto & ({}^{r}\overline{a}, {}^{s}\,\overline{a}) \end{array}$$

est un isomorphisme de groupes. En particulier, elle est bijective et les deux groupes sont donc du même ordre.

Preuve : Le corollaire résulte du lemme précédent et du lemme (3.8.5). ■

Définition 3.8.3 *Soit n un entier ≥ 2. On définit $\phi(n)$ comme le cardinal du groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. La fonction ϕ est l'**indicatrice d'Euler**.*

Corollaire 3.8.2 *Si r et s sont deux entiers ≥ 2 et premiers entre eux on a*

$$\phi(rs) = \phi(r)\phi(s).$$

Preuve : Ceci résulte aussitôt de la définition de $\phi(rs)$ et du corollaire (3.8.1). ■

Remarque 3.8.4 Le corollaire précédent nous permet de calculer la valeur de $\phi(n)$ pour tout entier dont nous connaissons la décomposition en facteurs premiers. En effet, si nous avons

$$n = p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_r^{\epsilon_r}$$

alors en appliquant le corollaire plusieurs fois nous trouvons

$$\phi(n) = \phi(p_1^{\epsilon_1})\phi(p_2^{\epsilon_2}) \dots \phi(p_r^{\epsilon_r})$$

Mais on sait que pour un nombre premier p

$$\phi(p^k) = p^k - p^{k-1}.$$

Donc

$$\phi(n) = (p_1^{\epsilon_1} - p_1^{\epsilon_1 - 1})(p_2^{\epsilon_2} - p_2^{\epsilon_2 - 1}) \dots (p_r^{\epsilon_r} - p_r^{\epsilon_r - 1}).$$

Par exemple, $\phi(36) = \phi(4 \times 9) = \phi(4)\phi(9) = (4-2) \times (9-3) = 12$ et $\phi(1995) = \phi(3 \times 5 \times 7 \times 19) = 864$.

3.9 Notion d'ordre d'un élément d'un groupe

Lemme 3.9.1 *Soit $(G, \star)$ un groupe et g un élément de G. Alors il existe une application*

$$\exp_g : \mathbb{Z} \to G$$

et une seule telle que

$$\exp_g(1) = g$$
$$\exp_g(k+l) = \exp_g(k) \star \exp_g(l)$$

quels que soient $k, l \in \mathbb{Z}$.

Exemple 3.9.1 La seconde condition de la définition signifie que $\exp_g$ est un homomorphisme de groupes de $\mathbb{Z}$ vers G. Supposons que $(G, \cdot)$ est un groupe dont la loi est notée multiplicativement. Alors pour tout n entier positif, nous avons

$$\exp_g(n) = \underbrace{gg \dots g}_{n}$$
$$\exp_g(-n) = \exp_g(n)^{-1} = (g^{-1})^n.$$

Nous écrirons g^n pour $\exp_g(n)$ pour tout n entier. Supposons que $(A, +)$ est un groupe dont la loi est notée additivement. Alors pour tout n entier positif, nous avons

$$\exp_a(n) = \underbrace{a + a + \dots + a}_{n}$$
$$\exp_a(-n) = -\exp_a(n) = -na.$$

Nous écrirons na pour $\exp_a(n)$ pour tout n entier.

Corollaire 3.9.1

1. *Soit $(G,)$ un groupe dont la loi est notée multiplicativement et g un élément de G. Pour $k,l \in \mathbb{Z}$, on a les égalités suivantes*
$$\begin{gathered} g^1 = g \\ g^{k+l} = g^k \star g^l \\ g^0 = e_G \\ (g^k)^l = g^{kl} \end{gathered}$$
2. *Soient $(A,+)$ un groupe commutatif dont la loi est notée additivement et a un élément de A. Pour $k,l \in \mathbb{Z}$ on a les égalités suivantes*
$$\begin{gathered} 1a = a \\ (k+l)a = ka + la \\ 0a = 0_A \\ k(la) = (kl)a \end{gathered}$$

Preuve : Les deux parties sont des traductions dans la nouvelle notation de certaines propriétés de la fonction exp. Montrons-les à l'aide des notations de 1. Les deux premières égalités ne font que traduire dans la nouvelle notation les propriétés de la définition de $\exp_g$. La troisième propriété résulte du fait que $\exp_g$ est un homomorphisme. Pour la dernière propriété, fixons $k \in \mathbb{Z}$ et considérons l'application
$$\begin{array}{rccc} f : & \mathbb{Z} & \to & G \\ & l & \mapsto & g^{kl}. \end{array}$$
Nous avons clairement $f(1) = g^k$ et $f(l+l') = g^{k(l+l')} = g^{kl+kl'} = g^{kl} \star g^{kl'} = f(l) \star f(l')$. Par unicité de l'application $\exp_{g^k}$ nous pouvons conclure que $f(l) = \exp_{g^k}(l)$ pour tout $l \in \mathbb{Z}$ et donc que $f(l) = (g^k)^l$ pour tout $l \in \mathbb{Z}$. ■

Définition 3.9.1 *Soit $(G,\star)$ un groupe et g un élément de G. L'**ordre** de g est le plus petit entier $n \geq 1$ tel que $\exp_g(n) = e_G$ s'il existe un tel entier. Sinon, l'ordre de g est infini. On note $ord_G(g)$ ou $ord(g)$ l'ordre de g dans G.*

Exemple 3.9.2

- Supposons que $(G,\cdot)$ est un groupe dont la loi est notée multiplicativement et soit $g \in G$. Alors nous avons $ord_G(g) = \inf\{n \in \mathbb{N}/n \geq 1 \text{ et } g^n = e\}$.
- Supposons que $(A,+)$ est un groupe commutatif dont la loi est notée additivement et soit $a \in A$. Alors nous avons $ord_G(a) = \inf\{n \in \mathbb{N}/n \geq 1 \text{ et } na = 0_A\}$.
- Soit $(G,)$ un groupe dont la loi est notée multiplicativement (pour alléger les notations). Supposons que $g \in G$ est d'ordre fini n. Alors nous avons $g^{k+n} = g^k g^n = g^k e = g^k$ pour tout entier k et n est le plus petit entier ≥ 1 avec cette propriété. Autrement dit, la suite des puissances de g : $g^0 = e, g, g^2, \ldots, g^k, \ldots$ est périodique de période n. Nous avons aussi $g^{a+kn} = g^a g^{kn} = g^a (g^n)^k = g^a e^k = g^a$ pour tout entier $a \in \mathbb{Z}$ et tout entier $k \in \mathbb{Z}$. Autrement dit la valeur de g^a ne dépend que de la classe de congruence de a modulo n.

Lemme 3.9.2 *Soit n un entier ≥ 2 et soit $\overline{a}$ une classe modulo n considérée comme élément du groupe $(A,+) = (\mathbb{Z}/n\mathbb{Z},+)$. Alors*
$$ord_{\mathbb{Z}/n\mathbb{Z}}(\overline{a}) = \frac{PPCM(a,n)}{a} = \frac{n}{PGCD(a,n)}.$$

Preuve : Nous avons $k\overline{a} = \overline{0}$ ssi ka est un multiple de n, c'est-à-dire un multiple commun à a et n. Donc ka doit être un multiple de $\text{PPCM}(a,n)$ et k un multiple de $\text{PPCM}(a,n)/a$. Compte tenu de l'égalité

$$\text{PPCM}(a,n) = \frac{an}{\text{PGCD}(a,n)}$$

nous obtenons aussi la seconde égalité. ■

Remarque 3.9.1 Il n'existe pas de formule analogue pour l'ordre d'un élément x dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\star$. Cependant nous verrons que cet ordre est toujours un diviseur de $\phi(n)$, l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^\star$.

Lemme 3.9.3 *Soit $(G,\star)$ un groupe et g élément de G. Alors g est d'ordre infini si et seulement si l'application $\exp_g : \mathbb{Z} \to G$ est injective. En particulier, tous les éléments d'un groupe fini sont d'ordre fini.*

Preuve : Si l'application $\exp_g$ est injective nous avons $\exp_g(n) \neq \exp_g(0)$ pour tout $n > 0$. Puisque $\exp_g(0) = e$, nous avons donc $\exp_g(n) \neq e$ pour tout $n > 0$ et g est d'ordre infini.
Réciproquement supposons g d'ordre infini. Soient $k \leq l$ des entiers tels que $\exp_g(k) = \exp_g(l)$. Alors nous avons $\exp_g(l-k) = e$. Puisque $l - k \geq 0$ et que g est d'ordre infini, il s'ensuit que $k = l$ et donc que $\exp_g$ est injective. ■

Lemme 3.9.4 *Soit $(G,\star)$ un groupe et $g \in G$ un élément d'ordre fini n. Alors l'application*

$$\begin{array}{rcl} \mathbb{Z}/n\mathbb{Z} & \to & G \\ a & \mapsto & \exp_g(a) \end{array}$$

est bien définie et injective. En particulier, l'ensemble des éléments de la forme $\exp_g(a)$, $a \in \mathbb{Z}$, est de cardinal n.

Preuve : Supposons pour alléger les notations que la loi de G est notée multiplicativement. Nous avons donc $\exp_g(a) = g^a$ et $g^n = e$ pour tout $a \in \mathbb{Z}$. Donc $\exp_g(a+kn) = g^{a+kn} = g^a g^{kn} = g^a (g^n)^k = g^a e^k = g^a$. L'application est donc bien définie. Supposons que $a \leq b$ sont deux entiers dont les classes ont même image. Alors nous avons $g^a = g^b$ et donc $g^{b-a} = e$. Pour montrer que n divise $b-a$, effectuons la division euclidienne $b - a = qn + r$ de $b - a$ par n. Par définition, nous avons $0 \leq r \leq (n-1)$. De l'autre côté, nous avons $e = gb - a = gr$. Puisque g est d'ordre n, il s'ensuit que n divise $b - a$ et donc que $a = b$. ■

Théorème 3.9.1 *(Lagrange)*
Soit $(G,\star)$ un groupe fini. L'ordre de tout élément de G divise l'ordre de G.

Exemple 3.9.3 Considérons le groupe $G = (\mathbb{Z}/11\mathbb{Z})^\star$. L'ordre de G est de 10. Voici les ordres des éléments de G :

g	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
$ord(g)$	1	10	5	5	5	10	10	10	5	2

Notons que le nombre d'éléments d'ordre 10 est de $4 = \phi(10)$, le nombre d'éléments d'ordre 5 est de $4 = \phi(5)$ et le nombre d'éléments d'ordre 2 est de $1 = \phi(2)$.

Preuve du théorème : Pour alléger les notations, supposons que la loi de G est notée multiplicativement. Soit $g \in G$. La démonstration se fait en plusieurs étapes :

- Première étape : la relation définie par $x \equiv x'(g) \Leftrightarrow x = x'g^k$ pour un $k \in \mathbb{Z}$, est une relation d'équivalence. Notons x la classe d'équivalence d'un élément x. Par définition, la classe de x est formée de tous les éléments de la forme xg^k, $k \in \mathbb{Z}$.
- Seconde étape : le cardinal de la classe de e est l'ordre de g. En effet, la classe de e est formée de tous les éléments de la forme g^k, $k \in \mathbb{Z}$. C'est donc l'image de l'application $\exp_g : \mathbb{Z} \to G$. Nous avons vu au lemme 3.9.4 qu'elle est en bijection avec $\mathbb{Z}/n\mathbb{Z}$ où n est l'ordre de g.
- Troisième étape : toutes les classes d'équivalence ont même cardinal que la classe de e. En effet, si x est un élément de G, nous avons des bijections inverses l'une de l'autre entre e et x données par les applications $y \mapsto xy$ respectivement $z \mapsto x^{-1}z$.
- Quatrième étape : le cardinal de la classe de e divise l'ordre de G. En effet, nous savons que G est la réunion disjointe des classes d'équivalence. L'ordre de G est donc la somme des cardinaux des classes. Or toutes les classes ont même cardinal que e. L'ordre de G est donc égal au cardinal de la classe de e multiplié par le nombre de classes d'équivalence.

Conclusion : l'ordre de g, qui est égal au cardinal de la classe de e (seconde étape), divise l'ordre de G (troisième étape). ■

Corollaire 3.9.2 *(Théorème d'Euler)*
Soit n un entier ≥ 2 et a un entier premier avec n. Alors on a

$$a^{\phi(n)} \equiv 1(n),$$

où ϕ est l'indicatrice d'Euler.

Preuve : Comme a est premier avec n, la classe $g = \overline{a}$ appartient au groupe $G = (\mathbb{Z}/n\mathbb{Z})^\star$. L'affirmation résulte du théorème de Lagrange car $\phi(n)$ est l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^\star$ par définition. ■

Corollaire 3.9.3 *(Petit Théorème de Fermat)*
Si p est un nombre premier et a un entier qui n'est pas divisible par p, on a

$$a^{p-1} \equiv 1(p).$$

Preuve : On applique le théorème d'Euler en utilisant que $\phi(p) = p - 1$ pour un nombre premier. ■

Remarque 3.9.2 Les théorèmes de Fermat (petit) et d'Euler permettent de calculer très rapidement certains restes de puissances. Dans les exemples suivants, on cherche le reste r de la division euclidienne de a par b.

Exemple 3.9.4

- $a = 67^{100}$, $b = 101$: le nombre 101 est premier et 67 n'est pas divisible par 101. D'après le petit théorème de Fermat, on a $67^{100} \equiv 1(101)$ et donc $r = 1$.
- $a = 1995^{540}$, $b = 541$: le nombre 541 est premier et 1995 n'est pas divisible par 541. D'après le petit théorème de Fermat, on a $1995^{540} \equiv 1(541)$ et donc $r = 1$.
- $a = 25^{24}$, $b = 72$: nous avons $\phi(72) = \phi(8 \times 9) = \phi(8)\phi(9) = 4 \times 6 = 24$. Les nombres 72 et 25 sont premiers entre eux. Nous pouvons donc appliquer le théorème d'Euler pour conclure que $25^{24} \equiv 1(72)$. Donc $r = 1$.
- $a = 51^{24}$, $b = 72$: nous avons $\phi(72) = 24$. Or, les nombres 51 et 72 ne sont pas premiers entre eux et nous ne pouvons pas appliquer le théorème d'Euler. Cependant, soit $x = 51^{24}$. D'après le lemme chinois, pour connaître la classe de x modulo 72, il suffit de connaître les restes de x modulo 8 et modulo 9. Or

$$x \equiv 51^{24} \equiv 3^{24} \equiv 1(8)$$
$$x \equiv 51^{24} \equiv 6^{24} \equiv 0(9).$$

Ici, nous avons appliqué le théorème d'Euler à 3 et 8 ($\phi(8) = 4$) et nous avons utilisé le fait que $62 \equiv 0(9)$. Le lemme chinois nous permet de conclure que $x \equiv 9(72)$ et le reste recherché est donc $r = 9$.

3.10 Algorithme de calcul rapide des puissances

Soit G un groupe dont la loi est notée multiplicativement. Soit g un élément de G et n un entier ≥ 2. Pour calculer g^n, on utilise l'algorithme suivant qui consiste à construire récursivement des suites x_k, y_k, q_k, $k \geq 1$, où $x_k, y_k \in G$ et $q_k \in \mathbb{N}$:

1. Initialisation : on pose $x_1 = g$, $y_1 = e$, $q_k = n$.
2. Passage à l'étape k : on pose $x_k = x_{k-1}^2$, on prend pour q_k le quotient de la division de q_{k-1} par 2 et on pose $y_k = \begin{cases} y_{k-1} \text{ si } q_{k-1} \text{ est pair} \\ x_{k-1}y_{k-1} \text{ si } q_{k-1} \text{ est impair} \end{cases}$
3. Arrêt : quand $q_k = 1$, l'algorithme s'arrête et la puissance recherchée est $g^n = x_k y_k$.

Dans la pratique, on organise les suites x_k, y_k, q_k dans un tableau. Voir les exemples ci-dessous.

Exemple 3.10.1

Calculons 2^{50} dans $(\mathbb{Z}/101\mathbb{Z})^\star$:

k	x_k	y_k	q_k
1	2	1	50
2	4	1	25
3	16	4	12
4	54	4	6
5	88	4	3
6	68	49	1
	100		

Nous trouvons donc que $2^{50} \equiv -1(101)$. La première colonne ne dépend que de $g = 2$ et nous pouvons la réutiliser. Dans le tableau suivant, nous utilisons deux fois la même première colonne pour calculer 3^{50} et 3^{20} dans $(\mathbb{Z}/101\mathbb{Z})^\star$:

x_k	y_k	q_k	y_k	q_k
3	1	50	1	20
9	1	25	1	10
81	9	12	1	5
97	9	6	81	2
16	9	3	81	1
54	43	1		
	100		84	

Lemme 3.10.1 *L'algorithme décrit ci-dessus est correct.*

Preuve : Nous allons montrer par récurrence que nous avons $x_k^{q_k} y_k = g^n$. Ceci entraînera l'affirmation car pour $q_k = e$, cette égalité se spécialise en $x_k y_k = g^n$.
À l'étape $k = 1$, l'affirmation est vraie par définition de l'initialisation de l'algorithme. Supposons qu'elle est vraie pour l'étape $k - 1$ et montrons la pour l'étape k. Soit $q^{k-1} = 2q^k + r^k$ la division euclidienne de q^{k-1} par 2. Par l'hypothèse de récurrence, nous avons

$$x_{k-1}^{q_{k-1}} y_{k-1} = g^n.$$

Si nous substituons le résultat de la division euclidienne pour q_{k-1}, nous trouvons

$$g^n = x_{k-1}^{2qk+rk} y_{k-1} = (x_{k-1}^2)^{q_k} (x_{k-1}^{r_k}) y_{k-1} = x_k^{q_k} y_k.$$

Pour la dernière égalité, nous avons utilisé la définition de x_k et y_k (le nombre q_{k-1} est pair ssi $r_k = 0$). ■

3.11 Calcul de l'ordre d'un élément

Soit n un entier. Un diviseur positif d de n est maximal s'il est de la forme n/p où p est un diviseur premier de n. Soit G un groupe fini dont la loi est notée multiplicativement. Soit g un élément de G. Soit n un entier positif.

Lemme 3.11.1

1. *On a $g^n = e$ si et seulement si n est un multiple de l'ordre de g.*
2. *L'élément g est d'ordre n si et seulement si $g^n = e$ et $g^d \neq e$ pour tout diviseur maximal de n.*
3. *Si g est d'ordre n et d divise n, alors g^d est d'ordre n/d.*
4. *Plus généralement, si g est d'ordre n et a un entier quelconque, alors g^a est d'ordre $n/PGCD(a,n)$.*

Preuve :

1. Ceci est clair d'après le lemme qui affirme que l'application
$$\begin{array}{rcl} \mathbb{Z}/ord(g)\mathbb{Z} & \to & G \\ k & \mapsto & g_k \end{array}$$
est injective.
2. La condition est clairement nécessaire. Supposons réciproquement qu'elle est vérifiée. Alors n est multiple de l'ordre de g d'après 1., mais aucun diviseur propre de n n'est multiple de l'ordre de g (tout diviseur propre divise un diviseur maximal de n). Donc $n = ord(g)$.
3. Nous avons $(g^d)^k = g^{dk}$ ce qui donne immédiatement l'affirmation.
4. D'après le lemme 3.9.4, nous avons $g^k = e$ ssi $k = 0$ dans $\mathbb{Z}/n\mathbb{Z}$. Donc l'ordre de g^a est égal à l'ordre de a dans $\mathbb{Z}/n\mathbb{Z}$. Ce dernier est égal à $n/\mathrm{PGCD}(a,n)$ d'après le lemme 3.9.2.

■

Remarque 3.11.1 Pour déterminer l'ordre de g, on calcule les puissances g^d pour les diviseurs maximaux d de n. Si on a $g^d \neq e$ pour tout diviseur maximal, alors g est d'ordre n (et G est cyclique engendré par g). Sinon, on a $g^d = e$ pour un diviseur maximal d de n et on recommence avec n remplacé par d. Dans le calcul des puissances $g^{d'}$ pour les diviseurs maximaux d' de d on pourra cependant omettre tous ceux qui divisent un diviseur maximal d'' de n pour lequel $g^{d''} \neq e$. Voir l'exemple suivant.

Exemple 3.11.1 Calculons l'ordre de 2 dans $(\mathbb{Z}/113\mathbb{Z})^\star$. Ce groupe est d'ordre $n = 112 = 7 \times 16$. Les diviseurs maximaux de n sont 16 et 56. Calculons donc 2^{56} et 2^{16}.

x_k	y_k	q_k	y_k	q_k
2	1	56	1	16
4	1	28	1	8
16	1	14	1	4
30	1	7	1	2
109	30	3	1	1
16	106	1		
	1		109	

Ainsi $2^{16} \neq e$ et $2^{56} = e$. Les diviseurs maximaux de 56 sont 8 et 28. Puisque $2^{16} \neq e$ nous avons $2^8 \neq e$ et il suffit de calculer 2^{28}. On trouve $2^{28} = 1$. Les diviseurs maximaux de 28 sont 4 et 14. Puisque $2^8 \neq 1$, nous avons $2^4 \neq 1$ et il suffit de calculer 2^{14}. On trouve $2^{14} = -1$ et l'ordre de 2 dans $(\mathbb{Z}/113\mathbb{Z})^\star$ est donc de 28. Déterminons les ordres des éléments de $(\mathbb{Z}/11\mathbb{Z})^\star$. Calculons l'ordre de 2. Nous avons $2^{10} \equiv 1(11)$ par le petit théorème de Fermat. Les diviseurs maximaux de 10 sont 2 et 5. Nous avons

$$2^2 = 4 \ , \ 2^5 \equiv 2 \times 4 \times 4 \equiv -1(11).$$

Donc 2 est d'ordre 10 et tout élément de $(\mathbb{Z}/11\mathbb{Z})^\star$ est une puissance de 2 d'après le lemme 3.9.4. Calculons ces puissances

k	0	1	2	3	4	5	6	7	8	9
2^k	1	2	4	8	5	10	9	7	3	6

Maintenant, on calcule facilement les ordres de tous les éléments à l'aide des parties 2. et 3. du lemme. Par exemple, on a

$$ord(3) = ord(2^8) = \frac{10}{\text{PGCD}(10,8)} = 5$$
$$ord(4) = ord(2^2) = \frac{10}{2} = 5.$$

On trouve la table ci-dessous (et on retrouve les résultats de l'exemple 3.9.3)

g	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
$ord(g)$	1	10	5	5	5	10	10	10	5	2

Chapitre 4

Les espaces vectoriels

4.1 Introduction

La structure d'espace vectoriel intervient dans une grande partie des mathématiques : elle réalise un lien fondamental entre l'algèbre et la géométrie. On l'utilisera en algèbre linéaire, en analyse et en géométrie. Un espace vectoriel est un ensemble muni d'une loi interne $+$ et d'une loi externe $\times$, vérifiant des conditions précises. Dans ce chapitre, K désignera un corps commutatif, en pratique $K = \mathbb{R}$ ou $\mathbb{C}$.

4.2 Structure d'espace vectoriel

Définition 4.2.1 *On appelle K-espace vectoriel tout ensemble E muni d'une loi interne notée $+$ et d'une loi externe définie par*

$$\begin{array}{ccc} K \times E & \to & E \\ (\lambda, x) & \mapsto & \lambda \times x \end{array}$$

telles que :

1. *$(E, +)$ est un groupe abélien,*
2. *$\forall (\lambda, \mu) \in K^2$, $\forall x \in E$, $(\lambda + \mu)x = \lambda x + \mu x$,*
3. *$\forall \lambda \in K$, $\forall (x, y) \in E^2$, $\lambda(x + y) = \lambda x + \lambda y$,*
4. *$\forall (\lambda, \mu) \in K^2$, $\forall x \in E$, $\lambda(\mu x) = (\lambda\mu)x$*
5. *$\forall x \in E$, $1x = x$.*

On abrègera espace vectoriel en « ev » et K-espace vectoriel en « K-ev ».

Définition 4.2.2 *Les éléments d'un K-ev seront appelés **vecteurs**, les éléments de K seront appelés **scalaires**.*

Exemple 4.2.1

1. Le corps K est un K-ev, en prenant pour loi interne $\begin{array}{ccc} K \times K & \to & K \\ (x, y) & \mapsto & x + y \end{array}$ et pour loi externe la multiplication dans K : $\begin{array}{ccc} K \times K & \to & K \\ (\lambda, x) & \mapsto & \lambda \times x \end{array}$. Ici les éléments de K sont simultanément considérés comme des vecteurs et comme des scalaires.
2. Plus généralement, soit L un corps tel que K soit un sous-corps de L. Alors L est un K-ev, pour les lois interne $\begin{array}{ccc} L \times L & \to & L \\ (x, y) & \mapsto & x + y \end{array}$ et externe $\begin{array}{ccc} K \times L & \to & L \\ (\lambda, x) & \mapsto & \lambda \times x \end{array}$ (multiplication dans L).
   En particulier, $\mathbb{C}$ est un $\mathbb{R}$-ev pour les lois usuelles.

3. Soient $n \in \mathbb{N}^\star$, $E_1, \ldots, E_n$ des K-ev. Le **produit** $E = \prod_{i=1}^{n} E_i$ est alors un K-ev pour la loi interne et la loi externe définies respectivement par :
   – $\forall ((x_1, \ldots, x_n), (y_1, \ldots, y_n)) \in E^2$, $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$
   – $\forall \lambda \in K$, $\forall (x_1, \ldots, x_n) \in E$, $\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$.
   En particulier, pour tout $n \in \mathbb{N}^\star$, K^n est un K-ev pour les lois usuelles.
4. Soient X un ensemble non vide. E est un K-ev. L'ensemble E^X des applications de X dans E est un K-ev pour les lois interne et externe définies respectivement par
   – $\forall (f, g) \in (E^X)^2$, $\forall x \in X$, $(f + g)(x) = f(x) + g(x)$,
   – $\forall \lambda \in K$, $\forall f \in E^X$, $\forall x \in X$, $(\lambda f)(x) = \lambda f(x)$.
   Par exemple, l'ensemble $\mathbb{R}^N$ des suites réelles est un $\mathbb{R}$-ev pour les lois usuelles.
5. L'ensemble $K[X]$ des polynômes à une indéterminée et à coefficients dans K est un K-ev pour l'addition et la multiplication externe.

Proposition 4.2.1 *Soit E un K-ev. On a, pour tous λ, μ de K et tous x, y de E :*

1. $\lambda x = 0 \Leftrightarrow (\lambda = 0$ *ou* $x = 0)$,
2. $(\lambda - \mu)x = \lambda x - \mu x$,
3. $\lambda(x - y) = \lambda x - \lambda y$.

Preuve :

1. • $0x = (0 + 0)x = 0x + 0x$ d'où $0x = 0$,
   • $\lambda 0 = \lambda(0 + 0) = \lambda 0 + \lambda 0$ d'où $\lambda 0 = 0$.
   • si $\lambda x = 0$ et si $\lambda \neq 0$ alors, en notant λ^{-1} l'inverse de λ dans le corps K on a $x = 1x = (\lambda^{-1}\lambda)x = \lambda^{-1}(\lambda x) = \lambda^{-1}0 = 0$.
2. $\lambda x = ((\lambda - \mu) + \mu)x = (\lambda - \mu)x + \mu x$ d'où $(\lambda - \mu)x = (\lambda x) - (\mu x)$ ce qui est noté $\lambda x - \mu x$.
3. $\lambda x = \lambda((x - y) + y) = \lambda(x - y) + \lambda y$ d'où $\lambda(x - y) = \lambda x - \lambda y$. ■

La proposition suivante est immédiate par récurrence :

Proposition 4.2.2 *Soient E un K-ev, $n, p \in \mathbb{N}^\star$, x, x_i, y_i, x_{ij} des éléments de E, $\lambda, \lambda_i, \ldots$ des éléments de K. On a :*

1. $\left(\sum_{i=1}^{n} x_i\right) + \left(\sum_{i=n+1}^{p} x_i\right) = \sum_{i=1}^{p} x_i$ *(si $p \geq n + 1$)*,
2. $\sum_{i=1}^{n}(x_i + y_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$
3. $\sum_{i=1}^{n}\left(\sum_{j=1}^{p} x_{ij}\right) = \sum_{j=1}^{p}\left(\sum_{i=1}^{n} x_{ij}\right)$,
4. $\forall \sigma \in S_n$ *(groupe des permutations d'indice n)*, $\sum_{i=1}^{n} x_{\sigma(i)} = \sum_{i=1}^{n} x_i$,
5. $\sum_{i=1}^{n}(\lambda x_i) = \lambda \sum_{i=1}^{n} x_i$,
6. $\sum_{i=1}^{n}(\lambda_i x) = \left(\sum_{i=1}^{n} \lambda_i\right) x$.

Définition 4.2.3 *On appelle K-**algèbre** tout ensemble A muni d'une loi interne notée $+$, d'une loi externe* $\begin{array}{ccc} K \times A & \to & A \\ (\lambda, x) & \mapsto & \lambda x \end{array}$ *, et d'une loi interne (appelée $3^{\text{ème}}$ loi) notée ici $\star$, telles que :*

- *$(A, +, \times)$ est un K-ev,*
- *$\star$ est distributive sur $+$,*
- *$\forall \lambda \in K$, $\forall (x, y) \in A^2$, $\lambda(x \star y) = (\lambda x) \star y = x \star (\lambda y)$.*

Une K-algèbre est dite
- associative si $\star$ est associative,
- commutative si $\star$ est commutative,
- unifère (ou unitaire) si et seulement si A admet un élément neutre pour $\star$.

Exemple 4.2.2
- Tout corps commutatif K est une K-algèbre associative, commutative, unifère en prenant pour $3^{\text{ème}}$ loi la multiplication.
- Plus généralement, si L est un surcorps de K, L est une K-algèbre associative et unifère en prenant pour $3^{\text{ème}}$ loi la multiplication dans L. Par exemple, $\mathbb{C}$ est une $\mathbb{R}$-algèbre associative, commutative, unifère pour les lois usuelles.
- Soit X un sous-ensemble non vide. K^X est un K-ev pour les lois usuelles. En munissant K^X d'une $3^{\text{ème}}$ loi, notée par l'absence de symbole, définie par
$$\forall x \in X,\ (fg)(x) = f(x)g(x),$$
K^X est une K-algèbre associative, commutative, unifère, le neutre pour la $3^{\text{ème}}$ loi étant l'application constante égale à 1.
- $K[X]$ est une K-algèbre associative, commutative et unifère.

Souvent on montrera que A est une algèbre en montrant que A est une sous-algèbre d'une algèbre connue.

4.3 Les sous-espaces vectoriels

Définition 4.3.1 *Soient E un K-ev, $F \in \mathcal{P}(E)$. On dit que F est un **sous-espace vectoriel** de E si et seulement si :*

1. *$F \neq \emptyset$,*
2. *$\forall (x, y) \in F^2$, $x + y \in F$,*
3. *$\forall \lambda \in K$, $\forall x \in F$, $\lambda x \in F$.*

On abrègera sous-espace vectoriel en « sev ». Pour rappeler le corps K utilisé, on dit parfois sous-K-ev au lieu de sev.

Proposition 4.3.1 *Soient E un K-ev, $F \in \mathcal{P}(E)$. Si F est un sev de E alors F est un K-ev pour les lois* $+ : \begin{array}{ccc} F \times F & \to & F \\ (x, y) & \mapsto & x + y \end{array}$ *et externe* $\times : \begin{array}{ccc} K \times F & \to & F \\ (\lambda, x) & \mapsto & \lambda x \end{array}$ *induites par celles de E.*

Exemple 4.3.1
- $\mathbb{R} \times \{0\}$ est un sev du $\mathbb{R}$-ev $\mathbb{R}^2$.
- Pour tout $n \in \mathbb{N}$, $K_n[X]$ est un sev du K-ev $K[X]$.

Remarque 4.3.1
- $\{0\}$ et E sont des sev du K-ev E.
- Si F est un sev de l'ev E et si G est un sev de F alors G est un sev de E, on dit qu'il y a transitivité de la notion de sev.

Proposition 4.3.2 *Soient E un K-ev et $(F_i)_{i\in I}$ une famille de sev de E alors $\bigcap_{i\in I} F_i$ est un sev de E.*

Preuve : Notons $F = \bigcap_{i\in I} F_i$.
- $F \neq \emptyset$; en effet, $0 \in F$ puisque $\forall i \in I,\ 0 \in F_i$.
- Soit $(x, y) \in F^2$. On a $\forall i \in I,\ x \in F_i$ et $y \in F_i$ donc $\forall i \in I,\ x + y \in F_i$ d'où $x + y \in F$.
- Soit $(\lambda, x) \in K \times F$. On a $\forall i \in I,\ x \in F_i$ donc $\forall i \in I,\ \lambda x \in F_i$ d'où $\lambda x \in F$. ■

Proposition 4.3.3 *Soient E un K-ev, F_1, F_2 deux sev de E. On note*

$$F_1 + F_2 = \{x \in E, \exists (x_1, x_2) \in F_1 \times F_2, x = x_1 + x_2\} = \{x_1 + x_2, (x_1, x_2) \in F_1 \times F_2\}$$

la somme de F_1 et F_2 alors $F_1 + F_2$ est un sev de E.

Preuve : Montrons que $F_1 + F_2$ est un sev de E :
- $F_1 + F_2 \neq \emptyset$ car $0 = 0 + 0 \in F_1 + F_2$.
- Soit $(x, y) \in (F_1 + F_2)^2$. Il existe $(x_1, x_2) \in F_1 \times F_2$, $(y_1, y_2) \in F_1 \times F_2$ tels que : $x = x_1 + x_2$ et $y = y_1 + y_2$. On a alors $x + y = (x_1 + x_2) + (y_1 + y_2) = (x_1 + y_1) + (x_2 + y_2) \in F_1 + F_2$.
- Soit $(\lambda, x) \in K \times (F_1 + F_2)$. Il existe $(x_1, x_2) \in F_1 \times F_2$ tel que $x = x_1 + x_2$. On a alors $\lambda x = \lambda(x_1 + x_2) = \lambda x_1 + \lambda x_2 \in F_1 + F_2$. ■

Proposition 4.3.4 *Soit E un K-ev. On a pour tous sev F_1, F_2, F_3 de E :*

$F_1 + F_2 = F_2 + F_1$	$F_1 \cap F_2 = F_2 \cap F_1$
$F_1 \subset F_1 + F_2$	$F_1 \subset F_1 \cap F_2$
$\begin{cases} F_1 \subset F_3 \\ F_2 \subset F_3 \end{cases} \Leftrightarrow F_1 + F_2 \subset F_3$	$\begin{cases} F_1 \subset F_3 \\ F_2 \subset F_3 \end{cases} \Leftrightarrow F_3 \subset F_1 \cap F_2$
$F_1 \subset F_2 \Rightarrow F_1 + F_3 \subset F_2 + F_3$	$F_1 \subset F_2 \Rightarrow F_1 \cap F_3 \subset F_2 \cap F_3$
$F_1 + F_1 = F_1$	$F_1 \cap F_1 = F_1$
$F_1 + \{0\} = F_1$	$F_1 \cap \{0\} = F_1$
$F_1 + E = E$	$F_1 \cap E = E$
$(F_1 + F_2) + F_3 = F_1 + (F_2 + F_3)$	$(F_1 \cap F_2) \cap F_3 = F_1 \cap (F_2 \cap F_3)$

Preuve : les démonstrations sont presque immédiates. Par exemple, pour démontrer qu $F_1 \subset F_1 + F_2$, on remarquera que $\forall x \in F_1$, on peut écrire $x = x + 0$ où $x \in F_1$ et $0 \in F_2$ donc $x \in F_1 + F_2$. ■

Exercice 72 Parmi les espaces suivants, quels sont ceux qui sont des espaces vectoriels ?

1. $A = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2, a + b = 1 \right\}$
2. $B = \left\{ \begin{pmatrix} a \\ b \\ c \end{pmatrix} \in \mathbb{R}^3, 2a - 5b + c = 0, b + c = 0 \right\}$
3. $C = \left\{ \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \in \mathbb{R}^4, a + c - 2d = -1, 2a - b + 3c = 0 \right\}$

4. $D = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2, a^2 + b = 0 \right\}$

Correction : On utilisera la caractérisation des sev d'un ev.

1. L'ensemble A est inclus dans $\mathbb{R}^2$ qui est un ev mais il ne contient pas 0 (l'élément nul de $\mathbb{R}^2$) car $0 + 0 \neq 1$ donc A n'est pas un ev.
2. B est inclus dans $\mathbb{R}^3$ qui est un ev. B n'est pas vide car il contient 0 (l'élément nul de $\mathbb{R}^3$), en effet, $2\times0-5\times0+0 = 0$ et $0+0 = 0$. Qu'en est-il de la stabilité par combinaison linéaire ? Soient $X = (x, y, z)$ et $X' = (x', y', z')$ deux éléments de B ainsi que deux réels λ et μ. Montrons que $\lambda X + \mu X' \in B$ soit
$$\begin{cases} 2x - 5y + z &= 0 \\ y + z &= 0 \\ 2x' - 5y' + z' &= 0 \\ y' + z' &= 0 \end{cases} \Rightarrow \begin{cases} 2(\lambda x + \mu x') - 5(\lambda x + \mu y') + (\lambda z + \mu z') &= 0 \\ (\lambda x + \mu y') + (\lambda z + \mu z') &= 0 \end{cases}$$
Pour cela, on développe puis on regroupe les termes en λ et les termes en μ : on a
$$\begin{cases} 2(\lambda x + \mu x') - 5(\lambda y + \mu y') + (\lambda z + \mu z') &= \lambda(2x - 5y + z) + \mu(2x' - 5y' + z') = \lambda \times 0 + \mu \times 0 = 0 \\ (\lambda y + \mu y') + (\lambda z + \mu z') &= \lambda(y + z) + \mu(y' + z') = \lambda \times 0 + \mu \times 0 = 0 \end{cases}$$
ce qui montre que C est stable par combinaison linéaire. Par conséquent, l'ensemble B est un ev.
3. C est inclus dans $\mathbb{R}^4$ qui est un ev mais il ne contient pas 0 (l'élément nul de $\mathbb{R}^4$) car $0+0-2\times0 \neq -1$ donc C n'est pas un ev.
4. D est inclus dans $\mathbb{R}^2$ qui est un ev. D n'est pas vide car il contient 0 ($0^2 + 0 = 0$).
Si D est un ev, D est stable par combinaison linéaire. Considérons le vecteur $X = (1, -1) \in D$, on a $2X = (2, -2) \notin D$ car $2^2 + (-2) = 2 \neq 0$ donc D n'est pas un ev.

Exercice 73 Déterminer lesquels des ensembles E_1, E_2, E_3 et E_4 sont des sev de $\mathbb{R}^3$.

1. $E_1 = \{(x, y, z) \in \mathbb{R}^3, x + y - z = x + y + z = 0\}$,
2. $E_2 = \{(x, y, z) \in \mathbb{R}^3, x^2 - z^2 = 0\}$,
3. $E_3 = \{(x, y, z) \in \mathbb{R}^3, e^x e^y = 0\}$,
4. $E_4 = \{(x, y, z) \in \mathbb{R}^3, z(x^2 + y^2) = 0\}$.

Correction :

1. E_1 est un sev de $\mathbb{R}^3$. En effet :
   (a) $(0, 0, 0) \in E_1$.
   (b) Soient (x, y, z) et (x', y', z') deux éléments de E_1. On a donc $x + y - z = x + y + z = 0$ et $x' + y' - z' = x' + y' + z' = 0$. Donc $(x + x') + (y + y') - (z + z') = (x + x') + (y + y') + (z + z') = 0$ et $(x, y, z) + (x', y', z') = ((x + x'), (y + y'), (z + z')) \in E_1$.
   (c) Soient $\lambda \in \mathbb{R}$ et $(x, y, z) \in E_1$. Alors la relation $x + y - z = x + y + z = 0$ implique que $\lambda x + \lambda y - \lambda z = \lambda x + \lambda y + \lambda z = 0$ donc que $\lambda(x, y, z) = (\lambda x, \lambda y, \lambda z) \in E_1$.
2. $E_2 = \{(x, y, z) \in \mathbb{R}^3, x^2 - z^2 = 0\}$ c'est-à-dire $E_2 = \{(x, y, z) \in \mathbb{R}^3, x = z \text{ ou } x = -z\}$. Donc $(1, 0, -1)$ et $(1, 0, 1)$ appartiennent à E_2 mais $(1, 0, -1) + (1, 0, 1) = (2, 0, 0)$ n'appartient pas à E_2 qui n'est en conséquence pas un sev de $\mathbb{R}^3$.
3. $(0, 0, 0) \notin E_3$ donc E_3 n'est pas un sev de $\mathbb{R}^3$.
4. Les vecteurs $(1, 0, 0)$ et $(1, 0, 0)$ appartiennent à E_4 mais leur somme $(1, 0, 0) + (0, 0, 1) = (1, 0, 1)$ ne lui appartient pas donc E_4 n'est pas un sev de $\mathbb{R}^3$.

Exercice 74 (non corrigé) Soit E l'ensemble des applications $f : \mathbb{R} \to \mathbb{R}$ telles qu'il existe $A \in \mathbb{R}_+^\star$ et $g, h : \mathbb{R} \to \mathbb{R}$ croissantes telles que : $\forall x \in \mathbb{R}$, $(|x| \geq A \Rightarrow f(x) = g(x) - h(x))$.
Montrer que E est un $\mathbb{R}$-ev pour les lois usuelles.

Exercice 75 Déterminer parmi les ensembles suivants ceux qui sont des sev :

1. $E_1 = \{(x, y, z) \in \mathbb{R}^3, x + y + a = 0 \text{ et } x + 3az = 0\}$,
2. $E_2 = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}), f(1) = 0\}$,
3. $E_3 = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}), f(0) = 1\}$,
4. $E_4 = \{P \in \mathbb{R}_n[X], P' = 3\}$.
5. $E_5 = \{(x, y) \in \mathbb{R}^2, x + \alpha y + 1 \geq 0\}$.

Correction :

1. E_1 n'est pas un sev si $a \neq 0$ car alors, $0 \notin E_1$. Par contre, si $a = 0$, E_1 est bien un ev car dans ce cas, l'intersection des sev $\{(x, y, z) \in \mathbb{R}^3, x + y = 0\}$ et $\{(x, y, z) \in \mathbb{R}^3, x = 0\}$.
2. E_2 est un sev de $\mathcal{F}(\mathbb{R}, \mathbb{R})$.
3. E_3 n'est pas un ev car la fonction nulle n'appartient pas à E_3.
4. E_4 n'est pas un ev car le polynôme nul n'appartient pas à E_4.
5. E_5 n'est pas un ev, en fait ce n'est même pas un sous-groupe de $(\mathbb{R}^2, +)$ car $(2, 0) \in E_5$ mais $-(2, 0) = (-2, 0) \notin E_5$.

Exercice 76 Soit E un ev (sur $\mathbb{R}$ ou $\mathbb{C}$).

1. Soient F et G deux sev de E. Montrer que
$$F \cup G \text{ est un sev de } E \Leftrightarrow F \subset G \text{ ou } G \subset F.$$
2. Soient H un troisième sev de E. Prouver que
$$G \subset F \Rightarrow F \cap (G + H) = G + (F \cap H).$$

Correction :

1. (a) Sens $\Leftarrow$. Si $F \subset G$ alors $F \cup G = G$ donc $F \cup G$ est un sev. De même si $G \subset F$.
   (b) Sens $\Rightarrow$. On suppose que $F \cup G$ est un sev. Par l'absurde supposons que F n'est pas inclus dans G et que G n'est pas inclus dans F. Alors il existe $x \in F \backslash G$ et $y \in G \backslash F$. Mais alors $x \in F \cup G$, $y \in F \cup G$ donc $x + y \in F \cup G$ (car $F \cup G$ est un sev). Comme $x + y \in F \cup G$ alors $x + y \in F$ ou $x + y \in G$.
   – Si $x + y \in F$ alors, comme $x \in F$, $(x + y) + (-x) \in F$ donc $y \in F$ ce qui est absurde.
   – Si $x + y \in G$ alors, comme $y \in G$, $(x + y) + (-y) \in G$ donc $x \in G$ ce qui est absurde.
   Dans les deux cas on obtient une contradiction donc F est inclus dans G ou G est inclus dans F.
2. Supposons $G \subset F$.
   – Inclusion $\supset$. Soit $x \in G + (F \cap H)$. Alors il existe $a \in G$, $b \in F \cap H$ tels que $x = a + b$. Comme $G \subset F$ alors $a \in F$, de plus $b \in F$ donc $x = a + b \in F$. D'autre part $a \in G$, $b \in H$ donc $x = a + b \in G + H$. Donc $x \in F \cap (G + H)$.
   – Inclusion $\subset$. Soit $x \in F \cap (G + H)$. Alors il existe $a \in G$, $b \in H$ tels que $x = a + b$. Maintenant $b = x - a$ avec $x \in F$ et $a \in G \subset F$ donc $b \in F$ et $b \in F \cap H$. Donc $x = a + b \in G + (F \cap H)$.

Définition 4.3.2 *Soient E un K-ev, F_1, F_2 deux sev de E. On dit que F_1 et F_2 sont en* ***somme directe*** *si et seulement si $F_1 \cap F_2 = \{0\}$.*
Lorsque F_1 et F_2 sont deux sev en somme directe, on note $F_1 \oplus F_2$ au lieu de $F_1 + F_2$.

Exemple 4.3.2 Pour $K = \mathbb{R}$, $E = \mathbb{R}^3$, les sev $F_1 = \mathbb{R} \times \{0\} \times \{0\}$ et $F_2 = \{0\} \times \mathbb{R} \times \{0\}$ sont en somme directe.

Proposition 4.3.5 *Pour que deux sev F_1 et F_2 d'un K-ev soient en somme directe, il faut et il suffit que tout élément de $F_1 + F_2$ se décompose d'une façon unique en somme d'un élément de F_1 et d'un élément de F_2.*

Preuve :

1. Supposons que F_1 et F_2 soient en somme directe, et soit $x \in F_1 + F_2$.
   - Par définition de $F_1 + F_2$, il existe $(x_1, x_2) \in F_1 \times F_2$ tel que $x = x_1 + x_2$.
   - Soient $(x_1, x_2) \in F_1 \times F_2$, $(y_1, y_2) \in F_1 \times F_2$ tels que $x = x_1 + x_2 = y_1 + y_2$.

   Alors $x_1 - y_1 = x_2 - y_2$. Comme $(x_1 - y_1 \in F_1, x_2 - y_2 \in F_2, F_1 \cap F_2 = \{0\})$, on en déduit que $x_1 - y_1 = x_2 - y_2 = 0$ donc $x_1 = y_1$ et $x_2 = y_2$. Ainsi, x se décompose d'une façon unique sur F_1 et F_2.
2. Réciproquement, supposons que tout élément de $F_1 + F_2$ se décompose de façon unique sur F_1 et F_2. Soit $x \in F_1 \cap F_2$, on dispose de deux décompositions de 0 sur F_1 et F_2 : $0 = 0 + 0$ et $0 = x + (-x)$ d'où $x = 0$. Ainsi $F_1 \cap F_2 = \{0\}$ et F_1 et F_2 sont en somme directe. ■

Définition 4.3.3 *Deux sev F_1 et F_2 d'un K-ev sont dits* ***supplémentaires*** *dans E si et seulement si*

$$F_1 \cap F_2 = \{0\} \text{ et } F_1 + F_2 = E.$$

Exemple 4.3.3

- Soient $K = \mathbb{R}$, $E = \mathbb{R}^2$, $F_1 = \mathbb{R} \times \{0\}$ et $F_2 = \{0\} \times \mathbb{R}$. F_1 et F_2 sont deux sev supplémentaires dans E.
- Soient $K = \mathbb{R}$ et $E = \mathbb{R}^{\mathbb{R}}$, F_1 (respectivement F_2) est l'ensemble des applications paires (respectivement impaires) de $\mathbb{R}$ dans $\mathbb{R}$. F_1 et F_2 sont deux sev de E supplémentaires dans E. En effet :
  . si $f \in F_1 \cap F_2$ alors f est paire et impaire donc $\forall x \in \mathbb{R}$, $f(x) = -f(x)$ d'où $f = 0$,
  . tout f de E se décompose en $f = g + h$ où $g \in F_1$ et $h \in F_2$ sont définies par
  $$\forall x \in \mathbb{R},\ g(x) = \frac{1}{2}(f(x) + f(-x)) \text{ et } h(x) = \frac{1}{2}(f(x) - f(-x)).$$

Remarque 4.3.2

1. Un sev F de E peut admettre plusieurs supplémentaires dans E. Par exemple, si $K = \mathbb{R}$ et $E = \mathbb{R}^2$, le sev $F = \mathbb{R} \times \{0\}$ de E admet une infinité de supplémentaires dans E, qui sont tous les $\mathbb{R}x$, $x \in E - F$.
2. On montrera plus loin que si E est de dimension finie, alors tout sev de E admet au moins un supplémentaire dans E.

Exercice 77 Soit $A \in \mathbb{R}[X]$ un polynôme non nul et $F = \{P \in \mathbb{R}[X]; A \text{ divise } P\}$. Montrer que F est un sous-espace vectoriel de $\mathbb{R}[X]$ et trouver un supplémentaire à F.
Correction : Remarquons que $F = \{AQ; Q \in \mathbb{R}[X]\}$, ce qui permet facilement de prouver que F est un sous-espace vectoriel de $\mathbb{R}[X]$. D'autre part, prenons maintenant $B \in \mathbb{R}[X]$. D'après la division euclidienne, il s'écrit de façon unique sous la forme $B = AQ + R$, où $Q \in \mathbb{R}[X]$ et $R \in \mathbb{R}_{d-1}[X]$, où d est le degré de B, c'est-à-dire de façon unique comme la somme d'un élément de F et d'un élément de $\mathbb{R}_{d-1}[X]$. Ceci signifie exactement que F et $\mathbb{R}_{d-1}[X]$ sont des sous-espaces vectoriels supplémentaires de $\mathbb{R}[X]$.

Exercice 78 Soit E l'espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$.

1. Soit $a \in \mathbb{R}$. On désigne par F le sous-espace des fonctions constantes et par G_a le sous-espace des fonctions qui s'annulent en a. Montrer que F et G_a sont supplémentaires dans E.

2. Plus généralement, soient $a_0, \ldots, a_N$ des éléments distincts de $\mathbb{R}$ et $G = \{f \in E; f(a_0) = \ldots = f(a_N) = 0\}$. Trouver un supplémentaire à G.

Correction :

1. On remarque d'abord que $F \cap G_a = \{0\}$ (une fonction constante qui s'annule en un point est forcément identiquement nulle). Ensuite, prenons $h \in E$, on doit prouver que h se décompose sous la forme $h = g + C$, où C est une constante et $g(a) = 0$. Admettons que ce soit le cas. Alors, nécessairement, $h(a) = C$ et $g(x) = h(x) - C = h(x) - h(a)$. On pose donc $C = f(a)$ et $g(x) = h(x) - h(a)$. Clairement, $h = g + C$ et $g(a) = 0$ ce qui prouve que $g \in G_a$.
2. On va prouver que G et $\mathbb{R}_N[X]$ sont en somme directe. Pour cela, il suffit de prouver que toute fonction $h \in E$ se décompose uniquement sous la forme $h = g + P$, avec $g \in G$ et $P \in \mathbb{R}_N[X]$.
   Unicité. Si $h = g + P$, alors, pour tout $i \in \{1, \ldots, N\}$, on a $P(a_i) = h(a_i)$. Or, par la théorie des polynômes interpolateurs de Lagrange (par exemple), on sait qu'il existe un unique polynôme $P \in \mathbb{R}_N[X]$ qui vérifie cette propriété. D'où l'unicité de P et par suite celle de g puisque $g = h - P$.
   Existence. Considérons P l'unique polynôme de $\mathbb{R}_N[X]$ tel que $P(a_i) = h(a_i)$ pour tout $i \in \{1, \ldots, N\}$ (un tel polynôme existe). De plus, on pose $g = h - P$. Alors $g(a_i) = P(a_i) - h(a_i) = 0$ et donc $g \in G$, et bien sûr $h = g + P$.

Exercice 79 Soient F et G deux sous-espaces vectoriels d'un espace vectoriel E tels que $F + G = E$. Soit F' un supplémentaire de $F \cap G$ dans F. Montrer que $F' \oplus G = E$.
Correction : Prouvons d'abord que F' et G sont en somme directe, c'est-à-dire que $F' \cap G = \{0\}$. Prenons $x \in G \cap F'$. Alors, puisque $F \cap G$ et F' sont en somme directe, et que $x \in F \cap G$ (x est dans G et dans $F' \subset F$), on en déduit $x = 0$. D'autre part, il faut montrer que $F' + G = E$. Soit $z \in E$. On sait que $z = f + g$, avec $f \in F$ et $g \in G$ (car $F + G = E$). D'autre part, on peut décomposer f en $g' + f'$, avec $g' \in F \cap G$ et $f' \in F'$. Ainsi, on obtient $z = g' + f' + g = f' + (g + g')$ avec $f' \in F'$ et $g + g' \in G$: $F' + G = E$ ce qui achève la preuve que F' et G sont supplémentaires.

Exercice 80 Soit $E = \Delta^1(\mathbb{R}, \mathbb{R})$ et $F = \{f \in E / f(0) = f'(0) = 0\}$. Montrer que F est un sev de E et déterminer un supplémentaire de F dans E.
Correction : Les fonctions de E qui ne sont pas dans F sont les fonctions h qui vérifient $h(0) \neq 0$ ou $h'(0) \neq 0$. Par exemple les fonctions constantes $x \mapsto b$, ($b \in \mathbb{R}$), ou les homothéties $x \mapsto ax$, ($a \in \mathbb{R}$) n'appartiennent pas à F. Posons

$$G = \{x \mapsto ax + b, (a, b) \in \mathbb{R}^2\}.$$

Montrons que G est un supplémentaire de F dans E. Soit $f \in F \cap G$ alors $f(x) = ax + b$ (car $f \in G$) et $f(0) = b$ et $f'(0) = a$. Mais $f \in F$ donc $f(0) = 0$ soit $b = 0$ et $f'(0) = 0$ c'est-à-dire $a = 0$. Maintenant f est la fonction nulle : $F \cap G = \{0\}$. Soit $h \in E$, on remarque que pour $f(x) = h(x) - h(0) - h'(0)x$ la fonction f vérifie $f(0) = 0$ et $f'(0) = 0$ donc $f \in F$. Si on écrit l'égalité différemment, on obtient

$$h(x) = f(x) + h(0) + h'(0)x.$$

On pose $g(x) = h(0) + h'(0)x$ alors la fonction $g \in G$ et $h = f + g$. Cela prouve que toute fonction de E s'écrit comme somme d'une fonction de F et d'une fonction de G : $E = F + G$. Conclusion, on a montré que $E = F \oplus G$.

Définition 4.3.4 *Soit A une K-algèbre, de $3^{\text{ème}}$ loi notée $\star$, $B \in \mathcal{P}(A)$. On dit que B est une* ***sous-algèbre*** *de A si et seulement si :*

$$\begin{cases} B \text{ est un sev du } K\text{ev}A \\ \forall (x, y) \in B^2,\ x \star y \in B \end{cases}$$

Autrement dit, une partie B d'une algèbre A est une sous-algèbre de A si et seulement si

$$\begin{cases} B \neq \emptyset, \\ \forall (x,y) \in B^2,\ x+y \in B, \\ \forall (\lambda, x) \in K \times B,\ \lambda x \in B, \\ \forall (x,y) \in B^2,\ x \star y \in B. \end{cases}$$

4.4 Dépendance et indépendance linéaires

4.4.1 Familles liées, familles libres

1. Combinaisons linéaires

Définition 4.4.1 *Soient E un K-ev, $n \in \mathbb{N}^\star$, $(x_1, \ldots, x_n) \in E^n$. On appelle* ***combinaison linéaire*** *de $x_1, \ldots, x_n$ tout élément x de E tel qu'il existe $(\lambda_1, \ldots, \lambda_n) \in K^n$ tel que*

$$x = \lambda_1 x_1 + \ldots + \lambda_n x_n = \sum_{i=1}^{n} \lambda_i x_i.$$

Plus généralement, si $(x_i)_{i \in I}$ est une famille (éventuellement infinie) d'éléments d'un K-ev E, on appelle combinaison linéaire de la famille $(x_i)_{i \in I}$ tout élément x de E tel qu'il existe une partie finie J de I et une famille $(\lambda_i)_{i \in J}$ d'éléments de K telles que $x = \sum_{i \in J} \lambda_i x_i$. Par convention $\sum_{i \in \emptyset} x_i = 0$.

Proposition 4.4.1 *Soient E un K-ev, $F \in \mathcal{P}(E)$. Pour que F soit un sev de E, il faut et il suffit que F soit non vide et que F soit stable par combinaison linéaire, c'est-à-dire :*

$$\forall (\lambda, \mu) \in K^2,\ \forall (x,y) \in F^2,\ \lambda x + \mu y \in F.$$

Preuve :

(a) Si F est un sev de E alors $F \neq \emptyset$ et, pour tous (λ, μ) de K^2 et (x,y) de F^2, λx et μy sont dans F, puis $\lambda x + \mu y \in F$.

(b) Réciproquement, supposons que $F \neq \emptyset$ et $\forall (\lambda, \mu) \in F^2$, $\lambda x + \mu y \in F$. En choisissant $\mu = 0$ puis $\lambda = \mu = 1$, on conclut que F est un sev de E. ∎

Remarque 4.4.1 Pour qu'une partie F d'un ev E soit un sev de E, il faut et il suffit que :

$$\begin{cases} F \neq \emptyset \\ \forall \lambda \in K, \forall (x,y) \in F^2,\ \lambda x + y \in F. \end{cases}$$

2. Familles liées, familles libres

Définition 4.4.2 *Soient E un K-ev, $n \in \mathbb{N}^\star$, $(x_1, \ldots, x_n) \in E^n$.*

(a) On dit que la famille finie $(x_1, \ldots, x_n)$ est ***liée*** *si et seulement si :*

$$\exists (\lambda_1, \ldots, \lambda_n) \in K^n - \{(0, \ldots, 0)\},\ \sum_{i=1}^{n} \lambda_i x_i = 0.$$

(b) On dit que la famille $(x_1, \ldots, x_n)$ est ***libre*** *si et seulement si elle n'est pas liée c'est-à-dire :*

$$\forall (\lambda_1, \ldots, \lambda_n) \in K^n,\ \left(\sum_{i=1}^{n} \lambda_i x_i = 0 \Rightarrow (\forall i \in \{1, \ldots, n\}, \lambda_i = 0) \right).$$

Plus généralement soit $(x_i)_{i \in I}$ une famille éventuellement infinie d'éléments de E.

(a) On dit que $(x_i)_{i \in I}$ est liée si et seulement s'il existe une sous-famille de $(x_i)_{i \in I}$ qui soit liée, c'est-à-dire si et seulement si'il existe une partie finie J de I telle que $(x_i)_{i \in J}$ soit liée.

(b) On dit que $(x_i)_{i\in I}$ est libre si et seulement si elle n'est pas liée, c'est-à-dire si et seulement si toute sous-famille finie de $(x_i)_{i\in I}$ est libre.

Pour rappeler le corps K utilisé, on utilise parfois l'expression K-libre (respectivement K-lié) au lieu de libre (respectivement lié).

Remarque 4.4.2

(a) Deux vecteurs $x, y \in E - \{0\}$ sont colinéaires si et seulement si (x, y) est lié, c'est-à-dire si et seulement s'il existe $\lambda \in K$ tel que $y = \lambda x$.

(b) Pour qu'une famille (x) à un seul élément soit liée, il faut et il suffit que : $x = 0$.

(c) Pour tout x de E, la famille (x, x) est liée puisque $1x + (-1)x = 0$ avec $(1, -1) \neq (0, 0)$.

(d) Si une famille $(x_i)_{i\in I}$ d'éléments de E est liée, alors toute sur-famille de $(x_i)_{i\in I}$ (c'est-à-dire toute famille éléments de E dont $(x_i)_{i\in I}$ est une sous-famille) est liée. Par exemple, toute famille contenant 0 est liée.

(e) Si une famille $(x_i)_{i\in I}$ d'éléments de E est libre, alors toute sous-famille de $(x_i)_{i\in I}$ est libre.

(f) Si une famille $(x_i)_{i\in I}$ d'éléments de E est libre, alors les x_i $(i \in I)$ sont deux à deux distincts. En effet, soit $(i, j) \in I^2$ tel que $i \neq j$. D'après le point précédent, la famille (x_i, x_j) à deux éléments est libre donc $x_i \neq x_j$.

(g) La liaison ou la liberté d'une famille $(x_i)_{i\in I}$ ne dépend pas de l'ordre des éléments x_i. Autrement dit, si $\sigma : I \to I$ est une permutation de I, la famille $(x_{\sigma(i)})_{i\in I}$ est liée (respectivement libre) si et seulement si la famille $(x_i)_{i\in I}$ est liée (respectivement libre).

La dernière remarque permet la définition suivante :

Définition 4.4.3 *Une partie A de E est libre si et seulement si la famille $(x)_{x\in A}$ est libre.*

Exemple 4.4.1

(a) $E = \mathbb{R}^3$, $n = 2$, $x_1 = (1, 0, 1)$, $x_2 = (2, 1, -1)$. La famille (x_1, x_2) est libre.

(b) $E = \mathbb{R}^3$, $n = 3$, $x_1 = (1, 1)$, $x_2 = (2, 1)$, $x_3 = (-1, 0)$. La famille (x_1, x_2, x_3) est libre puisque $x_1 - x_2 - x_2 = 0$.

(c) $E = \mathbb{R}^{\mathbb{R}}$ et pour $\alpha \in \mathbb{R}$, $\begin{array}{rccc} f_\alpha : \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & e^{\alpha x} \end{array}$, la famille $(f_\alpha)_{\alpha\in\mathbb{R}}$ est libre.

Exercice 81 Soit $\alpha \in \mathbb{R}$ et $f_\alpha : \begin{array}{rcl} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} 1 & \text{si } x = \alpha, \\ 0 & \text{sinon} \end{cases} \end{array}$. Montrer que la famille $(f_\alpha)_{\alpha\in\mathbb{R}}$ est libre.

Correction : À partir de la famille $(f\alpha)_{\alpha\in\mathbb{R}}$ on considère une combinaison linéaire (qui ne correspond qu'à un nombre fini de termes). Soient $\alpha_1, \ldots, \alpha_n$ des réels distincts, on considère la famille (finie) : $(f_\alpha)_{i=1,\ldots,n}$. Supposons qu'il existe des réels $\lambda_1, \ldots, \lambda_n$ tels que $\sum_{i=1}^{n} \lambda_i f_{\alpha_i} = 0$. Cela siginfie que, quel que soit $x \in \mathbb{R}$, $\sum_{i=1}^{n} \lambda_i f_{\alpha_i}(x) = 0$. En particulier, pour $x = \alpha_j$, l'égalité devient $\lambda_j = 0$ car $f_{\alpha_i}(\alpha_j)$ vaut 0 si $i \neq j$ et 1 si $i = j$. En appliquant le raisonnement ci-dessus pour $j = 1$ jusque $j = n$ on obtient $\lambda_j = 0$, $j = 1, \ldots, n$. Donc la famille $(f_\alpha)_\alpha$ est une famille libre.

4.4.2 Sous-espace engendré par une partie

Définition 4.4.4 *Soient E un K-ev, $A \in \mathcal{P}(E)$. On appelle* ***sev engendré par*** *A, et on note $Vect(A)$, l'intersection de tous les sev de E contenant A :*

$$Vect(A) = \bigcap_{\substack{F \in V(E) \\ F \supset A}} F.$$

Proposition 4.4.2 *Soient E un K-ev, $A \in \mathcal{P}(E)$.*

1. *$Vect(A)$ est le plus petit sev (au sens de l'inclusion) de E contenant A.*
2. *– Si $A \neq \emptyset$, alors $Vect(A)$ est l'ensemble des combinaisons linéaires d'éléments de A.*
   – $Vect(\emptyset) = \{0\}$.

Preuve :

1. – D'après la proposition (4.3.2), $Vect(A)$ est un sev de E en tant qu'intersection de sev de E.
   – Par la défintion de $Vect(A)$ on a $A \subset Vect(A)$.
   – Soit F un sev de E contenant A, et il est inclus dans tout sev de E contenant A.
2. Le singleton $\{0\}$ est à l'évidence le plus petit sev contenant $\emptyset$.
   Supposons que $A \neq \emptyset$ et notons C l'ensemble des combinaisons linéaires d'élements de A :

$$C = \left\{ x \in E, \exists n \in \mathbb{N}^\star, \exists (a_1, \ldots, a_n) \in A^n, \exists (\lambda_1, \ldots, \lambda_n) \in K^n,\ x = \sum_{i=1}^{n} \lambda_i a_i \right\}.$$

   Montrons que C est le plus petit sev de E contenant A.

   (a) Il est clair que $C \neq \emptyset$.

   Soit $(x, y) \in C^2$. Il existe $n \in \mathbb{N}^\star$, $(a_1, \ldots, a_n) \in A^n$, $(\lambda_1, \ldots, \lambda_n) \in K^n$ tels que $\sum_{i=1}^{n} \lambda_i a_i$ et $p \in \mathbb{N}^\star$, $(b_1, \ldots, b_p) \in A^p$, $(\mu_1, \ldots, \mu_p) \in K^p$ tels que $y = \sum_{j=1}^{p} \mu_j b_j$. En notant $c_k = \begin{cases} a_k & \text{si } 1 \leq k \leq n \\ b_{k-n} & \text{si } n+1 \leq k \leq n+p \end{cases}$ et $\nu_k = \begin{cases} \lambda_k & \text{si } 1 \leq k \leq n \\ \mu_{k-n} & \text{si } n+1 \leq k \leq n+p \end{cases}$, on a $\begin{cases} \forall k \in \{1, \ldots, n+p\},\ c_k \in A \\ x + y = \sum_{i=1}^{n} \lambda_i a_i + \sum_{j=1}^{p} \mu_j b_j = \sum_{k=1}^{n+p} \nu_k c_k \end{cases}$ donc $x + y \in C$. On montre de même $\forall \lambda \in K$, $\forall x \in C$, $\lambda x \in C$. Ainsi C est un sev de E.

   (b) Comme tout élément de A est combinaison linéaire d'éléments de A (il suffit d'écrire $a = 1a$), C contient A.

   (c) Soient G un sev de E contenant A et $x \in C$. Il existe $n \in \mathbb{N}^\star$, $(a_1, \ldots, a_n) \in A^n$, $(\lambda_1, \ldots, \lambda_n) \in K^n$ tels que $x = \sum_{i=1}^{n} \lambda_i a_i$. Comme G contient A et que G est un sev, on déduit $x \in G$, ce qui montre $C \subset G$.

   Ceci établit que C est le plus petit sev de E contenant A, et finalement $C = Vect(A)$. ∎

En particulier, le sev engendré par un singleton $\{x\}$ (où $x \in E$) est Kx, c'est-à-dire $\{\lambda x, \lambda \in K\}$.

Définition 4.4.5 *Soient E un K-ev, $(x_i)_{i \in I}$ une famille d'éléments de E. On appelle sev engendré par $(x_i)_{i \in I}$ et on note $Vect((x_i)_{i \in I})$ le sev engendré par la partie $\{x_i ; i \in I\}$ de E.*

En particulier, le sev de E engendré par une famille finie non vide $(x_1, \ldots, x_n)$ d'éléments de E est $\left\{ \sum_{i=1}^{n} \lambda_i x_i, (\lambda_1, \ldots, \lambda_n) \in K^n \right\}$ c'est-à-dire l'ensemble des combinaisons linéaires de $x_1, \ldots, x_n$.

Proposition 4.4.3 *Soient E un K-ev, $A, B \in \mathcal{P}(E)$. On a :*

1. $A \subset B \Rightarrow Vect(A) \subset Vect(B)$,
2. *A est un sev de E si et seulement si $Vect(A) = A$,*
3. $Vect(Vect(A)) = Vect(A)$,
4. $Vect(A \cup B) = Vect(A) + Vect(B)$.

Preuve : Les démonstrations de 1., 2. et 3. sont immédiates. Montrons 4.
$\left\{ \begin{array}{l} A \subset A \cup B \\ B \subset A \cup B \end{array} \right. \Rightarrow \left\{ \begin{array}{l} Vect(A) \subset Vect(A \cup B) \\ Vect(B) \subset Vect(A \cup B) \end{array} \right. \Rightarrow Vect(A) + Vect(B) \subset Vect(A \cup B).$
Réciproquement soit $x \in Vect(A \cup B)$. Il existe $n \in \mathbb{N}^\star$, $(c_1, \ldots, c_n) \in (A \cup B)^n$, $(\lambda_1, \ldots, \lambda_n) \in K^n$ tels que $x = \sum_{i=1}^{n} \lambda_i c_i$. En groupant les termes de A d'une part, ceux de B d'autre part, on en déduit qu'il existe $a \in Vect(A)$, $b \in Vect(B)$ tels que $x = a + b$. Ceci montre $Vect(A \cup B) \subset Vect(A) + Vect(B)$. ■

Exercice 82 Soient dans $\mathbb{R}^4$ les vecteurs $\vec{e_1}(1, 2, 3, 4)$ et $\vec{e_2} = (1, -2, 3, -4)$. Peut-on déterminer x et y pour que $(x, 1, y, 1) \in Vect\{\vec{e_1}, \vec{e_2}\}$? Et pour que $(x, 1, 1, y) \in Vect\{\vec{e_1}, \vec{e_2}\}$?
Correction :

1. $(x, 1, y, 1) \in Vect\{e_1, e_2\}$
   $\Leftrightarrow \exists \lambda, \mu \in \mathbb{R},\ (x, 1, y, 1) = \lambda(1, 2, 3, 4) + \mu(1, -2, 3, -4)$
   $\Leftrightarrow \exists \lambda, \mu \in \mathbb{R},\ (x, 1, y, 1) = (\lambda, 2\lambda, 3\lambda, 4\lambda) + (\mu, -2\mu, 3\mu, -4\mu)$
   $\Leftrightarrow \exists \lambda, \mu \in \mathbb{R},\ (x, 1, y, 1) = (\lambda + \mu, 2\lambda - 2\mu, 3\lambda + 3\mu, 4\lambda - 4\mu)$
   $\Rightarrow \exists \lambda, \mu \in \mathbb{R},\ 1 = 2(\lambda - \mu)$ et $1 = 4(\lambda - \mu) \Rightarrow \exists \lambda, \mu \in \mathbb{R}\ \lambda - \mu = \dfrac{1}{2}$ et $\lambda - \mu = \dfrac{1}{4}$
   ce qui est impossible (quels que soient x et y). Donc on ne peut pas trouver de tels x et y.
2. $(x, 1, 1, y) \in Vect\{e_1, e_2\}$
   $\Leftrightarrow \exists \lambda, \mu \in \mathbb{R},\ (x, 1, 1, y) = (\lambda + \mu, 2\lambda - 2\mu, 3\lambda + 3\mu, 4\lambda - 4\mu)$
   $\Rightarrow \exists \lambda, \mu \in \mathbb{R},\ 1 = 2(\lambda - \mu)$ et $1 = 3(\lambda + \mu) \Rightarrow \exists \lambda, \mu \in \mathbb{R},\ \lambda - \mu = \dfrac{1}{2}$ et $\lambda + \mu = \dfrac{1}{3}$ ce qui implique nécessairement que $\lambda = \dfrac{5}{12}$ et $\mu = -\dfrac{1}{12}$ et donc $(x, y) = \left(\dfrac{1}{3}, 2\right)$.

Exercice 83 Peut-on déterminer des réels x et y pour que le vecteur $v = (-2, x, y, 3)$ appartienne au sev engendré dans $\mathbb{R}^4$ par le système (e_1, e_2) où $e_1 = (1, -1, 1, 2)$ et $e_2 = (-1, 2, 3, 1)$?
Correction : $u \in Vect(e_1, e_2)$ est équivalent à l'existence de deux réels λ, μ tels que $v = \lambda e_1 + \mu e_2$. Alors $(-2, x, y, 3) = \lambda(1, -1, 1, 2) + \mu(-1, 2, 3, 1)$ est équivalent à

$$\left\{ \begin{array}{rcl} -2 & = & \lambda - \mu \\ x & = & -\lambda + 2\mu \\ y & = & \lambda + 3\mu \\ 3 & = & 2\lambda + \mu \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} \lambda & = & 1/3 \\ \mu & = & 7/3 \\ x & = & 13/3 \\ y & = & 22/3 \end{array} \right.$$

Le couple qui convient est donc $(x, y) = (13/3, 22/3)$.

4.4.3 Familles génératrices, bases

Définition 4.4.6 *Soient E un K-ev, G une famille d'éléments de E. On dit que G est une* ***famille génératrice*** *de E (ou que G engendre E) si et seulement si $Vect(G) = E$.*

Proposition 4.4.4 *Si $G = (x_1, \ldots, x_n)$ est une famille finie d'éléments d'un K-ev, G engendre E si et seulement si*

$$\forall x \in E,\ \exists (\lambda_1, \ldots, \lambda_n) \in K^n,\ x = \sum_{i=1}^{n} \lambda_i x_i.$$

Une partie G d'un K-ev est dite génératrice de E si et seulement si $Vect(G) = E$. Ceci revient à ce que la famille $(x)_{x \in G}$ des éléments de G engendre E au sens de la définition (4.4.6).

Définition 4.4.7 *On dit qu'une famille B d'éléments d'un K-ev est une* ***base*** *de E si et seulement si B est libre et génératrice de E.*

La proposition suivante est immédiate :

Proposition 4.4.5 *Une famille finie $B = (e_1, \ldots, e_n)$ d'éléments d'un K-ev E est une base de E si et seulement si :*

$$\forall x \in E,\ \exists ! (x_1, \ldots, x_n) \in K^n,\ x = \sum_{i=1}^{n} x_i e_i.$$

Si E admet une base finie $B = (e_1, \ldots, e_n)$, pour tout x de E, les éléments $x_1, \ldots, x_n$ définis ci-dessus s'appellent les ***coordonnées*** *(ou* ***composantes) de*** *x* ***dans*** *(ou* ***sur) la base*** *B. x_i s'appelle la* ***i-ème coordonnée*** *(ou* ***composante) de*** *x* ***dans*** *(ou* ***sur la base*** *B).*

Exercice 84

1. Montrer que les vecteurs $x_1 = (0, 1, 1)$,$x_2 = (1, 0, 1)$ et $x_3 = (1, 1, 0)$ forment une base de $\mathbb{R}^3$. Trouver dans cette base les composantes du vecteur $x = (1, 1, 1)$.
2. Donner, dans $\mathbb{R}^3$, un exemple de famille libre, qui n'est pas génératrice.
3. Donner, dans $\mathbb{R}^3$, un exemple de famille génératrice, mais qui n'est pas libre.

Correction :

1. Il est très simple de montrer que la famille (x_1, x_2, x_3) est libre et génératrice. Le vecteur x vérifie $x = \frac{1}{2}x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3$. Donc, dans la base (x_1, x_2, x_3), les coordonnées de x sont $\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$.
2. Par exemple la famille $\{(1, 0, 0), (0, 1, 0)\}$ est libre dans $\mathbb{R}^3$ mais pas génératrice.
3. La famille $\{(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 1)\}$ est génératrice dans $\mathbb{R}^3$ mais pas libre.

Exercice 85 Déterminer pour quelles valeurs de $t \in \mathbb{R}$ les vecteurs $(1, 0, t)$, $(1, 1, t)$ et $(t, 0, 1)$ forment une base de $\mathbb{R}^3$.
Correction : C'est une base pour $t \neq \pm 1$.

4.5 Théorie de la dimension

E désigne dans ce chapitre un K-ev.

4.5.1 Espaces vectoriels de dimension finie

Proposition 4.5.1 *Soient* $(n,p) \in \mathbb{N}^{\star 2}$, $(x_1,\ldots,x_{n+p}) \in E^{n+p}$,

$$F = (x_1,\ldots,x_p),\ F' = (x_1,\ldots,x_p,x_{p+1},\ldots,x_{n+p}).$$

1. *Si F' est libre, alors F est libre.*
2. *Si F est génératrice de E alors F' est génératrice de E.*

Preuve :

1. On rappelle (remarque (4.4.2)) que si une famille $(x_i)_{i\in I}$ d'éléments de E est libre alors toute sous-famille de $(x_i)_{i\in I}$ est libre.
2. Soit $x \in E$. Puisque F engendre E, il existe $(\lambda_1,\ldots,\lambda_p) \in K^p$ tel que $x = \sum_{i=1}^{p} \lambda_i x_i$. En notant $\lambda_{p+1} = \ldots = \lambda_{n+p} = 0$, on a alors $x = \sum_{i=1}^{n+p} \lambda_i x_i$. Ceci montre que F' engendre E. ■

La proposition précédente se généralise à des familles quelconques (non nécessairement finies) :

1. Si $F \subset F'$ et si F' est libre, alors F est libre.
2. Si $F \subset F'$ et si F est génératrice de E alors F' est génératrice de E (où $F \subset F'$ signifie que F est une sous-famille de F'.)

Proposition 4.5.2 *Soient $n \in \mathbb{N}^\star$, $(x_1,\ldots,x_{n+1}) \in E^{n+1}$, $F = (x_1,\ldots,x_n)$, $F' = (x_1,\ldots,x_n,x_{n+1})$.*

1. *Si F est libre et si $x_{n+1} \notin Vect(F)$ alors F' est libre.*
2. *Si F' est génératrice de E et si $x_{n+1} \in Vect(F)$ alors F est génératrice de E.*

Preuve :

1. Soit $(\lambda_1,\ldots,\lambda_{n+1}) \in K^{n+1}$ tel que $\sum_{i=1}^{n+1} \lambda_i x_i = 0$. Si $\lambda_{n+1} \neq 0$ alors on déduit $x_{n+1} = \sum_{i=1}^{n} \left(-\lambda_{n+1}^{-1}\lambda_i\right) x_i \in Vect(F)$ d'où une contradiction. Donc $\lambda_{n+1} = 0$ d'où $\sum_{i=1}^{n} \lambda_i x_i = 0$ puis $\lambda_1 = \ldots = \lambda_n = 0$ puisque F est libre.
2. Soit $x \in E$. Puisque F' est génératrice de E, il existe $(\lambda_1,\ldots,\lambda_{n+1}) \in K^{n+1}$ tel que $x = \sum_{i=1}^{n+1} \lambda_i x_i$. Comme $x_{n+1} \in Vect(F)$, il existe $(\mu_1,\ldots,\mu_n) \in K^n$ tel que $x_{n+1} = \sum_{i=1}^{n} \mu_i x_i$. On en déduit $x = \left(\sum_{i=1}^{n} \lambda_i x_i\right) + \lambda_{n+1}x_{n+1} = \sum_{i=1}^{n} (\lambda_i + \lambda_{n+1}\mu_i)x_i \in Vect(F)$, ce qui montre que F est génératrice de E. ■

La proposition précédente de généralise à des familles quelconques (non nécesairement finies) :

1. Si F est libre et si $x \notin Vect(F)$ alors $F \cup \{x\}$ est libre.
2. Si $F \cup \{x\}$ est génératrice de E et si $x \in Vect(F)$ alors F est génératrice de E.

Théorème 4.5.1 *Théorème de l'échange*
Soient $G = (x_1,\ldots,x_p)$, $L = (y_1,\ldots,y_r)$ deux familles finies d'éléments de E. Si G est génératrice de E et si L est libre alors

1. $r \leq p$.
2. *On peut remplacer d'au moins une façon r des vecteurs de G par ceux de L pour obtenir une famille génératrice de E.*

Preuve :

- Puisque G engendre E, il existe $(\lambda_{1,1}, \ldots, \lambda_{1,p}) \in K^p$ tel que $\sum_{j=1}^{p} \lambda_{1,j} x_j$. On a $(\lambda_{1,1}, \ldots, \lambda_{1,p}) \neq (0, \ldots, 0)$, car sinon $y_1 = 0$, ce qui contredit la liberté de L. Quitte à permuter $x_1, \ldots, x_p$ (et $\lambda_{1,1}, \ldots, \lambda_{1,p}$), on peut se ramener à $\lambda_{1,1} \neq 0$. Alors, en notant $G_1 = (y_1, x_2, \ldots, x_p)$, on a $x_1 = \lambda_{1,1}^{-1} - \sum_{j=2}^{p} \lambda_{1,1}^{-1} \lambda_{1,j} x_j \in Vect(G_1)$. Puisque G engendre E, $(y_1, x_2, \ldots, x_p)$ engendre E (d'après 2. dans la proposition (4.5.1)), puis, comme $x_1 \in Vect(G_1)$, G_1 engendre E (d'après 2. dans la proposition (4.5.2)). On a ainsi remplacé un des vecteurs de G par y_1 pour obtenir une famille génératrice $G_1 = (y_1, x_2, \ldots, x_p)$.
- Soit $s \in \mathbb{N}^\star$ tel que $s \leq \min(p-1, r-1)$. Supposons (après une éventuelle permutation de $x_1, \ldots, x_p$) que la famille $G_s = (y_1, \ldots, y_s, x_{s+1}, \ldots, x_p)$ soit génératrice de E. Il existe $(\lambda_{s+1,s+1}, \lambda_{s+1,p}) \in K^p$ tel que $y_{s+1} = \sum_{j=1}^{s} \lambda_{s+1,j} y_j + \sum_{j=s+1}^{p} \lambda_{s+1,j} x_j$. Si $(\lambda_{s+1,s+1}, \ldots, \lambda_{s+1,p}) = (0, \ldots, 0)$ alors $y_{s+1} = \sum_{j=1}^{s} \lambda_{s+1,j} y_j$, ce qui contredit la liberté de $(y_1, \ldots, y_{s+1})$ (donc de L). Quitte à permuter $x_{s+1}, \ldots, x_p$ (et $\lambda_{s+1,s+1}, \ldots, \lambda_{s+1,p}$) on peut se ramener à $\lambda_{s+1,s+1} \neq 0$. Alors, en notant
$$G_{s+1} = (y_1, \ldots, y_s, y_{s+1}, x_{s+2}, \ldots, x_p),$$
la même argumentation que précédemment montre que G_{s+1} est génératrice de E. On a ainsi remplacé des vecteurs de G par des vecteurs de L pour obtenir une famille génératrice.
- Supposons que $r > p$. Avec les notations précédentes, $G_p = (y_1, \ldots, y_p)$ est génératrice de E, donc $y_{p+1} \in Vect(G_p)$ ce qui contredit la liberté de $(y_1, \ldots, y_{p+1})$ donc de L. Donc $r \leq p$ et $G_r = (y_1, \ldots, y_r, x_{r+1}, \ldots, x_p)$ est génératrice de E. ■

Définition 4.5.1 *Un K-ev E est dit de **dimension finie** si et seulement si E admet au moins une famille génératrice finie.*

Exemple 4.5.1

1. $\{0\}$ et $K^n (n \in \mathbb{N}^\star)$ sont des K-ev de dimension finie.
2. $K[X]$ est un K-ev qui n'est pas de dimension finie car si $K[X]$ admettait une famille génératrice finie $(P_1, \ldots, P_n)$ alors pour tout P de $K[X]$, on aurait $deg(P) \leq \max_{1 \leq i \leq n} (deg(P_i))$ ce qui est impossible.

Théorème 4.5.2 *Soit E un K-ev de dimension finie alors :*

1. *E admet au moins une base finie.*
2. *Toutes les bases de E sont finies et ont le même cardinal.*

*Le cardinal d'une base de E est appelé la **dimension** de E et est notée $dim_K(E)$ ou plus simplement $dim(E)$.*

Preuve :

1. Puisque E est de dimension finie, E admet au moins une famille génératrice $G = (x_1, \ldots, x_p)$. Si G est libre alors G est une base finie de E.

Supposons que G soit liée, il existe $(\lambda_1, \ldots, \lambda_p) \in K^p - \{(0, \ldots, 0)\}$ tel que $\sum_{i=1}^{p} \lambda_i x_i = 0$. Quitte à permuter $x_1, \ldots, x_p$ et $(\lambda_1, \ldots, \lambda_p)$, on peut se ramener à $\lambda_p \neq 0$ d'où, en notant $G_1 = (x_1, \ldots, x_{p-1})$ on a $x_p = \sum_{i=1}^{p-1} \lambda_p^{-1} \lambda_i x_i \in Vect(G_1)$. D'après la proposition (4.5.2), G_1 est génératrice de E.
On réitère le procédé. S'il existe $r \in \{1, \ldots, p\}$ tel que la famille génératrice $G_r = (x_1, \ldots, x_{p-r})$ soit libre alors G_r est une base de E. Sinon $G_1 = (x_1)$ est liée et génératrice d'où $E = \{0\}$ et $\emptyset$ est une base finie de E.

2. D'après 1., E admet au moins une base finie B, notons n le nombre d'éléments de B. Soit B' une autre base de E. Si B' est infinie ou finie de cardinal $> n$ alors B' contient au moins une famille finie libre L ayant $n+1$ éléments. Mais B est génératrice à n éléments et L libre à $n+1$ éléments, ce qui contredit le résultat 1. du théorème de l'échange. Donc B' est finie de cardinal $\leq n$. De même, B' étant libre à n éléments et B' génératrice, le résultat 1. du théorème de l'échange montre que $n \leq Card(B')$. Finalement B' est finie et admet n éléments. ■

Remarque 4.5.1

- La preuve précédente établit plus précisément que toute famille génératrice finie d'un K-ev de dimension finie contient au moins une base.
- On dit qu'un sev F d'un ev E est de dimension finie si et seulement si l'ev F est de dimension finie.
- On dit parfois qu'un ev qui n'est pas de dimension finie est de dimension infinie.
- Pour tout ev E de dimension finie, $dim(E) = 0 \Leftrightarrow E = \{0\}$.
- La dimension d'un K-ev de dimension finie dépend du corps K. Par exemple, $dim_{\mathbb{C}}(\mathbb{C}^2) = 2$ mais $dim_{\mathbb{R}}(\mathbb{C}^2) = 4$.

Exercice 86 Soient $\vec{e_1}(0,1,-2,1)$, $\vec{e_2}(1,0,2,-1)$, $\vec{e_3}(3,2,2,-1)$, $\vec{e_4}(0,0,1,0)$ et $\vec{e_5}(0,0,0,1)$ des vecteurs de $\mathbb{R}^4$. Les propositions suivantes sont-elles vraies ou fausses ? Jusitifer les réponses.

1. $Vect\{\vec{e_1}, \vec{e_2}, \vec{e_3}, \vec{e_4}, \vec{e_5}\} = Vect\{(1,1,0,0), (-1,1,-4,2)\}$.
2. $(1,1,0,0) \in Vect\{\vec{e_1}, \vec{e_2}\} \cap Vect\{\vec{e_2}, \vec{e_3}, \vec{e_4}\}$.
3. $dim(Vect\{\vec{e_1}, \vec{e_2}\} \cap Vect\{\vec{e_2}, \vec{e_3}, \vec{e_4}\}) = 1$.
4. $Vect\{\vec{e_1}, \vec{e_2}\} + Vect\{\vec{e_2}, \vec{e_3}, \vec{e_4}\} = \mathbb{R}^4$. $Vect\{\vec{e_4}, \vec{e_5}\}$ est un sous-espace vectoriel de supplémentaire $Vect\{\vec{e_1}, \vec{e_2}, \vec{e_3}\}$ dans $\mathbb{R}^4$.

Correction : Faisons d'abord une remarque qui va simplifier les calculs : on a $\vec{e_3} = 2\vec{e_1} + 3\vec{e_2}$. Donc $Vect\{\vec{e_1}, \vec{e_2}, \vec{e_3}\} = Vect\{\vec{e_1}, \vec{e_2}\}$ qui est un espace de dimension 2 puisque $\vec{e_1}$ et $\vec{e_2}$ ne sont pas colinéaires. On a également $Vect\{\vec{e_1}, \vec{e_2}, \vec{e_3}\} = Vect\{\vec{e_2}, \vec{e_3}\}$.

1. VRAI. $Vect\{(1,1,0,0), (-1,1,4,2)\}$ est inclus dans $Vect\{\vec{e_1}, \vec{e_2}, \vec{e_3}\}$ car $(1,1,0,0) = \vec{e_1} + \vec{e_2}$ et $(-1,1,-4,2) = -\vec{e_1} + \vec{e_2}$. Comme ils sont de même dimension, ils sont égaux.
2. VRAI. On a $(1,1,0,0) = \vec{e_1} + \vec{e_2}$ donc $(1,1,0,0) \in Vect\{\vec{e_1}, \vec{e_2}\}$ or $Vect\{\vec{e_1}, \vec{e_2}\} = Vect\{\vec{e_2}, \vec{e_3}\} \subset Vect\{\vec{e_2}, \vec{e_3}, \vec{e_4}\}$. Donc $(1,1,0,0) \in Vect\{\vec{e_1}, \vec{e_2}\} \cap Vect\{\vec{e_2}, \vec{e_3}, \vec{e_4}\}$.
3. FAUX. Toujours d'après la même relation, on a $Vect\{\vec{e_1}, \vec{e_2}\} \cap Vect\{\vec{e_2}, \vec{e_3}, \vec{e_4}\} = Vect\{\vec{e_1}, \vec{e_2}\}$ donc $dim(Vect\{\vec{e_1}, \vec{e_2}\} \cap Vect\{\vec{e_2}, \vec{e_3}, \vec{e_4}\}) = 2$.
4. FAUX. Encore une fois, la relation nous donne $Vect\{\vec{e_1}, \vec{e_2}\} + Vect\{\vec{e_2}, \vec{e_3}, \vec{e_4}\} = Vect\{\vec{e_1}, \vec{e_2}, \vec{e_4}\}$ or 3 vecteurs ne peuvent engendrer $\mathbb{R}^4$ qui est de dimension 4.
5. VRAI. Il suffit de faire les calculs et montrer que l'intersection des deux sev est $\{0\}$ et leur somme est $\mathbb{R}^4$.

Exercice 87 On considère les vecteurs $v_1 = (1,0,0,1)$ et $v_2 = (0,0,1,0)$, $v_3 = (0,1,0,0)$, $v_4 = (0,0,0,1)$ et $v_5 = (0,1,0,1)$ dans $\mathbb{R}^4$.

1. $Vect\{v_1, v_2\}$ et $Vect\{v_3\}$ sont-ils supplémentaires dans $\mathbb{R}^4$?
2. Même question pour $Vect\{v_1, v_3, v_4\}$ et $Vect\{v_2, v_5\}$.

Correction :

1. Non. Ces deux sous-espaces vectoriels ne peuvent engendrer $\mathbb{R}^4$ car il n'y a pas assez de vecteurs. Premier type de raisonnement : on montre que $Vect\{v_1, v_2\} + Vect\{v_3\} = Vect\{v_1, v_2, v_3\}$ mais 3 vecteurs ne peuvent engendrer l'espace $\mathbb{R}^4$ de dimension 4. Autre type de raisonnement : on trouve un vecteur de $\mathbb{R}^4$ qui n'est pas dans $Vect\{v_1, v_2\} + Vect\{v_3\}$, il suffit pour s'en convaincre de faire le calcul avec $(0,0,0,1)$.
2. Non. Ces deux espaces ne sont pas supplémentaires car il y a trop de vecteurs. Ils engendrent tout mais l'intersection n'est pas triviale. En effet on remarque assez vite que $v_5 = v_3 + v_4$ est dans l'intersection. On peut aussi obtenir ce résultat en résolvant un système.

Théorème 4.5.3 *(théorème de la base incomplète)*
Soient E un K-ev de dimension finie, $L = (y_1, \ldots, y_r)$ une famille libre dans E.

1. *Forme forte :*
   Soit $B = (e_1, \ldots, e_n)$ une base de E. Il y a au moins une façon de compléter L par $n - r$ vecteurs de B pour obtenir une base de E.
2. *Forme faible :*
   Il y a au moins une façon de compléter L par $n - r$ vecteurs de E pour obtenir une base de E.

Preuve : pour la forme forte, il suffit d'appliquer le théorème de l'échange à la famille génératrice B et à la famille L.
La forme faible se déduit trivialement de la forme forte et de l'existence d'au moins une base finie de E. ■

Proposition 4.5.3 *Soient E un K-ev de dimension finie, $n = dim(E)$.*

1. *Toute famille libre de E est finie et a au plus n éléments.*
2. *Toute famille de E ayant au moins $n + 1$ éléments est liée.*
3. *Toute famille génératrice de E a au moins n éléments.*

Preuve : D'après le théorème (4.5.2), E admet au moins une base $B = (e_1, \ldots, e_n)$.

1. Soit L une famille libre dans E. Si L est infinie ou finie de cardinal $> n$, il y a alors contradiction avec le résultat 1. du théorème de l'échange, puisque B est génératrice.
2. se déduit de 1. par contraposition.
3. Soit G une famille génératrice de E. D'après le résultat 1. du théorème de l'échange, et puisque B est libre, G a au moins n éléments. ■

Proposition 4.5.4 *Soient E un K-ev de dimension finie, $n = dim(E)$, F est une famille finie d'éléments de E. Deux quelconques des trois propriétés suivantes entraînent la troisième :*

1. *F a n éléments.*
2. *F est libre.*
3. *F est génératrice de E.*

Preuve :

- Montrons que (1. et 2.)⇒ 3.
  Supposons $Card(F) = n$ et F libre. E admet au moins une base $B = (e_1, \ldots, e_n)$. D'après le théorème de l'échange, comme B est génératrice et F est libre, on peut remplacer d'au moins une façon n vecteurs de B par ceux de F pour obtenir une famille génératrice. Mais comme B a n éléments, la famille génératrice obtenue est F.
- Montrons que (1. et 3.)⇒ 2.
  Supposons $Card(F) = n$ et F génératrice. Raisonnons par l'absurde : supposons F liée. Il existe $(\lambda_1, \ldots, \lambda_n) \in K^n - \{(0, \ldots, 0)\}$ tel que $\sum_{i=1}^{n} \lambda_i x_i = 0$. Quitte à permuter $x_1, \ldots, x_n$ (et $\lambda_1, \ldots, \lambda_n$), on peut se ramener à $\lambda_n \neq 0$ d'où $x_n = -\sum_{i=1}^{n-1} \lambda_n^{-1} \lambda_i x_i \in Vect(x_1, \ldots, x_{n-1})$. D'après l'affirmation 2. de la proposition (4.5.2), $(x_1, \ldots, x_{n-1})$ est génératrice de E, ce qui contredit le point 3. de la proposition (4.5.3). Ceci prouve que F est libre.
- Montrons que (2. et 3.)⇒ 1.
  Cela résulte simplement du théorème (4.5.2). ■

Exercice 88 Soit $F = \mathbb{R}_4[X]$ l'espace vectoriel réel des polynômes réels de degré inférieur ou égal à 4.

1. Peut-on compléter la famille $(2, 1 + X^2)$ en une base de F ? Si oui, donner une telle base.
2. Peut-on compléter la famille $((X + 1)^2, (X - 1)^2, X)$ en une base de F ? Si oui, donner une telle base.

Correction :

1. OUI. La famille est bien libre (le lemme des degrés nous dit que quand on a une famille finie de polynômes de degrés 2 à 2 distincts, cette famille est libre). On peut alors compléter en choisissant des vecteurs dans un système générateur, par exemple la base canonique $(1, X^2, X^3, X^4)$. D'après le lemme des degrés, le système à 5 vecteurs $(2, X, 1 + X^2, X^3, X^4)$ est libre, dans F qui est de dimension 5, donc c'est une base.
2. NON. En effet $(X + 1)^2 - (X - 1)^2 = 4X$ donc la famille $((X + 1)^2, (X - 1)^2, X)$ n'est pas libre et ne peut être complétée en une base.

Exercice 89 Pour $E = \mathbb{R}^4$, dire si les familles de vecteurs suivantes peuvent être complétées en une base de E. Si oui, le faire.

1. (u, v, w) avec $u = (1, 2, -1, 0)$, $v = (0, 1, -4, 1)$ et $w = (2, 5, -6, 1)$;
2. (u, v, w) avec $u = (1, 0, 2, 3)$, $v = (0, 1, 2, 3)$ et $w = (1, 2, 0, 3)$;
3. (u, v) avec $u = (1, -1, 1, -1)$ et $v = (1, 1, 1, 1)$.

Correction :

1. On remarque que $w = 2u + v$. La famille (u, v, w) est liée. On ne peut pas la compléter en une base de E.
2. On va d'abord vérifier que la famille (u, v, w) est libre. Une équation du type $au + bv + cw = 0$ est équivalente au système

$$\begin{cases} a + c &= 0 \\ b + 2c &= 0 \\ 2a + 2b &= 0 \\ a + b + c &= 0 \end{cases}$$

La première et la dernière équations donnent immédiatement $b = 0$, d'où on tire $a = 0$ et $c = 0$. La famille (u, v, w) est libre. D'après le théorème de la base incomplète, on peut la compléter en une base de $\mathbb{R}^4$ à l'aide de vecteurs de n'importe quelle famille génératrice de $\mathbb{R}^4$. Ici, il suffit d'un vecteur (la famille compte déjà 3 éléments, et on travaille dans un espace de dimension 4), et on va choisir la famille génératrice la plus simple, la base canonique notée $(e_1, \ldots, e_4)$. Montrons que (u, v, w, e_2) est libre. En effet, si $au + bv + cw + de_2 = 0$, on obtient le système

$$\begin{cases} a + c &= 0 \\ b + 2c + d &= 0 \\ 2a + 2b &= 0 \\ a + b + c &= 0 \end{cases}$$

Comme précédemment, la première et la dernière équations donnent $b = 0$, d'où $a = 0$ d'après la deuxième, puis $c = 0$ et $d = 0$. La famille (u, v, w, e_2) est donc une famille libre de 4 éléments dans un espace de dimension 4. C'est une base de $\mathbb{R}^3$. Remarquons que le choix de e_2 n'est pas fait au hasard : on l'a choisi plutôt que e_1 afin de ne pas perturber la première et la dernière équations du système, et donc d'obtenir facilement $b = 0$.

3. Les vecteurs u et v sont non proportionnels. La famille (u, v) est donc libre et on peut la compléter à l'aide de deux (cette fois) vecteurs de la base canonique. On vérifie d'abord que (u, v, e_1) est libre. En effet, si $au + bv + ce_1 = 0$, on trouve le système

$$\begin{cases} a + b + c &= 0 \\ -a + b &= 0 \\ a + b &= 0 \\ -a + b &= 0 \end{cases}$$

De la première et la troisième équations, on trouve $c = 0$, d'où l'on tire facilement $a = b = c = 0$. Expliquons maintenant le choix du deuxième vecteur pour compléter. La deuxième et la quatrième équations sont identiques. Elles apportent donc la même information. Pour obtenir vraiment un système de quatre équations différentes, il suffit de perturber l'une des deux, par exemple la deuxième. C'est pourquoi on va montrer que (u, v, e_1, e_2) est une famille libre. En effet, si $au + bv + ce_1 + de_2 = 0$, alors on trouve le système

$$\begin{cases} a + b + c &= 0 \\ -a + b + d &= 0 \\ a + b &= 0 \\ -a + b &= 0 \end{cases}$$

Comme précédemment, on a $c = 0$, et les deuxième et quatrième équations montrent que $d = 0$. On en déduit alors facilement que $a = b = c = d = 0$. La famille (u, v, e_1, e_2) est libre. Elle comporte 4 éléments dans un espace de dimension 4 : c'est une base de $\mathbb{R}^4$.

4.5.2 Sev d'un ev de dimension finie

Proposition 4.5.5 *Soit E un K-ev de dimension finie. Tout sev F de E est de dimension finie, et $dim(F) \leq \dim(E)$.*

Preuve Le résultat est évident lorsque $F = \{0\}$.
Supposons $F = \{0\}$. Il existe $x_1 \in F$ tel que $x_1 \neq 0$. Notons $L_1 = (x_1)$ qui est libre. Si L_1 engendre F alors F est de dimension finie et $dim(F) = 1$. Sinon, il exite $x_2 \in F$ tel que $x_2 \notin Vect(L_1)$. D'après 2. dans (4.5.2), la famille $L_2 = (x_1, x_2)$ est libre et on réitère le raisonnement. Soit $p \in \mathbb{N}^\star$, supposons définis $x_1, \ldots, x_p$ dans F tels que $L_p = (x_1, \ldots, x_p)$ soit libre. Si L_p engendre F alors F est de dimension finie et $dim(F) = p$. Sinon il existe $x_{p+1} \in F$ tel que $x_{p+1} \notin Vect(L_p)$ et la famille $L_{p+1} = (x_1, \ldots, x_{p+1})$ est libre dans F. En notant $n = dim(E)$, comme toute famille de E ayant au moins $n + 1$ éléments est liée, il existe $p \in \{1, \ldots, n\}$ tel que L_p engendre F. Ainsi F est de dimension finie et $dim(F) \leq n$. ∎

Définition 4.5.2 *On appelle **droite vectorielle** (respectivement **plan vectoriel**) tout ev ou sev de dimension 1 (respectivement 2). Une droite vectorielle est engendrée (on dit aussi dirigée) par n'importe lequel de ses vecteurs $\neq 0$.*
*Dans un ev de dimension finie n ($n \geq 1$), on appelle **hyperplan** tout sev de dimension $n-1$.*

Proposition 4.5.6 *Soient E un K-ev de dimension finie $n = dim(E)$, F un sev de E, $p = dim(F)$.*

1. *F admet au moins un supplémentaire dans E.*
2. *Tout supplémentaire de F dans E est dimension $n-p$.*

Preuve :

1. D'après le théorème (4.5.2) et la proposition précédente, E admet au moins une base $B = (e_1, \ldots, e_n)$, F admet au moins une base $C = (f_1, \ldots, f_p)$ et $p \leq n$. D'après le théorème de la base incomplète (forme forte), quitte à permuter dans B et dans C, la famille $B' = (f_1, \ldots, f_p, e_{p+1}, \ldots, e_n)$ est une base de E.
   Notons $G = Vect(e_{p+1}, \ldots, e_n)$ et montrons que G est un supplémentaire de F dans E.
   - Soit $x \in E$. Il existe $(\lambda_1, \ldots, \lambda_n) \in K^n$ tel que $x = \sum_{i=1}^{p} \lambda_i f_i + \sum_{i=p+1}^{n} \lambda_i e_i$ d'où $x \in F + G$. Ceci montre que $F + G = E$.
   - Soit $x \in F \cap G$. Il existe $(\lambda_1, \ldots, \lambda_n) \in K^n$ tel que $x = \sum_{i=1}^{p} \lambda_i x_i = \sum_{i=p+1}^{n} \lambda_i e_i$. On a alors $x = \sum_{i=1}^{p} \lambda_i f_i + \sum_{i=p+1}^{n} (-\lambda_i) e_i = 0$ d'où, puisque B' est libre, $\lambda_1 = \ldots, \lambda_p = \lambda_{p+1} = \ldots = \lambda_n = 0$ soit $x = 0$. Ceci montre que $F \cap G = \{0\}$. Finalement, G est un supplémentaire de F dans E.
2. Soit H un supplémentaire de F dans E. D'après la proposition (4.5.5), H est de dimension finie. D'après la proposition (4.5.2), F (respectivement H) admet au moins une base $(f_1, \ldots, f_p)$ (respectivement $(h_{p+1}, \ldots, h_q)$). Montrons que $(f_1, \ldots, f_p, h_{p+1}, \ldots, h_q)$ est une base de E.
   - Soit $(\lambda_1, \ldots, \lambda_q) \in K^q$ tel que $x = \sum_{i=1}^{p} \lambda_i f_i + \sum_{i=p+1}^{q} \lambda_i h_i = 0$. Alors $\sum_{i=1}^{p} \lambda_i f_i = -\sum_{i=p+1}^{q} \lambda_i h_i \in F \cap H = \{0\}$ donc $\sum_{i=1}^{p} \lambda_i f_i = 0$ et $\sum_{i=p+1}^{q} \lambda_i h_i = 0$ d'où $\lambda_1 = \ldots = \lambda_p = \lambda_{p+1} = \ldots = \lambda_q = 0$ puisque $(f_1, \ldots, f_p)$ et $(h_{p+1}, \ldots, h_q)$ sont libres. Ceci établit que $(f_1, \ldots, f_p, h_{p+1}, \ldots, h_q)$ est libre.
   - Soit $x \in E$. Puisque $E = F + H$, il existe $(f, h) \in F \times H$ tel que $x = f + h$. Puis il existe $(\lambda_1, \ldots, \lambda_p) \in K^p$ et $(\lambda_{p+1}, \ldots, \lambda_q) \in K^{q-p}$ tels que $f = \sum_{i=1}^{p} \lambda_i f_i$ et $h = \sum_{i=p+1}^{q} \lambda_i h_i$.

   On obtient $x = \sum_{i=1}^{p} + \sum_{i=p+1}^{q} \lambda_i h_i$ ce qui montre que $(f_1, \ldots, f_p, h_{p+1}, \ldots, h_q)$ engendre E. ∎

Remarque 4.5.2

$$\text{Si} \begin{cases} E \text{ est un } K\text{-ev de dimension finie} \\ F, G \text{ sont deux sev de } E \text{ supplémentaires dans } E \\ B(\text{respectivement } C) \text{ est une base de } F \text{ (respectivement } G) \end{cases} \quad \text{alors } B \cup C \text{ est une base de } E$$

Corollaire 4.5.1 *Soient E un K-ev de dimension finie, F et G deux sev de E en somme directe. On a alors*

$$dim(F \oplus G) = dim(F) + dim(G).$$

Preuve : il suffit d'utiliser la proposition (4.5.6), appliquée à $F \oplus G$ au lieu de E. ■

Corollaire 4.5.2 *Soient E un K-ev de dimension finie, F et G deux sev de E.*
Si $\begin{cases} F \subset G \\ dim(F) = dim(G) \end{cases}$ *alors* $F = G$.

Preuve : F admet au moins un supplémentaire H dans G, et $dim(H) = dim(G) - dim(F) = 0$, d'où $H = \{0\}$, $G = F + H = F$. ■

Exercice 90 Soient E et F les sev de $\mathbb{R}^3$ engendrés respectivement par les vecteurs $\{(2,3,-1),(1,-1,2)\}$ et $\{(3,7,0),(5,0,-7)\}$. Montrer que E et F sont égaux.
Correction : Pour que deux ensembles X et Y soient égaux, il faut et il suffit que $X \subset Y$ et $Y \subset X$. Dans le cas des ev de dimension finie, la situation est un peu plus simple : pour que $E = F$ il faut et il suffit que $F \subset E$ et $dim(E) = dim(F)$. Appliquons ce critère : E est engendré par deux vecteurs donc $dim(E) \leq 2$. Les deux vecteurs $(2,3,-1)$ et $(1,-1,-2)$ sont linéairement indépendants donc $dim(E) \geq 2$ c'est-à-dire $dim(E) = 2$. Un raisonnement identique montre que $dim(F) = 2$. Enfin, les égalités $(3,7,0) = 2(2,3,-1) - (1,-1,-2)$ et $(5,0,-7) = (2,3,-1) + 3(1,-1,-2)$ montrent que $F \subset E$ c'est-à-dire $E = F$.

Théorème 4.5.4 *Formule de Grassmann (Hermann GRASSMANN 1809-1877) ou formule de la dimension Soit E un K-ev de dimension finie. On a a pour tous sev F, G de E :*

$$dim(F + G) = dim(F) + dim(G) - dim(F \cap G).$$

Preuve : D'après la proposition (4.5.6), $F \cap G$ admet au moins un supplémentaire F' dans F.

1. Montrons que F' et G sont en somme directe et que $F' \oplus G = F + G$.
   . $F' \subset F$ d'où $F' \cap = (F' \cap F) \cap G = F' \cap (F \cap G) = \{0\}$.
   . $F + G = (F' + (F \cap G)) + G = F' + ((F \cap G) + G) = F' + G$.
2. D'après le corollaire (4.5.1), $\begin{cases} dim(F + G) = dim(F' \oplus G) = dim(F') + dimG \\ dim(F) = dim(F' \oplus (F \cap G)) = dim(F') + dim(F \cap G) \end{cases}$ d'où la relation voulue. ■

Exercice 91 Autour du théorème des quatre dimensions.
Soient E un espace vectoriel de dimension finie, F et G deux sev de E. Montrer que deux quelconques des trois propriétées suivantes entraînent la troisième :

1. $F \cap G = \{0\}$;
2. $F + G = E$;
3. $dim(F) + dim(G) = dim(E)$.

Correction : Tout repose sur la formule des quatre dimensions $dim(F+G) = dim(F)+dim(G)-dim(F \cap G)$ et sur la propriété : si H est un sev de E tel que $dim(H) = dim(E)$, alors $H = E$.

- Si 1. et 2. sont vraies, alors $dim(F+G) = dim(F)+dim(G)-dim(F \cap G) = dim(F)+dim(G)$ tandis que $E = F + G$ implique $dim(E) = dim(F) + dim(G)$. 3. est donc vérifié.
- Si 1. et 3. sont vraies, alors $dim(F + G) = dim(F) + dim(G) - dim(F \cap G) = dim(E) - 0 = dim(E)$. Ainsi, $F + G$ est un sev de E de même dimension que E : $F + G = E$.
- Si 2. et 3. sont vraies, alors $dim(E) = dim(F + G) = dim(F) + dim(G) - dim(F \cap G) = dim(E) - dim(F \cap G)$. On en déduit que $dim(F \cap G) = 0$ et donc que $F \cap G = \{0\}$.

Exercice 92 Soient E un espace vectoriel de dimension finie n, et F, G deux sous-espaces vectoriels de E de même dimension $p < n$. Montrer que F et G ont un supplémentaire commun, c'est-à-dire qu'il existe un sous-espace H de E tel que $F \oplus H = G \oplus H = E$.
Correction : On raisonne par récurrence descendante sur $p \in \{0, \ldots, n-1\}$. Traitons d'abord le cas $p = n-1$. On sait que $F \cup G \neq E$. En effet, si $F = G$ ce n'est pas le cas, et si $F \neq G$, alors on n'a ni $F \subset G$, ni $G \subset F$ (les deux espaces ont même dimension, une inclusion entraînerait l'égalité), et donc $F \cup G$ n'est pas un espace vectoriel. En particulier, il n'est pas égal à E. On peut choisir a tel que $a \notin F \cup G$. Alors $F \cap vect(a) = \{0\}$ et $G \cap vect(a) = \{0\}$. F et $vect(a)$ (respectivement G et $vect(a)$) sont en somme directe, et puisque $dim(F \oplus vect(a)) = n$ (respectivement $dim(G \oplus vect(a)) = n$), on a $F \oplus vect(a) = G \oplus vect(a) = E$. $vect(a)$ est le supplémentaire commun recherché. Supposons maintenant le rsultat prouv pour $p+1$, et prouvons-le pour p. Comme précédemment, on peut trouver $a \notin F \cup G$ et comme précédemment, F et $vect(a)$ (respectivement G et $vect(a)$) sont en somme directe. Posons $F_1 = F \oplus vect(a)$ et $G_1 = G \oplus vect(a)$. Alors F_1 et G_1 ont même dimension, égale à $p+1$. D'après l'hypothèse de récurrence, ils possèdent un supplémentaire commun que l'on note H_1. Mais alors, F et $vect(a) \oplus H_1$ sont en somme directe. En effet, si $x \in F \cap vect(a) \oplus H_1$, on a $x = f = \lambda a + h$, avec $f \in F$, $\lambda \in K$ et $h \in H_1$. On en déduit $h = f - \lambda_a \in H_1 \cap F_1 = \{0\}$ et donc $h = 0$. Puisque $F \cap vect(a) = \{0\}$, on obtient également $f = \lambda = 0$, et par suite $x = 0$. Ainsi, si on pose $H = vect(a) \in H_1$, alors H et F sont en somme directe. De même, H et G sont en somme directe, et donc F et G ont un supplémentaire commun. Ceci achève la preuve par rcurrence.

4.5.3 Produit cartésien d'ev de dimensions finies

Proposition 4.5.7 *Soient E, F deux K-ev de dimension finie. Alors $E \times F$ est de dimension finie et :*

$$dim(E \times F) = dim(E) + dim(F).$$

Preuve : D'après le théorème (4.5.2), E et F admettent des bases finies $(e_1, \ldots, e_n)$ et $(f_1, \ldots, f_p)$ respectivement où $n = dim(E)$ et $p = dim(F)$. Montrons que $B = ((e_1, 0), \ldots, (e_n, 0), (0, f_1), \ldots, (0, f_p))$ est une base de $E \times F$.

1. Soit $(\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_p) \in H^{n+p}$ tel que $\sum_{i=1}^{n} \lambda_i(e_i, 0) + \sum_{j=1}^{p} \mu_j(0, f_j) = 0$. On a alors $\left(\sum \lambda_i e_i, \sum_{j=1}^{p} \mu_j f_j\right) = (0,0)$ d'où $\sum_{i=1}^{n} \lambda_i e_i = 0$ et $\sum_{j=1}^{p} \mu_j f_j = 0$ et donc, $\lambda_1 = \ldots = \lambda_n = \mu_1 = \ldots = \mu_p = 0$, puisque $(e_1, \ldots, e_n)$ et $(f_1, \ldots, f_p)$ sont libres. Ceci montre que B est libre.
2. Soit $(x, y) \in E \times F$. Puisque $(e_1, \ldots, e_n)$ et $(f_1, \ldots, f_p)$ engendrent respectivement les sev de E et F, il existe $(\lambda_1, \ldots, \lambda_n) \in K^n$ et $(\mu_1, \ldots, \mu_p) \in K^p$ tels que $\sum_{i=1}^{n} \lambda_i e_i$ et $\sum_{j=1}^{p} \mu_j f_j$. On a alors $(x, y) = \left(\sum_{i=1}^{n} \lambda_i e_i, \sum_{j=1}^{p} \mu_j f_j\right) = \sum_{i=1}^{n} \lambda_i(e_i, 0) + \sum_{j=1}^{p} \mu_j(0, f_j)$. Ceci montre que B engendre E.

Ainsi, B est une base de $E \times F$ donc $E \times F$ est de dimension finie et $dim(E \times F) = card(B) = n + p = dim(E) + dim(F)$. ∎

Corollaire 4.5.3 *Soient $n \in \mathbb{N}^\star$, $E_1, \ldots, E_n$ des K-ev de dimension finie. Alors $\prod_{i=1}^{n} E_i$ est de dimension finie et*

$$dim\left(\prod_{i=1}^{n} E_i\right) = \sum_{i=1}^{n} dim(E_i).$$

Preuve : récurrence immédiate à partir de la proposition précédente. ■

En particulier, pour tout $n \in \mathbb{N}^\star$, K^n est un K-ev de dimension finie et $dim(K^n) = n$. La famille $(e_1, \ldots, e_n)$ d'éléments de K^n définie par $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ où le « 1 »est à la i-ième place, $1 \leq i \leq n$ est une base de K^n appelée **base canonique** de K^n.

4.5.4 Rang d'une famille finie de vecteurs

Définition 4.5.3 *Soient E un K-ev, F une famille finie d'éléments de E. On appelle **rang** de F, et on note $rg(F)$ l'entier naturel*

$$rg(F) = dim(Vect(F))$$

Proposition 4.5.8 *Pour toutes familles finies F, F' d'éléments de E :*

1. $F \subset F' \Rightarrow rg(F) \leq rg(F')$,
2. $\max(rg(F), rg(F')) \leq rg(F \cup F') \leq rg(F) + rg(F')$.

Preuve :

1. $F \subset F' \Rightarrow Vect(F) \subset Vect(F') \Rightarrow dim(Vect(F)) \leq dim(Vect(F'))$.
2. – $\left\{ \begin{array}{l} F \subset F \cup F' \\ F' \subset F \cup F' \end{array} \right. \Rightarrow \left\{ \begin{array}{l} rg(F) \leq rg(F \cup F') \\ rg(F') \leq rg(F \cup F') \end{array} \right. \Rightarrow \max(rg(F), rg(F')) \leq rg(F \cup F')$.
   – $rg(F \cup F') = dim(Vect(F \cup F')) = dim(Vect(F) + Vect(F')) \leq dim(Vect(F)) + dim(Vect(F')) = rg(F) + rg(F')$, en utilisant 4. de la proposition (4.4.3). ■

Proposition 4.5.9 *Soient E un K-ev, F une famille finie d'éléments de E.*

1. *Le rang de F est le plus grand cardinal des sous-familles libres de F.*
2. *F est libre si et seulement si $Card(F) = rg(F)$.*

Preuve :

1. – Puisque F est finie, $Vect(F)$ est de dimension finie. D'après la remarque (4.5.1), il existe une sous-famille B de F qui soit une base de $Vect(F)$ donc telle que $Card(B) = rg(F)$.
   – Soit L une sous-famille libre de F. D'après le point 1. de la proposition (4.5.3), $Card(L) \leq dim(Vect(F)) = rg(F)$.
2. – Si F est libre, d'après 1., $rg(F) = card(F)$.
   – Réciproquement, si $card(F) = rg(F)$, comme F engendre $Vect(F)$, d'après la proposition (4.5.4), F est une base de $Vect(F)$ et est donc libre. ■

Exemple 4.5.2 Soient $K = \mathbb{R}$, $E = \mathbb{R}^3$, $F = (v_i)_{1<i<4}$ où :

$$v_1 = (1, -1, 1),\ v_2 = (-1, 1, -1),\ v_3 = (0, 1, 1),\ v_4 = (1, 0, 2).$$

Comme (v_1, v_3) est libre et que $v_2 = -v_1$ et $v_4 = v_1 + v_3$, on a $rg(F) = 2$.

Chapitre 5

Les applications linéaires

5.1 Introduction

Après avoir étudié dans le chapitre précédent la structure d'espace vectoriel, on envisage les applications linéaires, c'est-à-dire les applications linéaires entre espaces vectoriels qui conservent l'addition et la loi externe. Une attention particulière sera portée aux applications linéaires entre ev de dimension finie, intervenant souvent et pour lesquelles on dispose de résultats remarquables. Les applications linéaires en dimension finie se traduiront dans le chapitre suivant par des matrices.

5.2 Généralités

5.2.1 Définitions, propriétés, exemples

Définition 5.2.1

1. *Soient E, F deux K-ev, une application $f : E \to F$ est dite* ***linéaire*** *(ou* ***K-linéaire*** *ou, est un* ***morphisme de K-ev****) si et seulement si :*
$$\begin{cases} \forall (x,y) \in E^2, & f(x+y) = f(x) + f(y) \\ \forall \lambda \in K, \forall x \in E, & f(\lambda x) = \lambda f(x) \end{cases}$$
On note $\mathcal{L}(E,F)$ (ou $\mathcal{L}_K(E,F)$) l'ensemble des applications linéaires de E dans F.
2. *Soient E un K-ev, $f : E \to E$ une application. On dit que f est un* ***endomorphisme*** *de E si et seulement si f est linéaire.*
On note $\mathcal{L}(E)$ (ou $\mathcal{K}_E$) l'ensemble des endomorphismes de E.

On a donc $\mathcal{L}(E) = \mathcal{L}(E,E)$.

Remarque 5.2.1 Pour toute fonction $f \in \mathcal{L}(E,F)$, $f(0) = 0$ car $f(0) = f(0+0) = f(0) + f(0)$.

Définition 5.2.2

1. *Soient E, F deux K-ev, $f : E \to F$ une application. On dit que f est un* ***isomorphisme*** *de E sur F si et seulement si f est linéaire et bijective.*
2. *Soient E un K-ev, $f : E \to E$ une application. On dit que f est un* ***automorphisme*** *de E si et seulement si f est linéaire et bijective.*

On note $\mathcal{GL}(E)$ (ou $\mathcal{GL}_K(E)$) l'ensemble des automorphismes de l'ev E.

Définition 5.2.3 *Soit E un K-ev. On appelle* ***forme linéaire*** *sur E toute application linéaire φ de E dans K. On note $E^\star$ l'ensemble des formes linéaires sur E ; $E^\star$ est appelé le* ***dual*** *de E.*

On a donc $E^\star = \mathcal{L}(E, K)$.

Proposition 5.2.1 *Soient E et F deux K-ev, $f : E \to F$ une application ; f est linéaire si et seulement si*

$$\forall \lambda \in K, \forall (x, y) \in E^2, f(\lambda x + y) = \lambda f(x) + f(y).$$

Preuve :

1. Si f est linéaire alors, pour tout $(\lambda, x, y) \in K \times E \times E$:
$$f(\lambda x + y) = f(\lambda x) + f(y) = \lambda f(x) + f(y).$$
2. Réciproquement, si la condition précédente est satisfaite, alors :
   - en prenant $\lambda = 1$, on obtient $f(x + y) = f(x) + f(y)$, et donc $f(0) = 0$,
   - en prenant $y = 0$, on obtient $f(\lambda x) = \lambda f(x)$ et donc f est linéaire. ■

Proposition 5.2.2 *Soient E, F deux K-ev, $f \in \mathcal{L}(E, F)$. On a, pour tous n de $\mathbb{N}^\star$, $(\lambda_1, \ldots, \lambda_n)$ de K^n, $(x_1, \ldots, x_n)$ de E^n :*

$$f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = \sum_{i=1}^{n} \lambda_i f(x_i).$$

Preuve : Récurrence sur n. La propriété est immédiate pour $n = 1$; pour $n = 2$, $f(\lambda_1 x_1 + \lambda_2 x_2) = f(\lambda_1 x_1) + f(\lambda_2 x_2) = \lambda_1 f(x_1) + \lambda_2 f(x_2)$.
Si la propriété est vraie pour un n de $\mathbb{N}^\star$, alors, pour tous $(\lambda_1, \ldots, \lambda_{n+1})$ de K^{n+1} et $(x_1, \ldots, x_{n+1})$ de E^{n+1} :

$$f\left(\sum_{i=1}^{n+1} \lambda_i x_i\right) = f\left(\sum_{i=1}^{n} \lambda_i x_i + \lambda_{n+1} x_{n+1}\right) = f\left(\sum_{i=1}^{n} \lambda_i x_i\right) + f(\lambda_{n+1} x_{n+1}) =$$
$$f\left(\sum_{i=1}^{n} \lambda_i x_i\right) + \lambda_{n+1} f(x_{n+1}) = \sum_{i=1}^{n+1} \lambda_i f(x_i).$$

■

On en déduit le corollaire suivant :

Corollaire 5.2.1 *Soient E un K-ev de dimension finie, F un K-ev, $B = (e_1, \ldots, e_n)$ une base de E, $f \in \mathcal{L}(E, F)$, $x \in E$, $(x_1, \ldots, x_n)$ les composantes de x dans la base B (c'est-à-dire : $x = \sum_{i=1}^{n} x_i e_i$). On a alors :*

$$f(x) = \sum_{i=1}^{n} x_i f(e_i).$$

Exemple 5.2.1

1. **Homothéties**. Soit E un K-ev. Pour tout α de K, on appelle **homothétie (vectorielle) de rapport** α l'application $h_\alpha : \begin{array}{ccc} E & \to & E \\ x & \mapsto & \alpha x \end{array}$. Il est clair que $h_\alpha \in \mathcal{L}(E)$.
   En particulier : $h_0 = 0$, $h_1 = Id_E$.
2. **Projecteurs**. Soient E un K-ev, F, G deux sev de E supplémentaires dans E ($E = F \oplus G$). Pour tout x de E, il existe $(x', x'') \in F \times G$ unique tel que $x = x' + x''$. L'application $p : \begin{array}{ccc} E & \to & E \\ x & \mapsto & x' \end{array}$ est un endomorphisme de E. En effet, si $\lambda \in K$ et $(x, y) \in E^2$, il existe $(x', x'') \in F \times G$ et $(y', y'') \in F \times G$ tels que $x = x' + x''$ et $y = y' + y''$, d'où :

$$\begin{cases} \lambda x + y = \lambda(x' + x'') + (y' + y'') = (\lambda x' + y') + (\lambda x'' + y'') \\ (\lambda x' + y', \lambda x'' + y'') \in F \times G. \end{cases}$$

et donc $p(\lambda x + y) = \lambda x' + y' = \lambda p(x) + p(y)$.
L'application $\begin{array}{rcl} p : E & \to & E \\ x & \mapsto & x' \end{array}$ est appelée le **projecteur sur F parallèlement à G.**
Il est clair que l'application $\begin{array}{rcl} q : E & \to & E \\ x & \mapsto & x'' \end{array}$ est le projecteur sur G parallèlement à F.
On a $q = e - p$, c'est-à-dire $\forall x \in E$, $q(x) = x - p(x)$.

3. **Symétries**. Soient E un K-ev, F, G deux sev de E supplémentaires dans E : $E = F \oplus G$. Notons p le projecteur sur F parallèlement à G. L'application $s = 2p - e$ définie par :

$$\begin{array}{rcl} s : E & \to & E \\ x & \mapsto & 2p(x) - x \end{array}$$

est un endomorphisme de E, appelé **symétrie par rapport à F parallèlement à G.**

4. **Inclusion canonique**. Soient E un K-ev, F un sev de E. l'**inclusion** (ou **injection canonique**)

$$\begin{array}{rcl} i_{F,E} : F & \to & E \\ x & \mapsto & x \end{array}$$

est linéaire.

5. **Projections canoniques**. Soient $n \in \mathbb{N}^\star$, $E_1, \ldots, E_n$ des K-ev. Pour chaque i de $\{1, \ldots, n\}$, la **i-ème projection canonique**

$$\begin{array}{rcl} p_{r_i} : E_1 \times \ldots \times E_n & \to & E_i \\ (x_1, \ldots, x_n) & \mapsto & x_i \end{array}$$

est linéaire.

6. **Opérateur de dérivation**. Soient I un intervalle de $\mathbb{R}$, non vide et non réduit à un point, $D^1(I, \mathbb{R})$ le $\mathbb{R}$-ev des applications de I dans $\mathbb{R}$ dérivables sur I. L'application

$$\begin{array}{rcl} D : D^1(I, \mathbb{R}) & \to & \mathbb{R}^I \\ f & \mapsto & f' \end{array}$$

est linéaire.

7. **Intégration**. Soient $(a, b) \in \mathbb{R}^2$ tel que $a \leq b$, $\mathcal{CM}$ le $\mathbb{R}$-ev des applications de $[a, b]$ dans $\mathbb{R}$ continues par morceaux. L'application

$$\begin{array}{rcl} \mu : \mathcal{CM} & \to & \mathbb{R} \\ f & \mapsto & \displaystyle\int_a^b f \end{array}$$

est linéaire.

Définition 5.2.4

1. *Soient A, B deux K-algèbres (la 3ème loi étant notée multiplicativement) ; une application $f : A \to B$ est appelée **morphisme d'algèbres** si et seulement si :*

$$\begin{cases} \forall (x, y) \in A^2, & f(x + y) = f(x) + f(y) \\ \forall \lambda \in K, \forall x \in A, & f(\lambda x) = \lambda f(x) \\ \forall (x, y) \in A^2, & f(xy) = f(x) f(y). \end{cases}$$

2. *Soient A une K-algèbre, $f : A \to A$ une application. On dit que f est un **endomorphisme de l'algèbre** A si et seulement si f est un morphisme d'algèbres de A dans A.*

Exercice 93 (non corrigé) Déterminer si les applications f_i suivantes (de E_i dans F_i) sont linéaires :

1. $f_1 : (x, y) \in \mathbb{R}^2 \mapsto (2x + y, x - y) \in \mathbb{R}^2$,
2. $f_2 : (x, y, z) \in \mathbb{R}^3 \mapsto (xy, x, y) \in \mathbb{R}^3$,
3. $f_3 : (x, y, z) \in \mathbb{R}^3 \mapsto (2x + y + z, y - z, x + y) \in \mathbb{R}^3$,
4. $f_4 : P \in \mathbb{R}[X] \mapsto P' \in \mathbb{R}[X]$,
5. $f_5 : P \in \mathbb{R}_3[X] \mapsto P' \in \mathbb{R}_3[X]$,
6. $f_6 : P \in \mathbb{R}_3[X] \mapsto (P(-1), P(0), P(1)) \in \mathbb{R}^3$,
7. $f_7 : P \in \mathbb{R}[X] \mapsto P - (X - 2)P' \in \mathbb{R}[X]$.

5.2.2 Noyau, Image

Proposition 5.2.3 *Soient E, F deux K-ev, $f \in \mathcal{L}(E, F)$.*

1. *Pour tout sev F_1 de F, l'image réciproque $f^{-1}(F_1)$ est un sev de E.*
2. *Pour tout sev E_1 de E, l'image directe $f(E_1)$ est un sev de F.*

Preuve :

1. – $f^{-1}(F_1) \neq \emptyset$, $0 \in f^{-1}(F_1)$ car $f(0) = 0 \in F_1$.
   – Soient $\lambda \in K$, $(x, y) \in (f^{-1}(F_1))^2$. On a $(f(x), f(y)) \in (F_1)^2$ d'où : $f(\lambda x + y) = \lambda f(x) + f(y) \in F_1$ et donc $\lambda x + y \in f^{-1}(F_1)$.
2. – $f(E_1) \neq \emptyset$, $0 \in f(E_1)$ car $0 = f(0)$.
   – Soient $\lambda \in K$, $(x', y') \in (f(E_1))^2$. Il existe $(x, y) \in (E_1)^2$ tel que $x' = f(x)$ et $y' = f(y)$. On a alors $\lambda x' + y' = \lambda f(x) + f(y) = f(\lambda x + y) \in f(E_1)$. ■

On rappelle qu'un sev V d'un ev est dit **stable** par un endomorphisme f de E si et seulement si $f(V) \subset V$.

Définition 5.2.5 *Soient E, F deux K-ev, $f \in \mathcal{L}(E, F)$. On appelle **noyau** de f, et on note $Ker(f)$, le sev de E défini par :*

$$Ker(f) = f^{-1}(\{0\}) = \{x \in E, f(x) = 0\}.$$

*On appelle **image** de f, et on note $Im(f)$, le sev de F défini par :*

$$Im(f) = f(E) = \{y \in F, \exists x \in E, y = f(x)\}.$$

Proposition 5.2.4 *Soient E, F deux K-ev, $f \in \mathcal{L}(E, F)$.*

1. *f est injective si et seulement si $Ker(f) = \{0\}$.*
2. *f est surjective si et seulement si $Im(f) = F$.*

Preuve :

1. – Supposons f injective, et soit $x \in Ker(f)$. Alors $f(x) = 0 = f(0)$, d'où puisque f est injective, $x = 0$. Ainsi $Ker(f) = \{0\}$.
   – Réciproquement, supposons $Ker(f) = \{0\}$ et soit $(x, y) \in E^2$ tel que $f(x) = f(y)$. Alors $f(x - y) = f(x) - f(y) = 0$ donc $x - y \in Ker(f) = \{0\}$ d'où $x = y$. Ceci montre que f est injective.
2. f surjective $\Leftrightarrow \forall y \in F, \exists x \in E, y = f(x) \Leftrightarrow f(E) = F \Leftrightarrow Im(f) = F$. ■

Exercice 94 E_1 et E_2 étant deux sous-espaces vectoriels de dimensions finies d'un espace vectoriel E, on définit l'application $f : E_1 \times E_2 \to E$ par $f(x_1, x_2) = x_1 + x_2$.

1. Montrer que f est linéaire.

2. Déterminer le noyau et l'image de f.

Correction :

1. Évident.
2. Par définition de f et ce qu'est la somme de deux sous-espaces vectoriels, l'images est $Im(f) = E_1 + E_2$. Pour le noyau, $Ker(f) = \{(x_1, x_2), f(x_1, x_2) = 0\} = \{(x_1, x_2), x_1 + x_2 = 0\} = \{(x, -x), x \in E_1 \cap E_2\}$. De plus, par l'application $x \mapsto (x, -x)$, $Kerf(f)$ est isomorphe à $E_1 \cap E_2$.

Exercice 95 Soient f et g deux endomorphismes de E tels que $f \circ g = g \circ f$. Montrer que $Ker(f)$ et $Im(f)$ sont stables par g.
Correction : Montrons que $g(Ker(f)) \subset Ker(f)$. Soit $y \in g(Ker(f))$. Il existe $x \in Ker(f)$ tel que $y = g(x)$. Montrons que $y \in Ker(f)$: $f(y) = f(g(x)) = f \circ g(x) = g \circ f(x) = g(0) = 0$. On peut suivre un raisonnement similaire pour l'image.

Exercice 96 Donner des exemples d'applications linéaires de $\mathbb{R}^2$ dans $\mathbb{R}^2$ vérifiant :

1. $Ker(f) = Im(f)$,
2. $Ker(f)$ inclus strictement dans $Im(f)$,
3. $Im(f)$ inclus strictement dans $Ker(f)$.

Correction :

1. Par exemple, si $f(x, y) = (0, x)$ alors $Ker(f) = Im(f) = \{0\} \times \mathbb{R} = \{(0, y), y \in \mathbb{R}\}$.
2. Par exemple l'identité $f(x, y) = (x, y)$. (Un petit exercice consiste à montrer que les seules applications possibles sont les applications bijectives.)
3. L'application nulle : $f(x, y) = (0, 0)$ (qui est la seule possible).

Exercice 97 Soient E et F deux espaces vectoriels et $f \in \mathcal{L}(E, F)$. Soit G un supplémentaire de $Ker(f)$ dans E. Montrer que G et $Im(f)$ sont isomorphes.
Correction : On définit $g : G \to Im(f)$ par $g(x) = f(x)$. Alors :

- g est linéaire : c'est une conséquence directe du fait que f est linéaire.
- g est injective : si $x \in Ker(g)$ alors $x \in G$ et $x \in Ker(f)$. Comme G et $Ker(f)$ sont supplémentaires, on a $x = 0$.
- g est surjective : prenons $y \in Im(f)$. Alors $y = f(x)$ avec $x \in E$. Décomposons x en $x = u + v$ avec $u \in G$ et $v \in Ker(f)$. Alors $y = f(x) = f(u) + f(v) = f(u) = g(u)$ avec $u \in G$, ce qui prouve bien que g est surjective.

Ainsi, g définit un isomorphisme de G sur $Im(f)$.

5.2.3 Applications linéaires et familles de vecteurs

Dans ce chapitre E, F désignent deux K-ev, $f \in \mathcal{L}(E, F)$, $\mathcal{F} = (x_1, \ldots, x_n)$ est une famille finie d'éléments de E.

Proposition 5.2.5 *Pour toute f de $\mathcal{L}(E, F)$ et toute famille finie $\mathcal{F}$ d'éléments de E :*

$$f(Vect(\mathcal{F})) = Vect(f(\mathcal{F})).$$

Preuve :

1. Soit $y \in f(Vect(\mathcal{F}))$. Il existe $x \in Vect(\mathcal{F})$ tel que $y = f(x)$, puis il existe $(\lambda_i)_{1<i<n} \in K^n$ tel que $x = \sum_{i=1}^{n} \lambda_i x_i$. On a alors $y = f(x) = f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = \sum_{i=1}^{n} \lambda_i f(x_i) \in Vect(f(\mathcal{F}))$. Ceci montre que $f(Vect(\mathcal{F})) \subset Vect(f(\mathcal{F}))$.

2. L'inclusion réciproque se montre de façon analogue. ■

Corollaire 5.2.2 *Si $f \in \mathcal{L}(E,F)$ est surjective et si $\mathcal{F}$ engendre E, alors $f(\mathcal{F})$ engendre F.*

Preuve : $F = f(E) = f(Vect(\mathcal{F})) = Vect(f(\mathcal{F}))$. ■

Proposition 5.2.6 *Soient $f \in \mathcal{L}(E,F)$ et $\mathcal{F}$ une famille d'éléments de E.*

1. *Si $\mathcal{F}$ est liée alors $f(\mathcal{F})$ est liée.*
2. *Si $f(\mathcal{F})$ est libre alors $\mathcal{F}$ est libre.*

Preuve :

1. Puisque $\mathcal{F}$ est liée, il existe $(\lambda_1, \ldots, \lambda_n) \in K^n - \{(0,\ldots,0)\}$ tel que $\sum_{i=1}^{n} \lambda_i x_i = 0$. On a alors : $\sum_{i=1}^{n} \lambda_i f(x_i) = f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = f(0) = 0$, et donc $f(\mathcal{F})$ est liée.
2. Se déduit de 1. par contraposition.

Proposition 5.2.7 *Soient $f \in \mathcal{L}(E,F)$, $\mathcal{F}$ une famille d'éléments de E. Si f est injective et si $\mathcal{F}$ est libre alors $f(\mathcal{F})$ est libre.*

Preuve : Soit $(\lambda_1, \ldots, \lambda_n) \in K^n$ tel que $\sum_{i=1}^{n} \lambda_i f(x_i) = 0$. Alors $f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = \sum_{i=1}^{n} \lambda_i f(x_i) = 0$ d'où, puisque f est injective, $\sum_{i=1}^{n} \lambda_i x_i = 0$. Enfin, comme $\mathcal{F}$ est libre, $\forall i \in \{1,\ldots,n\}$, $\lambda_i = 0$. ■

Proposition 5.2.8 *Soient E un K-ev de dimension finie, F un K-ev, $f \in \mathcal{L}(E,F)$. Les propriétés suivantes sont deux à deux équivalentes :*

1. *f est bijective.*
2. *Pour toute base $\mathcal{B}$ de E, $f(\mathcal{B})$ est une base de F.*
3. *Il existe une base $\mathcal{B}$ de E telle que $f(\mathcal{B})$ soit une base de F.*

Preuve :
1. $\Rightarrow$ 2. : On suppose f bijective. Soit $\mathcal{B}$ une base de E. Puisque f est surjective et $\mathcal{B}$ est génératrice de E, $f(\mathcal{B})$ est génératrice de F. Puisque f est injective et $\mathcal{B}$ libre, $f(\mathcal{B})$ est libre d'après la proposition précédente.
2. $\Rightarrow$ 3. : Cette implication résulte de l'existence d'une base de E (cf théorème (4.5.2), chapitre 4 - espaces vectoriels).
3. $\Rightarrow$ 1. : Supposons qu'il existe une base $\mathcal{B} = (e_1, \ldots, e_n)$ de E telle que $f(\mathcal{B}) = (f(e_1), \ldots, f(e_n))$ soit une base de F.

- Soit $x \in Ker(f)$. Il existe $(x_1, \ldots, x_n) \in K^n$ tel que $x = \sum_{i=1}^{n} x_i e_i$. On a alors $0 = f(x) = f\left(\sum_{i=1}^{n} x_i e_i\right) = \sum_{i=1}^{n} x_i f(e_i)$, donc, puisque $f(\mathcal{B})$ est libre, $\forall i \in \{1,\ldots,n\}$, $x_i = 0$ d'où $x = 0$.

– Soit $y \in F$. Puisque $f(\mathcal{B})$ engendre F, il existe $(x_1, \ldots, x_n) \in K^n$ tel que $y = \sum_{i=1}^{n} x_i f(e_i)$ d'où $y = f\left(\sum_{i=1}^{n} x_i e_i\right) \in Im(f)$. Ceci montre que f est surjective. Finalement, f est bijective. ■

Exercice 98 Soit E un espace vectoriel et $f \in \mathcal{L}(E)$ tel que, pour tout $x \in E$, la famille $(x, f(x))$ est liée. Montrer que f est une homothétie.
Correction : L'hypothèse nous dit, que pour tout x non nul, il existe un scalaire λ_x tel que $\lambda_x = \lambda$ pour tout x de E, ou encore que $\lambda_x = \lambda_y$ quels que soient x et y non nuls. Si la famille (x, y) est liée, c'est clair car $y = \mu x$ et $\mu\lambda_y x = \lambda_y y = f(y) = \mu f(x) = \mu\lambda_x x$ et on peut simplifier par $\mu x \neq 0$. Si la famille $(x, f(x))$ est libre, calculons $f(x+y)$. D'une part, $f(x+y) = \lambda_{x+y}(x+y) = \lambda_{x+y}x + \lambda_{x+y}y$, et d'autre part, $f(x+y) = f(x) + f(y) = \lambda_x x + \lambda_y y$. Puisque la famille (x, y) est libre, toute décomposition d'un vecteur à l'aide de combinaisons linéaire de ces vecteurs est unique. On obtient donc $\lambda_x = \lambda_y = \lambda_{x+y}$, ce qui est le résultat voulu.

5.3 Opérations sur les applications linéaires

5.3.1 L'espace vectoriel $\mathcal{L}(E, F)$

Proposition 5.3.1 *$\mathcal{L}(E, F)$ est un K-ev pour les lois usuelles.*

Preuve : On va montrer que $\mathcal{L}(E, F)$ est un sev de F^E.

1. $\mathcal{L}(E, F) \neq \emptyset$ puisque l'application nulle $\begin{array}{rccc} 0 : & E & \to & F \\ & x & \mapsto & 0 \end{array}$ est à l'évidence linéaire.
2. Soient $\alpha \in K$, $f, g \in \mathcal{L}(E, F)$. On a pour tous $\lambda \in K$ et $x, y \in E$,
$$\begin{aligned} (\alpha f + g)(\lambda x + y) &= \alpha f(\lambda x + y) + g(\lambda x + y) \\ &= \alpha((\lambda f(x) + f(y)) + (\lambda g(x) + g(y)) \\ &= \lambda(\alpha f(x) + g(x)) + (\alpha f(y) + g(y)) \\ &= \lambda(\alpha f + g)(x) + (\alpha f + g)(y). \end{aligned}$$
Ceci montre que $\alpha f + g$ est linéaire donc $\alpha f + g \in \mathcal{L}(E, F)$. ■

5.3.2 Composition

1. **Généralités**.

Proposition 5.3.2 *Soient E, F, G trois K-ev. On a :*
$$\forall f \in \mathcal{L}(E, F),\ \forall g \in \mathcal{L}(F, G),\ g \circ f \in \mathcal{L}(E, G).$$
Preuve : $\forall \lambda \in K, \forall (x, y) \in E^2$, $(g \circ f)(\lambda x + y) = g(f(\lambda x + y)) = g(\lambda f(x) + f(y)) = \lambda g(f(x)) + g(f(y)) = \lambda(g \circ f)(x) + (g \circ f)(y)$. ■

Proposition 5.3.3 *Soient E, F, G trois K-ev. On a :*
(a) $\forall f_1, f_2 \in \mathcal{L}(E, F),\ \forall g \in \mathcal{L}(F, G),\ g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2$ *(pseudo-distributivité à gauche).*
(b) $\forall f \in \mathcal{L}(E, F),\ \forall g_1, g_2 \in \mathcal{L}(F, G),\ (g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$ *(pseudo-distributivité à droite).*
(c) $\forall \alpha \in K,\ \forall f \in \mathcal{L}(E, F),\ \forall g \in \mathcal{L}(F, G),\ (\alpha g) \circ f = g \circ (\alpha f) = \alpha(g \circ f)$.

Preuve :

(a) $\forall x \in E$, $(g \circ (f_1 + f_2))(x) = g((f_1 + f_2)(x)) = g(f_1(x)) + g(f_2(x)) = (g \circ f_1)(x) + (g \circ f_2)(x) = (g \circ f_1 + g \circ f_2)(x)$.

(b) $\forall x \in E$, $((g_1 + g_2) \circ f)(x) = (g_1 + g_2)(f(x)) = g_1(f(x)) + g_2(f(x)) = (g_1 \circ f)(x) + (g_2 \circ f)(x) = (g_1 \circ f + g_2 \circ f)(x)$.

(c) $\forall x \in E$, $\begin{cases} ((\alpha g) \circ f)(x) = (\alpha g)(f(x)) = \alpha g(f(x)) = \alpha(g \circ f)(x) = (\alpha(g \circ f))(x) \\ (g \circ (\alpha f))(x) = g(\alpha f(x)) = \alpha g(f(x)). \end{cases}$ ■

Proposition 5.3.4 *Soient E, F deux K-ev, $f \in \mathcal{L}(E, F)$. Si f est un isomorphisme de E sur F alors f^{-1} est un isomorphisme de F sur E.*

Preuve : Supposons que f soit linéaire et bijective et montrons que $f^{-1} : F \to E$ qui est déja bijective, est linéaire. Soient $\lambda \in K$, $(x', y') \in F^2$. On a : $f^{-1}(\lambda x' + y') = f^{-1}\left(\lambda f(f^{-1}(x')) + f(f^{-1}(y'))\right) = f^{-1}\left(f\left(\lambda f^{-1}(x') + f^{-1}(y')\right)\right) = \lambda f^{-1}(x') + f^{-1}(y')$, et donc f^{-1} est linéaire. ■

Définition 5.3.1 *Deux K-ev E et F sont dits **isomorphes** si et seulement s'il existe un isomorphisme de K-ev de E sur F.*

Proposition 5.3.5

(a) Soient E, F deux K-ev de dimension finie. Pour que E et F soient isomorphes, il faut et il suffit que $dim(E) = dim(F)$.

(b) Soit $n \in \mathbb{N}^\star$. Tout K-ev de dimension finie n est isomorphe à K^n.

Preuve :

(a) Supposons que E et F soient isomorphes, il existe donc un isomorphisme f de E sur F. L'ev E admet au moins une base $\mathcal{B}$ et donc (proposition (5.2.8)), $f(\mathcal{B})$ est une base de F d'où $dim(F) = Card(f(\mathcal{B})) = Card(\mathcal{B}) = dim(E)$.
Réciproquement, supposons $dim(E) = dim(F)$ alors E (respectivement F) admet une base $\mathcal{B} = (e_1, \ldots, e_n)$ (respectivement $\mathcal{C} = (e'_1, \ldots, e'_n)$), où $n = dim(E) = dim(F) \in \mathbb{N}$. Considérons $f \in \mathcal{L}(E, F)$, $g \in \mathcal{L}(F, E)$ définies par : $\forall i \in \{1, \ldots, n\}$, $(f(e_i) = e'_i$ et $g(e'_i) = e_i)$. Il est clair que $g \circ f = Id_E$ et $f \circ g = Id_F$ donc f et g sont bijectives, réciproques l'une de l'autre. Ainsi, f est un isomorphisme de K-ev de E sur F.

(b) Résulte de 1., puisque $dim(E) = dim(K^n) = n$. ■

Proposition 5.3.6 $(\mathcal{L}(E), +, ., \circ)$ *est une K-algèbre associative unitaire.*

Preuve :

(a) On a déja vu que $(\mathcal{L}(E), +, .)$ est un k-ev (voir début de section).

(b) La loi $\circ$ est interne dans $\mathcal{L}(E)$, distributive sur $+$ et vérifie la formule : $(\alpha g) \circ f = g \circ (\alpha f) = \alpha(g \circ f)$.

(c) La loi $\circ$ est associative dans E^E donc dans $\mathcal{L}(E)$.

(d) $Id_E \in \mathcal{L}(E)$ et Id_E est neutre pour $\circ$. ■

Remarque 5.3.1 D'après la proposition précédente, $(\mathcal{L}(E), +, \circ)$ est un anneau.

2. **Endomorphismes nilpotents.**

Définition 5.3.2 *Un endomorphisme f d'un K-ev est dit **nilpotent** si et seulement s'il existe $p \in \mathbb{N}^\star$ tel que $f^p = 0$.*

Si f est nilpotent, l'ensemble $\{k \in \mathbb{N}^\star, f^k = 0\}$ est une partie non vide de $\mathbb{N}^\star$ donc admet un plus petit élément, noté ici $\nu(f)$, et appelé **indice de nilpotence** de f. On a :
– $\forall k \in \mathbb{N}^\star$, $(k < \nu(f) \Rightarrow f^k \neq 0)$, par définition de $\nu(f)$.
– $\forall k \in \mathbb{N}^\star$, $(k \geq \nu(f) \Rightarrow f^k \neq 0)$, car $f^k = f^{k-\nu(f)} \circ f^{\nu(f)} = f^{k-\nu(f)} \circ 0 = 0$.

3. **Projecteurs.**
Soit E un K-ev

(a) On a vu précédemment que, pour tout couple (F, G) de sev supplémentaires dans E, on appelle projecteur sur F parallèlement à G l'application linéaire $p : \begin{array}{ccc} E & \to & E \\ x & \mapsto & x' \end{array}$ où $(x', x'') \in F \times G$ est tel que $x = x' + x''$.
Avec les notations ci-dessus, $x' = x' + 0$ et $(x', 0) \in F \times G$ d'où $p(x') = x'$. Autrement dit, $(p \circ p)(x) = p(x)$.
Déterminons $Im(p)$: Avec les notations précédentes, $p(x) = x' \in F$ d'où $Im(p) \subset F$. D'autre part, $\forall x \in F$, on a $x = x + 0$ et $(x, 0) \in F \times G$ donc $x = p(x) \in Im(p)$. Ainsi $Im(p) = F$.
Déterminons $Ker(p)$: Pour tout x de G, $x = 0 + x$ et $(0, x) \in F \times G$ donc $p(x) = 0$ d'où $G \subset Ker(p)$. D'autre part, pour tout x de E, on a, avec les notations précédentes, $p(x) = 0 \Leftrightarrow x' = 0 \Leftrightarrow x' = x'' \Rightarrow x \in G$, donc $Ker(p) \subset G$. Ainsi $Ker(p) = G$.

(b) Réciproquement, soit $p \in \mathcal{L}(E)$ tel que $p \circ p = p$ (on dit que p est un **idempotent** de l'anneau $\mathcal{L}(E)$). Montrons que $Im(p)$ et $Ker(p)$ sont deux sev de E supplémentaires dans E et que p est le projecteur sur $Im(p)$ parallèlement à $Ker(p)$.
Soit $x \in Ker(p) \cap Im(p)$. Alors $p(x) = 0$ et il existe $y \in E$ tel que $x = p(y)$ d'où $0 = p(x) = p(p(y)) = (p \circ p)(y) = p(y) = x$. Ceci montre que $Im(p) \cap Ker(p) = \{0\}$.
Soit $x \in E$. On dispose de la décomposition $x = p(x) + (x - p(x))$ et $\left\{ \begin{array}{l} p(x) \in Im(p) \\ x - p(x) \in Ker(p) \end{array} \right.$, car $p(x - p(x)) = p(x) - (p \circ p)(x) = 0$. Ceci montre que $E = Im(p) + Ker(p)$.
Puisque, pour tout x de E, $\left\{ \begin{array}{l} x = p(x) + (x - p(x)) \\ p(x) \in Im(p) \\ x - p(x) \in Ker(p) \end{array} \right.$, p est le projecteur sur $Im(p)$ parallèlement à $Ker(p)$.

Résumons l'étude :

Proposition 5.3.7

(a) Soient F, G deux sev de E supplémentaires dans E, p le projecteur sur F parallèlement à G. On a $p \circ p = p$, $Im(p) = F$, $Ker(p) = G$.

(b) Réciproquement, si $p \in \mathcal{L}(E)$ est tel que $p \circ p = p$ alors $Im(p)$ et $Ker(p)$ sont deux sev supplémentaires dans E, et p est le projecteur sur $Im(p)$ parallèlement à $Ker(p)$.

De plus, pour tout x de E,

$$x = p(x) + (x - p(x)),\ p(x) \in Im(p),\ x - p(x) \in Ker(p).$$

5.3.3 Le groupe $\mathcal{GL}(E)$

Proposition 5.3.8 *Soit E un K-ev. L'ensemble $\mathcal{GL}(E)$ des automorphismes de E est un groupe pour $\circ$, appelé **groupe linéaire** de E.*

Preuve :

1. La loi $\circ$ est interne dans $\mathcal{GL}(E)$ car, si $f, g : E \to E$ sont linéaires et bijectives, alors $g \circ f$ est linéaire et bijective.
2. $Id_E \in \mathcal{GL}(E)$ et Id_E est neutre pour $\circ$.

3. La loi $\circ$ est associative dans E^E donc dans $\mathcal{GL}(E)$.
4. Soit $f \in \mathcal{GL}(E)$. D'après la proposition (5.3.4), f^{-1} est un automorphisme de E, c'est-à-dire $f^{-1} \in \mathcal{GL}(E)$. ■

Remarque 5.3.2 :

1. Le groupe $\mathcal{GL}(E)$ n'est pas commutatif, sauf si E est de dimension finie et $dim(E) \leq 1$
2. Si E est de dimension finie et $dim(E) = 1$ alors $(\mathcal{GL}(E), \circ)$ est un groupe isomorphe au groupe $(K - \{0\}, .)$ par l'isomorphisme de groupes $\begin{array}{ccc} K-\{0\} & \to & \mathcal{GL}(E) \\ \alpha & \mapsto & h_\alpha \end{array}$ où $\begin{array}{ccc} h_\alpha : E & \to & E \\ x & \mapsto & \alpha x \end{array}$ est l'homothétie de rapport α.
3. $\mathcal{GL}(E)$ est aussi l'ensemble des éléments inversibles de l'anneau $(\mathcal{L}(E), +, \circ)$.

5.4 Cas de la dimension finie

5.4.1 Le théorème du rang et ses conséquences

Définition 5.4.1 *Soient E, F deux K-ev de dimension finie, $f \in \mathcal{L}(E, F)$. On appelle rang de f, et on note $rg(f)$, l'entier naturel défini par :*

$$rg(f) = dim(Im(f)).$$

Remarque 5.4.1

1. $Im(f)$ est bien de dimension finie, puisque $Im(f)$ est un sev de F et que F est de dimension finie, ou bien autrement, parce que E est de dimension finie. Plus généralement, soient E, F deux K-ev (non nécessairement de dimension finie), $f \in \mathcal{L}(E, F)$. On dit que f est de rang **fini** si et seulement si $Im(f)$ est de dimension finie, et dans ce cas, on appelle rang de f l'entier naturel, noté $rg(f)$, défini par $rg(f) = dim(Im(f))$.
2. Si $\mathcal{B}$ est une base de E alors, pour toute base f de $\mathcal{L}(E, F) : rg(f) = dim(f(Vect(\mathcal{B}))) = dim(Vect(f(\mathcal{B}))) = rg(f(\mathcal{B}))$.
3. Pour toute f de $\mathcal{L}(E, F)$, $rg(f) \leq \min(dim(E), dim(F))$. En effet,
   – E admet au moins une base $\mathcal{B}$, et on a : $rg(f) = rg(f(\mathcal{B}))$ et $Card(f(\mathcal{B})) \leq dim(E)$.
   – $rg(f) = dim(Im(f)) \leq dim(F)$.

Théorème 5.4.1 *Soient E, F deux K-ev, $f \in \mathcal{L}(E, F)$. On a*

$$rg(f) = dim(E) - dim(Ker(f)).$$

Preuve : On note $p = dim(E)$, $n = dim(F)$. Le sev $Ker(f)$ de E admet au moins une base $(e_1, \ldots, e_q)$ où $q = dim(Ker(f)) \in \mathbb{N}$. D'après le théorème de la base incomplète, forme faible, on peut compléter $(e_1, \ldots, e_q)$ en une base $(e_1, \ldots, e_q, e_{q+1}, \ldots, e_p)$ de E. On va montrer que $(f(e_{q+1}), \ldots, f(e_p))$ est une base de $Im(f)$.

1. $f(e_{q+1}), \ldots, f(e_p)$ sont à l'évidence dans $Im(f)$.
2. Soit $(\lambda_{q+1}, \ldots, \lambda_p) \in K^{p-q}$ tel que $\sum_{i=q+1}^{p} \lambda_i f(e_i) = 0$. Alors $f\left(\sum_{i=q+1}^{p} \lambda_i e_i\right) = \sum_{i=q+1}^{p} \lambda_i f(e_i) = 0$ donc $\sum_{i=q+1}^{p} \lambda_i e_i \in Ker(f)$. Il existe donc $(\mu_1, \ldots, \mu_q) \in K^q$ tel que $\sum_{i=q+1}^{p} \lambda_i e_i = \sum_{i=1}^{q} \mu_i e_i$, d'où $\mu_1 e_1 + \ldots + \mu_q e_q - \lambda_{q+1} e_{q+1} - \ldots - \lambda_p e_p = 0$. Comme $(e_1, \ldots, e_p)$ est libre, on déduit (entre autres) $\lambda_{q+1} = \ldots = \lambda_p = 0$. Ceci montre que $(f(e_{q+1}), \ldots, f(e_p))$ est libre.

3. Soit $y \in Im(f)$. Il existe $x \in E$ tel que $y = f(x)$. Puis, comme $(e_1, \ldots, e_p)$ engendre E, il existe $(\alpha_1, \ldots, \alpha_p) \in K^p$ tel que $x = \sum_{i=1}^{p} \alpha_i e_i$. On a $y = f(x) = f\left(\sum_{i=1}^{p} \lambda_i e_i\right) = \sum_{i=1}^{p} \lambda_i f(e_i) = \sum_{i=q+1}^{p} \lambda_i f(e_i)$, puisque $f(e_1) = \ldots = f(e_q) = 0$. Ceci montre que $(f(e_{q+1}), \ldots, f(e_p))$ engendre $Im(f)$. Comme $(f(e_{q+1}), \ldots, f(e_p))$ est une base de $Im(f)$, on conclut $rg(f) = dim(Im(f)) = p - q = dim(E) - dim(Ker(f))$. ■

Remarque 5.4.2

1. La preuve précédente montre aussi que pour tout supplémentaire E_1 de $Ker(f)$ dans E, l'application linéaire $\begin{array}{ccc} E_1 & \to & Im(f) \\ x & \mapsto & f(x) \end{array}$ est un isomorphisme d'ev. Ainsi, tout supplémentaire de $Ker(f)$ dans E est isomorphe à $Im(f)$.
2. Bien que $dim(Ker(f))+dim(Im(f)) = dim(E)$, en général $Ker(f)$ et $Im(f)$ ne sont pas supplémentaires dans E. En effet, d'abord $Im(f)$ est un sev de F et non de E (à priori). Et puis, même si $F = E$, $Ker(f)$ et $Im(f)$ peuvent ne pas être supplémentaires dans E, comme le montre l'exemple : $K = \mathbb{R}$, $E = F = \mathbb{R}^2$, $\begin{array}{ccc} f : \mathbb{R}^2 & \to & \mathbb{R}^2 \\ (x, y) & \mapsto & (y, 0) \end{array}$, dans lequel on a $Ker(f) = Im(f) = Vect((1, 0))$.

Proposition 5.4.1 *Soient E, F deux K-ev de dimension finie, $f \in \mathcal{L}(E, F)$. On a :*

1. *f injective $\Leftrightarrow rg(f) = dim(E)$.*
2. *f surjective $\Leftrightarrow rg(f) = dim(F)$.*

Preuve :

1. En utilisant le théorème du rang, f injective $\Leftrightarrow Ker(f) = \{0\} \Leftrightarrow dim(Ker(f)) = 0 \Leftrightarrow rg(f) = dim(E)$.
2. f surjective $\Leftrightarrow rg(f) = dim(F)$. ■

Définition 5.4.2 *Un élément f de $\mathcal{L}(E)$ est dit :*

- ***inversible à gauche*** *pour $\circ$ dans $\mathcal{L}(E)$ si et seulement si :*
$$\exists f' \in \mathcal{L}(E), f' \circ f = Id_E$$
- ***inversible à droite*** *pour $\circ$ dans $\mathcal{L}(E)$ si et seulement si :*
$$\exists f'' \in \mathcal{L}(E), f \circ f'' = Id_E$$
- ***inversible*** *pour $\circ$ dans $\mathcal{L}(E)$ si et seulement si :*
$$\exists f' \in \mathcal{L}(E), f' \circ f = f \circ f' = Id_E.$$

On rappelle qu'un élément f de $\mathcal{L}(E)$ est dit :

- régulier à gauche pour $\circ$ dans $\mathcal{L}(E)$ si et seulement si :
$$\forall (g, h) \in (\mathcal{L}(E))^2,\ f \circ g = f \circ h \Rightarrow g = h,$$
- régulier à droite pour $\circ$ dans $\mathcal{L}(E)$ si et seulement si :
$$\forall (g, h) \in (\mathcal{L}(E))^2,\ g \circ f = h \circ f \Rightarrow g = h,$$
- régulier pour $\circ$ dans $\mathcal{L}(E)$ si et seulement si f est régulier à gauche et régulier à droite pour $\circ$ dans $\mathcal{L}(E)$.

Théorème 5.4.2 *Soient E un K-ev de dimension finie, $f \in \mathcal{L}(E)$. Les propriétés suivantes sont deux à deux équivalentes :*

1. *f est inversible à gauche pour $\circ$ dans $\mathcal{L}(E)$*
2. *f est inversible à droite pour $\circ$ dans $\mathcal{L}(E)$*

3. *f est inversible pour $\circ$ dans $\mathcal{L}(E)$*
4. *f est régulier à gauche pour $\circ$ dans $\mathcal{L}(E)$*
5. *f est régulier à droite pour $\circ$ dans $\mathcal{L}(E)$*
6. *f est régulier pour $\circ$ dans $\mathcal{L}(E)$*
7. *f est injectif*
8. *f est surjectif*
9. *f est bijectif*

Preuve : 1. $\Rightarrow$ 4. : Supposons f inversible à gauche pour $\circ$ dans $\mathcal{L}(E)$; il existe $f' \in \mathcal{L}(E)$ tel que $f' \circ f = e$. Alors $\forall (g,h) \in (\mathcal{L}(E))^2$, $f \circ g = f \circ h \Rightarrow f' \circ f \circ g = f' \circ f \circ h \Rightarrow g = h$ donc f est régulier à gauche pour $\circ$ dans $\mathcal{L}(E)$. On montre de même 2. $\Rightarrow$ 5. et on en déduit 3. $\Rightarrow$ 6.
4. $\Rightarrow$ 7. : Supposons f régulier à gauche pour $\circ$ dans $\mathcal{L}(E)$. Le sev $Ker(f)$ de l'ev de dimension finie E admet au moins un supplémentaire E_1 dans E. Considérons le projecteur p sur E_1 parallèlement à $Ker(f)$. On a $\forall x \in E$, $f(x) = f(p(x) + (x - p(x))) = f(p(x)) + f(x - p(x)) = f(p(x))$ puisque $x - p(x) \in Ker(f)$. Ainsi, $f \circ e = f \circ p$ d'où, puisque f est régulière à gauche, $e = p$ et donc $E = e(E) = p(E) = E_1$, $Ker(f) = \{0\}$, f est injective.
5. $\Rightarrow$ 8. : Supposons f régulier à droite pour $\circ$ dans $\mathcal{L}(E)$. Le sev $Im(f)$ de l'ev de dimension finie E admet au moins un supplémentaire E_2 dans E. Considérons le projecteur q sur $Im(f)$ parallèlement à E_2. On a $\forall x \in E$, $f(x) = q(f(x))$, puisque $f(x) \in Im(f)$. Ainsi $e \circ f = q \circ f$ d'où, puisque f est régulier à droite, $e = q$ et donc $E = e(E) = q(E) = Im(f)$, f est surjective. Comme 4. $\Rightarrow$ 7. et 5. $\Rightarrow$ 8., on déduit 6. $\Rightarrow$ 9.
7. $\Leftrightarrow$ 8. : En utilisant le théorème du rang, on obtient f injective $\Leftrightarrow Ker(f) = \{0\} \Leftrightarrow dim(Ker(f)) = 0 \Leftrightarrow rg(f) = dim(E) \Leftrightarrow dim(Im(f)) = dim(E) \Leftrightarrow Im(f) = E \Leftrightarrow f$ surjective.
De l'équivalence 7. $\Leftrightarrow$ 8., on déduit trivialement 7. $\Rightarrow$ 9. et 8. $\Rightarrow$ 9.
9. $\Rightarrow$ 3. : Si f est linéaire et bijective alors f^{-1} est linéaire donc f admet un inverse pour $\circ$ dans $\mathcal{L}(E)$.
3. $\Rightarrow$ 1. et 3. $\Rightarrow$ 2. : évident. Le cycle 1. $\Rightarrow$ 4. $\Rightarrow$ 7. $\Rightarrow$ 9. $\Rightarrow$ 3. $\Rightarrow$ 1. montre que les propriétés 1., 4., 7., 9. et 3. sont deux à deux équivalentes. De même, 2., 5., 8., 9., et 3. sont deux à deux équivalentes et 3., 6., 9. sont deux à deux équivalentes. Finalement, les neuf propriétés envisagées sont deux à deux équivalentes. ■

5.4.2 Dimension de $\mathcal{L}(E,F)$

Proposition 5.4.2 *Soient E, F deux K-ev de dimension finie. Alors, $\mathcal{L}(E,F)$ est de dimension finie et :*

$$dim(\mathcal{L}(E,F)) = dim(E).dim(F).$$

Preuve : Notons $p = dim(E)$, $n = dim(F)$, $\mathcal{B} = (e_1, \ldots, e_p)$ une base de E, $\mathcal{C} = (e'_1, \ldots, e'_n)$ une base de F. Pour chaque $(i,j) \in \{1, \ldots, n\} \times \{1, \ldots, p\}$, notons φ_{ij} l'application linéaire de E dans F définie par $\forall k \in \{1, \ldots, p\}$, $\varphi_{ij}(e_k) = \delta_{kj} e'_i$ où δ_{kj} est le symbole de Kronecker, défini par :

$$\delta_{ij} = \begin{cases} 1 & \text{si} \quad k = j \\ 0 & \text{si} \quad k \neq j \end{cases}$$

Montrons que la famille $\phi = (\varphi_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}}$ est une base de $\mathcal{L}(E,F)$.

1. On a alors pour tout k de $\{1, \ldots, p\}$:

$$0 = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \lambda_{ij} \varphi_{ij}(e_k) = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \lambda_{ij} \varphi_{ij}(e_k) = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \lambda_{ij} \delta_{kj} e'_i = \sum_{i=1}^{n} \lambda_{ik} e'_i.$$

Comme $(e'_1, \ldots, e'_n)$ est libre, on déduit $\forall k \in \{1, \ldots, p\}$, $\forall i \in \{1, \ldots, n\}$, $\lambda_{ik} = 0$. Ceci montre que ϕ est libre.

2. Soit $f \in \mathcal{L}(E,F)$. Pour chaque j de $\{1,\dots,p\}$, $f(e_j)$ se décompose dans la base $(e'_1,\dots,e'_n)$ de F, il existe donc $(\lambda_{1j},\dots,\lambda_{nj}) \in K^n$ tel que $f(e_j) = \sum_{i=1}^{n} \lambda_{ij} e'_i$. On a alors comme dans 1. :

$$\forall k \in \{1,\dots,p\},\ \left(\sum_{\substack{1 \le i \le n \\ 1 \le j \le p}} \lambda_{ij}\varphi_{ij} \right)(e_k) = \sum_{i=1}^{n} \lambda_{ik} e'_i = f(e_k)$$

d'où $f = \sum_{\substack{1 \le i \le n \\ 1 \le j \le p}} \lambda_{ij}\varphi_{ij}$. Ceci montre que ϕ engendre $\mathcal{L}(E,F)$. Finalement ϕ est une base de $\mathcal{L}(E,F)$ et $dim(\mathcal{L}(E,F)) = Card(\phi) = pn = dim(E).dim(F)$. ■

Exercice 99 Soit u l'application linéaire de $\mathbb{R}^3$ dans $\mathbb{R}^4$ définie par

$$u(x,y,z) = (-x+y, x-y, -x+z, -y+z).$$

1. Montrer que u est linéaire.
2. Soient $\{\epsilon_1,\epsilon_2,\epsilon_3\}$ la base canonique de $\mathbb{R}^3$ et $\{\mathcal{F}_1,\mathcal{F}_2,\mathcal{F}_3,\mathcal{F}_4\}$ la base canonique de $\mathbb{R}^4$. Calculer $u(\epsilon_1)$, $u(\epsilon_2)$ et $u(\epsilon_3)$ en fonction de $\mathcal{F}_1,\mathcal{F}_2,\mathcal{F}_3$, et $\mathcal{F}_4$.
3. Écrire la matrice de u dans les bases canoniques.
4. Montrer que $\{\mathcal{F}_1,\mathcal{F}_2,u(\epsilon_1),u(\epsilon_2)\}$ est une base de $\mathbb{R}^4$.
5. Écrire la matrice de u dans les bases $\{\epsilon_1,\epsilon_2,\epsilon_3\}$ et $\{\mathcal{F}_1,\mathcal{F}_2,u(\epsilon_1),u(\epsilon_2)\}$.

Correction :

1. Soient $X=(x,y,z)$, $X'=(x',y',z')$ et $\lambda \in \mathbb{R}$. Alors on a $u(X+X') = u(x+x',y+y',z+z') = (-x-x'+y+y', x+x'-y-y', -x-x'+z+z', -y-y'+z+z') = ((-x+y)+(-x'+y'),(x-y)+(x'-y'),(-x+z)+(-x'+z'),(-y+z)+(-y'+z')) = (-x+y,x-y,-x+z,-y+z)+(-x'+y',x'-y',-x'+z',-y'+z') = u(X)+u(X')$.
   De même on a $u(\lambda X) = u(\lambda x,\lambda y,\lambda z) = (-\lambda x+\lambda y,\lambda x-\lambda y,-\lambda x+\lambda z,-\lambda y+\lambda z) = \lambda(-x+y,x-y,-x+z,-y+z) = \lambda u(X)$.
   Ainsi u est linéaire. On aurait également pu utiliser la caractérisation des applications linéaires de $\mathbb{R}^p$ dans $\mathbb{R}^n$: chaque coordonnée de $u(x,y,z)$ s'écrit comme combinaison linéaire de (x,y,z).
2. On a
   - $u(\epsilon_1) = u(1,0,0) = (-1,1,-1,0) = -\mathcal{F}_1 + \mathcal{F}_2 - \mathcal{F}_3$,
   - $u(\epsilon_2) = u(0,1,0) = (1,-1,0,-1) = \mathcal{F}_1 - \mathcal{F}_2 - \mathcal{F}_4$,
   - $u(\epsilon_3) = u(0,0,1) = (0,0,1,1) = \mathcal{F}_3 + \mathcal{F}_4$.
3. On verra dans le chapitre suivant que la matrice recherchée s'écrit $\begin{pmatrix} -1 & 1 & 0 \\ 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 1 \end{pmatrix}$.
4. Puisque $\mathbb{R}^4$ est de dimension 4 et que la famille considérée a quatre éléments, il suffit de montrer qu'il s'agit d'une famille libre. C'est particulièrement facile ici car la famille est triangulaire par rapport à la base canonique de $\mathbb{R}^4$. En effet, si on a $a\mathcal{F}_1 + b\mathcal{F}_2 + cu(\epsilon_1) + du(\epsilon_2) = 0$, ceci se traduit par

$$\begin{cases} a - c + d &= 0 \\ b + c - d &= 0 \\ -c &= 0 \\ -d &= 0 \end{cases} \Leftrightarrow a = b = c = d = 0.$$

5. Il s'agit d'exprimer chaque $u(\epsilon_i)$ en fonction des vecteurs de la nouvelle base. Pour deux des vecteurs, c'est très facile car $u(\epsilon_1) = u(\epsilon_1)$ et $u(\epsilon_2) = u(\epsilon_2)$. C'est plus difficile pour $u(\epsilon_3)$, qu'il faut exprimer dans la nouvelle base. Autrement dit, il faut trouver a, b, c, d de sorte que $a\mathcal{F}_1 + b\mathcal{F}_2 + cu(\epsilon_1) + du(\epsilon_2) = (0, 0, 1, 1)$. Ceci revient à résoudre le système

$$\left\{\begin{array}{rcl} a-c+d &=& 0\\ b+c-d &=& 0\\ -c &=& 1\\ -d &=& 1 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcl} a &=& 0\\ b &=& 0\\ c &=& -1\\ d &=& -1 \end{array}\right. .$$

Ainsi, on a $u(\epsilon_3) = -u(\epsilon_1) - u(\epsilon_2)$ et la matrice de u dans les bases $\{\epsilon_1, \epsilon_2, \epsilon_3\}$ et $\{\mathcal{F}_1, \mathcal{F}_2, u(\epsilon_1), u(\epsilon_2)\}$ est donc

$$\begin{pmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 1 & 0 & -1\\ 0 & 1 & -1 \end{pmatrix}$$

Exercice 100 Soient $\{\epsilon_1, \epsilon_2, \epsilon_3\}$ la base canonique de $\mathbb{R}^3$, $w_1 = (1, -2, 0)$, $w_2 = (-1, 2, 0)$, $w_3 = (0, 0, 2)$ et u l'endomorphisme de $\mathbb{R}^3$ défini par la donnée des images des vecteurs de la base :

$$u(\epsilon_1) = w_1,\ u(\epsilon_2) = w_2,\ u(\epsilon_3) = w_3.$$

1. (a) Exprimer w_1, w_2, w_3 en fonction de ϵ_1, ϵ_2 et ϵ_3. En déduire la matrice de u dans la base canonique.
   (b) Soit $W = (x, y, z) \in \mathbb{R}^3$. Calculer $u(W)$.
2. (a) Trouver une base de $Ker(u)$ et une base de $Im(u)$.
   (b) Montrer que $\mathbb{R}^3 = Ker(u) \oplus Im(u)$.
3. Déterminer $Ker(u - Id)$ et $Im(u - Id)$ où Id désigne l'identité de $\mathbb{R}^3$. En déduire que $u - Id$ est un automorphisme de $\mathbb{R}^3$.

Correction :

1. (a) On a $w_1 = \epsilon_1 - 2\epsilon_2$, $w_2 = -\epsilon_1 + 2\epsilon_2$ et $w_3 = 2\epsilon_3$. On en déduit que la matrice de u est $\begin{pmatrix} 1 & -1 & 0\\ -2 & 2 & 0\\ 0 & 0 & 2 \end{pmatrix}$.
   (b) On a $u(W) = \begin{pmatrix} 1 & -1 & 0\\ -2 & 2 & 0\\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} x\\ y\\ z \end{pmatrix} = \begin{pmatrix} x-y\\ -2x+2y\\ 2z \end{pmatrix}$.
2. (a) On a $W \in Ker(u) \Leftrightarrow \left\{\begin{array}{rcl} x-y &=& 0\\ -2x+2y &=& 0\\ z &=& 0 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcl} x &=& -y\\ y &=& y\\ z &=& 0 \end{array}\right.$. On a donc $Ker(u) = Vect(-1, 1, 0)$.
   Le vecteur $(-1, 1, 0)$ est une base de $Ker(u)$. En utilisant le théorème du rang, la dimension de $Im(u)$ vérifie :
   $$dim(\mathbb{R}^3) = dim(Im(u)) + dim(Ker(u)).$$
   ce qui donne $dim(Im(u)) = 2$. Une famille génératrice de $Im(u)$ est donnée par (w_1, w_2, w_3). Il suffit d'en extraire une famille libre à deux éléments. C'est par exemple le cas de (w_1, w_3). On en déduit que (w_1, w_3) est une base de $Im(u)$.
   (b) Il suffit de démontrer que la réunion d'une base de $Ker(u)$ et d'une base de $Im(u)$ est une base de $\mathbb{R}^3$. Autrement dit, avec les calculs précédents, il suffit de prouver que la famille $((-1, 1, 0), w_1, w_3)$ est libre.

3. On calcule $u-Id$: $(u-Id)(x,y,z) = \begin{pmatrix} -y \\ -2x+y \\ z \end{pmatrix}$. On a donc $(u-Id)(x,y,z) = 0 \Leftrightarrow \left\{ \begin{array}{rcl} y & = & 0 \\ -2+y & = & 0 \\ z & = & 0 \end{array} \right. \Leftrightarrow$ $\left\{ \begin{array}{rcl} x & = & 0 \\ y & = & 0 \\ z & = & 0 \end{array} \right.$. On a donc $Ker(u-Id) = \{0\}$ donc u est injective. Grâce au théorème du rang, on a $dim(Im(u-Id)) = 3$. Comme $Im(u-Id)$ est un sous-espace vectoriel de $\mathbb{R}^3$, on a en fait $Im(u-Id) = \mathbb{R}^3$. u est aussi surjective. C'est donc un automorphisme de $\mathbb{R}^3$.

Exercice 101 On considère l'application linéaire f de $\mathbb{R}^3$ dans $\mathbb{R}^4$ définie par

$$f(x,y,z) = (x+z, y-x, z+y, x+y+2z).$$

1. Calculer les images par f des vecteurs de la base canonique (e_1,e_2,e_3) de $\mathbb{R}^3$. En déduire une base de $Im(f)$.
2. Déterminer une base de $Ker(f)$.
3. L'application f est-elle injective ? Surjective ?

Correction :

1. On utilise la définition de f et on a :

$$\begin{array}{c} f(e_1) = (1,-1,0,1), \\ f(e_2) = (0,1,1,1), \\ f(e_3) = (1,0,1,2). \end{array}$$

On sait que la famille $(f(e_1), f(e_2), f(e_3))$ est une famille génératrice de $Im(f)$. Or, $f(e_3) = f(e_1) + f(e_2)$ et donc $f(e_3)$ est combinaison linéaire de $(f(e_1), f(e_2))$. Ainsi, la famille $(f(e_1), f(e_2))$ est déja génératrice de $Im(f)$. De plus, elle est libre car les deux vecteurs sont non nuls et ne sont pas proportionnels. On en déduit que $(f(e_1), f(e_2))$ est une base de $Im(f)$.

2. On a $(x,y,z) \in Ker(f) \Leftrightarrow \left\{ \begin{array}{rcl} x+z & = & 0 \\ -x+y & = & 0 \\ y+z & = & 0 \\ x+y+2z & = & 0 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} y+z & = & 0 \\ y+z & = & 0 \\ y+z & = & 0 \\ y+z & = & 0 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} x & = & -z \\ y & = & -z \\ z & = & z \end{array} \right.$. On en déduit que le vecteur $(-1,-1,1)$ engendre $Ker(f)$. Comme il est non nul, c'est une base de $Ker(f)$. En particulier, on trouve que $Ker(f)$ est de dimension 1, ce que l'on peut aussi obtenir en utilisant le théorème du rang.
3. f n'est pas injective, car son noyau n'est pas réduit à $\{0\}$. f n'est pas surjective car son image n'est pas $\mathbb{R}^3$ tout entier. En effet, la dimension de $Im(f)$ est 2 et non 3.

Exercice 102 Soit $E = \mathbb{R}_3[X]$ l'espace vectoriel des polynômes à coefficients réels de degré inférieur ou égal à 3. On définit u l'application de E dans lui-même par

$$u(P) = P + (1-X)P'.$$

1. Montrer que u est un endomorphisme de E.
2. Déterminer une base de $Im(u)$.
3. Déterminer une base de $Ker(u)$.
4. Montrer que $Ker(u)$ et $Im(u)$ sont deux sous-espaces vectoriels supplémentaires de E.

Correction :

1. Remarquons d'abord que si $P \in E$, $u(P)$ est bien un polynôme de degré inférieur ou égal à 3, et donc u envoie bien E dans E. Pour montrer qu'il s'agit d'un endomorphisme, on doit prouver que u est linéaire. Mais si $P, Q \in E$ et $\lambda \in \mathbb{R}$ on a :
$$u(P+\lambda Q) = (P+\lambda Q) + (1-X)(P+\lambda Q)' = P + \lambda Q + (1-X)(P' + \lambda Q') = \\ P + (1-X)P' + \lambda(Q + (1-X)Q') = u(P) + u(Q).$$
u est donc bien linéaire.
2. Puisque $(1, X, X^2, X^3)$ est une base de E, on sait que $u(1), u(X), u(X^2), u(X^3)$ est une famille génératrice de $Im(u)$. On va donc pouvoir en extraire une base. On a :
$$u(1) = 1,\ u(X) = 1,\ u(X^2) = -X^2 + 2X,\ u(X^3) = -2X^3 + 3X^2.$$
On en déduit que $(u(1), u(X^2), u(X^3))$ est une famille libre (ce sont des polynômes de degrés différents) et que $u(X)$ s'écrit comme combinaison linéaire de ceux-ci (on a même $u(X) = u(1)$). Ainsi, ceci prouve que $(u(1), u(X^2), u(X^3))$ est une base de $Im(u)$.
3. Écrivons $P(X) = aX^3 + bX^2 + cX + d$, et calculons $u(P)$:
$$u(P) = -2aX^3 + (3a-2b)X^2 + 2bX + c + d.$$
On obtient donc
$$u(P) = 0 \Leftrightarrow \left\{ \begin{array}{rcl} -2a & = & 0 \\ 3a-2b & = & 0 \\ 2b & = & 0 \\ c+d & = & 0 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} a & = & 0 \\ b & = & 0 \\ c & = & c \\ d & = & -c \end{array} \right. .$$
Ainsi, $P \in Ker(u) \Leftrightarrow \exists c \in \mathbb{R}, P = c(X-1)$. Une base de $Ker(u)$ est donné par le polynôme $X-1$.
4. La réunion des bases de $Im(u)$ et $Ker(u)$ trouvées précédemment est $(1, -X^2+2X, -2X^3+3X^2, X-1)$. Ces polynômes sont tous de degrés différents. Ils forment une base de E. Ceci prouve que $Im(u)$ et $Ker(u)$ sont supplémentaires.

Exercice 103 On note E l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$ qui s'écrivent sous la forme
$$\lambda \cos + \mu \sin \text{ avec } \lambda, \mu \in \mathbb{R}.$$

1. Montrer que E est un espace vectoriel. En donner une base et calculer sa dimension.
2. Montrer que la dérivation des fonctions de la variable réelle définit une application de E dans E. On note D cette application.
3. Rappeler les résultats permettant d'affirmer que D est un endomorphisme.
4. Donner la matrice de D dans la base trouvée en 1.
5. Montrer que D est un isomorphisme, c'est-à-dire que pour tout vecteur v de E, il existe un unique vecteur u de E tel que $Du = v$.
6. Montrer qu'on peut alors construire un isomorphisme D^{-1} de E tel que, pour tout vecteur u de E on a $D(D^{-1}(u)) = u$ et $D^{-1}(D(u)) = u$.
7. Donner la matrice de D^{-1} dans la base trouvée en 1.

Correction :

1. Il suffit de remarquer que E est un sous-espace vectoriel de $\mathcal{F}(\mathbb{R}, \mathbb{R})$, l'espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. En effet,
   - la fonction nulle est élément de E : $0 = 0.\cos + 0.\sin$,
   - si $f = \lambda \cos + \mu \sin$ et $g = \lambda' \cos + \mu' \sin$ et $a \in \mathbb{R}$, alors $af + g = (a\lambda + \lambda')f + (a\mu + \mu')g$ est élément de E.

On peut aussi tout simplement remarquer que $E = Vect(\cos, \sin)$. La famille $(\cos, \sin)$ est, par définition de E, une famille génératrice de E. De plus, cette famille est libre. En effet, si $\lambda \cos + \mu \sin = 0$, ceci signifie que pour tout $x \in \mathbb{R}$, on a $\lambda \cos(x) + \mu \sin(x) = 0$. Si on choisit $x = 0$, on trouve $\lambda = 0$ et si on choisit $x = \pi/2$, on trouve $\mu = 0$. La famille $(\cos, \sin)$ est donc une base de E qui est un espace vectoriel de dimension 2.

2. Soit $f = \lambda \cos + \mu \sin$ un élément de E. Utilisant les formules bien connues concernant la dérivation du sinus et du cosinus, on a $Df = f' = \mu \cos - \lambda \sin \in E$ et donc $Df \in E$.
3. On sait que, pour toutes fonctions dérivables f, g et tout réel c, $(f+g)' = f' + g'$ et $(cf)' = cf'$, ce qui se réécrit pour les fonctions de E en $D(f+g) = Df + Dg$ et $D(cf) = cD(f)$. Autrement dit, D est un endomorphisme de E.
4. Puisque $D(\cos) = -\sin$ et $D(\sin) = \cos$, la matrice de D dans la base $(\cos, \sin)$ est donnée par $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.
5. Puisque D est un endomorphisme de E qui est de dimension finie égale à deux, il suffit de prouver que D est injectif. Mais si $f = \lambda \cos + \mu \sin$ et $Df = 0$ alors $-\lambda \sin + \mu \cos = 0 \Rightarrow \lambda = \mu = 0$ puisque la famille $(\cos, \sin)$ est libre. On en déduit que D est injective, donc bijective.
6. Soit H l'endomorphisme de E défini par l'image de la base : $H(\cos) = \sin$ et $H(\sin) = -\cos$. Alors $D \circ H(\cos) = D(\sin) = \cos$ et $D \circ H(\sin) = D(-\cos) = \sin$. Par linéarité, on obtient que $D \circ H = Id_E$. De même, on a $H \circ D = Id_E$. Ainsi, $H = D^{-1}$ est l'isomorphisme réciproque de D.
7. On trouve par le même raisonnement $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Chapitre 6

Les matrices

6.1 Introduction

Étant donné deux K-espaces vectoriels E et F, une base $\mathcal{B} = (e_1, \ldots, e_p)$ de E, une base $\mathcal{C} = (f_1, \ldots, f_n)$ de F, une application linéaire f de E dans F est entièrement déterminée par la donnée de $f(e_1), \ldots, f(e_p)$ c'est-à-dire par la donnée des coordonnées de chacun des vecteurs $f(e_1), \ldots, f(e_p)$ dans la base $\mathcal{C}$ de F. Ces coordonnées peuvent être rangées dans un tableau à n lignes et p colonnes, appelé matrice. Ceci va nous permettre d'utiliser des algorithmes de calcul en algèbre linéaire. Ainsi les matrices sont étudiées en soi (en tant que tableau) et aussi en liaison avec les vecteurs et les applications linéaires.

6.2 Calcul matriciel

6.2.1 Notion de matrice

Soient $n, p \in \mathbb{N}^\star$.

Définition 6.2.1 *On appelle* ***matrice à*** n ***lignes et*** p ***colonnes, et à éléments*** *(ou* ***coefficients*** *ou* ***termes)*** ***dans*** K*, toute application de* $\{1, \ldots, n\} \times \{1, \ldots, p\}$ *dans* K*. Une application*

$$\begin{array}{rcl} A : \{1, \ldots, n\} \times \{1, \ldots, p\} & \to & K \\ (i, j) & \mapsto & a_{ij} (ou a_{i,j}) \end{array}$$

est notée sous la forme d'un tableau :

$$A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq p} = (a_{ij})_{ij} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1p} \\ a_{21} & a_{22} & \ldots & a_{2p} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{np} \end{pmatrix}.$$

Remarque 6.2.1

- Le couple (n, p) est appelé le **format** de la matrice A ; n est le nombre de lignes de A, p est le nombre de colonnes de A.
  Pour $(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, p\}$ le terme a_{ij}, situé à la i-ième ligne et à la j-ième colonne s'appelle le (i, j)-ième élément ou coefficient ou terme de A.
- A est une matrice **carrée** si et seulement si $n = p$. On dit alors que A est une matrice carrée d'ordre n.
- A est une matrice **colonne** si et seulement si $p = 1$.
- A est une matrice **ligne** si et seulement si $n = 1$.

– Si $A = (a_{ij})_{1\leq i,j\leq n}$ est carrée d'ordre n, les a_{ii} $(1 \leq i \leq n)$ sont appelés les **éléments diagonaux** de A et $(a_{11}, \ldots, a_{nn})$ est appelé la **diagonale** de A.

Notation 6.2.1 Pour $(n,p) \in (\mathbb{N}^\star)^2$, on note $\mathcal{M}_{n,p}(K)$ l'ensemble des matrices à n lignes et p colonnes, et à éléments dans K.
Soit $A = (a_{ij})_{1\leq i\leq n, 1\leq j\leq p} \in \mathcal{M}_{n,p}(K)$:

– Pour $i \in \{1, \ldots, n\}$, la matrice ligne $(a_{ij})_{1\leq j\leq p} = (a_{i1}, \ldots, a_{ip})$ de $\mathcal{M}_{1,p}(K)$ est appelée la i-ième ligne de A.

– Pour $j \in \{1, \ldots, p\}$, la matrice colonne $(a_{ij})_{1\leq j\leq n} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}$ de $\mathcal{M}_{n,1}(K)$ est appelée la j-ième colonne de A.

6.2.2 Matrices et applications linéaires

Définition 6.2.2 *Soient E un K-ev, $n = dim(E)$, $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E, $x \in E$, $(x_1, \ldots, x_n)$ les composantes de x dans la base $\mathcal{B}$: $x = \sum_{i=1}^{n} x_i e_i$.*

*La matrice colonne $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ s'appelle la **matrice colonne (des composantes) de x dans $\mathcal{B}$** et est notée $Mat_{\mathcal{B}}(x)$.*

Il est clair que l'application $\begin{array}{rccc} Mat_{\mathcal{B}} : & E & \to & \mathcal{M}_{n,1}(K) \\ & x & \mapsto & Mat_{\mathcal{B}}(x) \end{array}$ est une bijection.
Lorsque $X = Mat_{\mathcal{B}}(x)$, on dit que x est représenté par x dans la base $\mathcal{B}$, ou que x représente x dans $\mathcal{B}$.

Définition 6.2.3 *Soient E un K-ev, $n = dim(E)$, $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E, $p \in \mathbb{N}^\star$, $\mathcal{F} = (V_1, \ldots, V_p)$ un famille finie de p éléments de E et, pour chaque j de $\{1, \ldots p\}$, $(a_{1j}, \ldots, a_{nj})$ les composantes de V_j dans $\mathcal{B}$:*

$$\forall j \in \{1, \ldots, p\},\ V_j = \sum_{i=1}^{n} a_{ij} e_i.$$

*La matrice $(a_{ij})_{1\leq i\leq n, 1\leq j\leq p} = \begin{pmatrix} a_{11} & \ldots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{np} \end{pmatrix}$ de $\mathcal{M}_{n,p}(K)$ s'appelle la **matrice de la famille** $(V_1, \ldots, V_p)$ **relativement à la base** $\mathcal{B}$ et est notée $Mat_{\mathcal{B}}(\mathcal{F})$.*

Définition 6.2.4

1. *Soient E, F deux K-ev, $p = dim(E)$, $n = dim(F)$, $\mathcal{B} = (e_1, \ldots, e_p)$ une base de E, $\mathcal{C} = (f_1, \ldots, f_n)$ une base de F, $f \in \mathcal{L}(E,F)$. Pour chaque j de $\{1, \ldots, p\}$, notons $(a_{1j}, \ldots, a_{nj})$ les composantes de $f(e_j)$ dans $\mathcal{C}$:*

$$f(e_j) = \sum_{i=1}^{n} a_{ij} f_i.$$

*On appelle **matrice de f relativement aux bases $\mathcal{B}$ et $\mathcal{C}$**, et on note$Mat_{\mathcal{B},\mathcal{C}}(f)$ la matrice de $\mathcal{M}_{n,p}(K)$ définie par :*

$$Mat_{\mathcal{B},\mathcal{C}}(f) = (a_{ij})_{1\leq i\leq n, 1\leq j\leq p}.$$

2. *Soient E un K-ev, $n = dim(E)$, $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E, $f \in \mathcal{L}(E)$. On appelle* ***matrice de f relativement à la base $\mathcal{B}$****, et on note $Mat_{\mathcal{B}}(f)$, la matrice de $\mathcal{M}_n(K)$ définie par :*

$$Mat_{\mathcal{B}}(f) = Mat_{\mathcal{B},\mathcal{B}}(f).$$

Il est clair que l'application $\begin{array}{rcl} Mat_{\mathcal{B},\mathcal{C}} : \mathcal{L}(E,F) & \to & \mathcal{M}_{n,p}(K) \\ f & \mapsto & Mat_{\mathcal{B},\mathcal{C}}(f) \end{array}$ est une bijection.

Lorsque $A = Mat_{\mathcal{B},\mathcal{C}}(f)$, on dit que f est représentée par A dans les bases $\mathcal{B}, \mathcal{C}$, ou que A représente f dans les bases $\mathcal{B}, \mathcal{C}$.

6.2.3 L'espace vectoriel $\mathcal{M}_{n,p}(K)$

On "transporte" la structure vectorielle de $\mathcal{L}(E,F)$ sur $\mathcal{M}_{n,p}(K)$, grâce à la bijection $Mat_{\mathcal{B},\mathcal{C}}$ où $\mathcal{B} = (e_1, \ldots, e_p)$ et $\mathcal{C} = (f_1, \ldots, f_n)$ sont des bases fixées de E, F respectivement. Soient $\lambda \in K$, $f, g \in \mathcal{L}(E,F)$, $A = (a_{ij})_{ij} = Mat_{\mathcal{B},\mathcal{C}}(f)$, $B = (b_{ij})_{ij} = Mat_{\mathcal{B},\mathcal{C}}(g)$. On a donc :

$$\forall j \in \{1, \ldots, p\}, \begin{cases} f(e_j) = \sum_{i=1}^{n} a_{ij} f_i \\ g(e_j) = \sum_{i=1}^{n} b_{ij} f_i \end{cases}$$

d'où : $\forall j \in \{1, \ldots, p\}$, $(\lambda f + g)(e_j) = \sum_{i=1}^{n} (\lambda a_{ij} + b_{ij}) f_i$.

Ceci nous amène à la définition suivante :

Définition 6.2.5

1. *On appelle* ***addition*** *dans $\mathcal{M}_{n,p}(K)$ la loi interne, notée $+$, définie par :*

$$\forall (a_{ij})_{ij} \in \mathcal{M}_{n,p}(K),\ \forall (b_{ij})_{ij} \in \mathcal{M}_{n,p}(K), (a_{ij})_{ij} + (b_{ij})_{ij} = (a_{ij} + b_{ij})_{ij}.$$

2. *On appelle* ***multiplication par les scalaires*** *la loi externe $K \times \mathcal{M}_{n,p}(K) \to \mathcal{M}_{n,p}(K)$, notée par un point (ou par l'absence de symbole) définie par :*

$$\forall \alpha \in K,\ \forall (a_{ij})_{ij} \in \mathcal{M}_{n,p}(K),\ \alpha (a_{ij})_{ij} = (\alpha a_{ij})_{ij}.$$

Proposition 6.2.1

1. *$(\mathcal{M}_{n,p}(K), +, .)$ est un K-ev.*
2. *Pour tous K-ev E (de dimension p) et F (de dimension n) et pour toutes bases $\mathcal{B}$ de E et $\mathcal{C}$ de F, l'application $\begin{array}{rcl} Mat_{\mathcal{B},\mathcal{C}} : \mathcal{L}(E,F) & \to & \mathcal{M}_{n,p}(K) \\ f & \mapsto & Mat_{\mathcal{B},\mathcal{C}}(f) \end{array}$ est un isomorphisme de K-ev.*

Preuve : L'application $Mat_{\mathcal{B},\mathcal{C}}$ est bijective et :

$$\forall \alpha \in K,\ \forall (f,g) \in (\mathcal{L}(E,F))^2,\ Mat_{\mathcal{B},\mathcal{C}}(\alpha f + g) = \alpha Mat f_{\mathcal{B},\mathcal{C}}(f) + Mat_{\mathcal{B},\mathcal{C}}(g).$$

Il en résulte aisément, par transport de structure que $\mathcal{M}_{n,p}(K)$ est un K-ev et que $Mat_{\mathcal{B},\mathcal{C}}$ est un isomorphisme de K-ev. ∎

Notation 6.2.2

1. On note $O_{n,p}$ ou plus simplement 0 (ou O) la matrice de $\mathcal{M}_{n,p}(K)$ dont tous les termes sont nuls.

2. Pour $(n,p) \in (\mathbb{N}^\star)^2$ et $(i,j) \in \{1,\dots,n\} \times \{1,\dots,p\}$, on note E_{ij} la matrice de $\mathcal{M}_{n,p}(K)$ dont le (i,j)-ième terme vaut 1 et tous les autres sont nuls. Les matrices E_{ij} sont appelées les **matrices élémentaires**.

Remarque 6.2.2

1. Dans la notation E_{ij}, on omet de rappeler le format (n,p).
2. En notant δ le **symbole de Kronecker**, défini par $\delta_{xy} = \begin{cases} 1 & \text{si} \quad x = y \\ 0 & \text{si} \quad x \neq y \end{cases}$, on a clairement : $E_{ij} = (\delta_{ki}\delta_{ij})_{\substack{1 \leq k \leq n \\ 1 \leq l \leq p}}$.

Proposition 6.2.2

1. *$(E_{ij})_{(i,j)\in\{1,\dots,n\}\times\{1,\dots,p\}}$ est une base de $\mathcal{M}_{n,p}(K)$ appelée **base canonique** de $\mathcal{M}_{n,p}(K)$.*
2. *$dim(\mathcal{M}_{n,p}(K)) = np$.*

Preuve :

1. Il est clair que, pour toute matrice $A = (a_{ij})_{ij}$ de $\mathcal{M}_{n,p}(K)$ on a : $A = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} a_{ij}E_{ij}$, ce qui montre que $(E_{ij})_{ij}$ engendre $\mathcal{M}_{n,p}(K)$.
2. Si $(a_{ij})_{ij}$ vérifie $\sum_{i,j} a_{ij}E_{ij} = 0$ alors $(a_{ij})_{ij} = 0$ ce qui montre que $(E_{ij})_{ij}$ est libre. ■

Exercice 104 Soient $A = \begin{pmatrix} -1 & 2 \\ 1 & 0 \end{pmatrix}$ et f l'application de $\mathcal{M}_2(\mathbb{R})$ dans $\mathcal{M}_2(\mathbb{R})$ définie par $f(M) = AM$.

1. Montrer que f est linéaire.
2. Déterminer sa matrice dans la base canonique de $\mathcal{M}_2(\mathbb{R})$.

Correction :

1. Évident.
2. On rappelle que la base canonique de $\mathcal{M}_2(\mathbb{R})$ est la base $(E_{1,1}, E_{1,2}, E_{2,1}, E_{2,2})$ avec
$$E_{1,1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ E_{1,2} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ E_{2,1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ E_{2,2} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$
Il suffit de calculer l'image par f de ces matrices, et de les exprimer dans la base canonique. On a
$$\begin{aligned} f(E_{1,1}) &= \begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix} = -1E_{1,1} + 0E_{1,2} + 1E_{2,1} + 0E_{2,2}, \\ f(E_{1,2}) &= \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} = 0E_{1,1} - 1E_{1,2} + 0E_{2,1} + 1E_{2,2}, \\ f(E_{2,1}) &= \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} = 2E_{1,1} + 0E_{1,2} + 0E_{2,1} + 0E_{2,2}, \\ f(E_{2,2}) &= \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = 0E_{1,1} + 2E_{1,2} + 0E_{2,1} + 0E_{2,2}. \end{aligned}$$
La matrice de f dans la base canonique de $\mathcal{M}_2(\mathbb{R})$ est donc $\begin{pmatrix} -1 & 0 & 2 & 0 \\ 0 & -1 & 0 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$.

6.2.4 Multiplication des matrices

Soient E, F, G trois K-ev de dimensions respectives q, p, n, $\mathcal{B} = (e_1, \ldots, e_q)$, $\mathcal{C} = (f_1, \ldots, f_p)$, $\mathcal{D} = (g_1, \ldots, g_n)$ des bases de E, F, G respectivement, $f \in \mathcal{L}(E, F)$, $g \in \mathcal{L}(F, G)$, $A = (a_{jk})_{jk} = Mat_{\mathcal{B},\mathcal{C}}(f)$, $B = (b_{ij})_{ij} = Mat_{\mathcal{C},\mathcal{D}}(g)$. On va déterminer la matrice de $g \circ f$ relativement aux bases $\mathcal{B}$ et $\mathcal{D}$. Soit $k \in \{1, \ldots, q\}$. On a par définition de A, $f(e_k) = \sum_{j=1}^{p} a_{jk} f_j$. D'où $(g \circ f)(e_k) = g\left(\sum_{j=1}^{p} a_{jk} f_j\right) = \sum_{j=1}^{p} a_{jk} g(f_j)$.

Par définition de B, $\forall j \in \{1, \ldots, p\}$, $g(f_j) = \sum_{i=1}^{n} b_{ij} g_i$. Donc $(g \circ f)(e_k) = \sum_{j=1}^{p} a_{jk} \left(\sum_{i=1}^{n} b_{ij} g_i\right) = \sum_{j=1}^{p} \sum_{i=1}^{n} b_{ij} a_{jk} g_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{p} b_{ij} a_{jk}\right) g_i$. Donc $Mat_{\mathcal{B},\mathcal{D}}(g \circ f) = (c_{ik})_{ik}$ où $\forall (i, k) \in \{1, \ldots, n\} \times \{1, \ldots, q\}$, $c_{ik} = \sum_{j=1}^{p} b_{ij} a_{jk}$. Ceci nous amène à la définition suivante, après échange de A et B.

Définition 6.2.6 *Soient $A = (a_{ij})_{ij} \in \mathcal{M}_{n,p}(K)$, $B = (b_{jk})_{jk} \in \mathcal{M}_{p,q}(K)$. On appelle **produit de A par B**, et on note AB la matrice de $\mathcal{M}_{n,p}(K)$ définie par $AB = (c_{ik})_{ik}$ où*

$$\forall (i, k) \in \{1, \ldots, n\} \times \{1, \ldots, q\},\ c_{ik} = \sum_{j=1}^{p} a_{ij} b_{jk}.$$

L'application $\begin{array}{ccc} \mathcal{M}_{n,p}(K) \times \mathcal{M}_{p,q}(K) & \to & \mathcal{M}_{n,q}(K) \\ (A, B) & \mapsto & AB \end{array}$ s'appelle la **multiplication des matrices**. Nous avons montré le résultat suivant :

Proposition 6.2.3 *Soient E, F, G trois K-ev, $\mathcal{B}, \mathcal{C}, \mathcal{D}$ des bases de E, F, G respectivement, $f \in \mathcal{L}(E, F), x \in E$. On a :*

$$Mat_{\mathcal{B},\mathcal{D}}(g \circ f) = Mat_{\mathcal{C},\mathcal{D}}(g) Mat_{\mathcal{B},\mathcal{C}}(f).$$

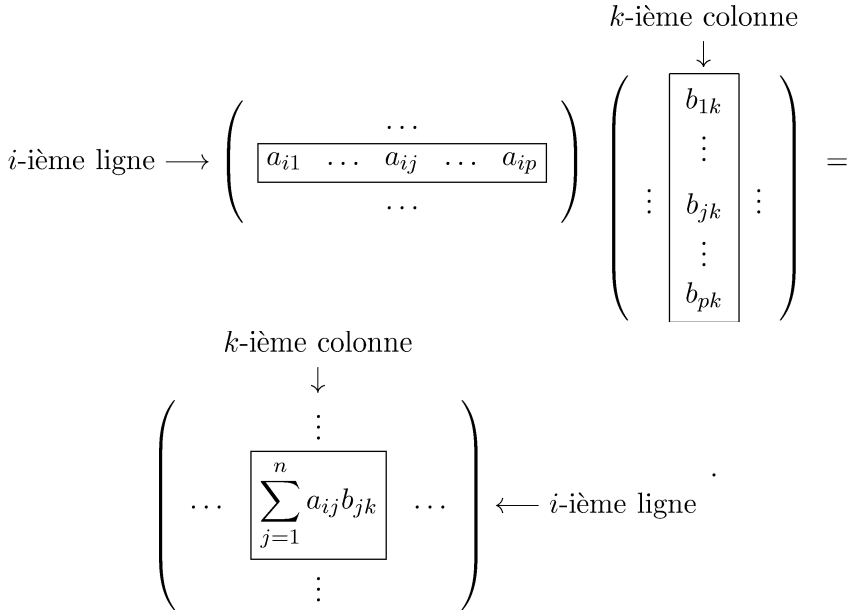
Proposition 6.2.4 *Soient E, F deux K-ev, $\mathcal{B}, \mathcal{C}$ des bases de E, F respectivement, $f \in \mathcal{L}(E, F), x \in E$. On a :*

$$Mat_{\mathcal{C}}(f(x)) = Mat_{\mathcal{B},\mathcal{C}}(f) Mat_{\mathcal{B}}(x).$$

Preuve : Notons $\mathcal{B} = (e_1, \ldots, e_p)$, $\mathcal{C} = (f_1, \ldots, f_n)$, $X = Mat_{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$, $A = Mat_{\mathcal{B},\mathcal{C}}(f) = (a_{ij})_{\substack{1 \le i \le n \\ 1 \le j \le p}}$. On a

$$f(x) = f\left(\sum_{j=1}^{p} x_j e_j\right) = \sum_{j=1}^{p} x_j f(e_j) = \sum_{j=1}^{p} \left(x_j \sum_{i=1}^{n} a_{ij} f_i\right) = \sum_{j=1}^{p} \sum_{i=1}^{n} a_{ij} x_j f_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{p} a_{ij} x_j\right) f_i,$$

d'où $Mat_{\mathcal{C}}(f(x)) = \left(\sum_{j=1}^{p} a_{ij} x_j\right)_{1 \le i \le n} = AX$. En pratique, pour effectuer le produit AB de deux matrices, on utilise la disposition suivante :



Remarque 6.2.3 Si $A \in \mathcal{M}_{n,p}(K)$ et $B \in \mathcal{M}_{p,q}(K)$ alors $AB \in \mathcal{M}_{n,q}(K)$. Ainsi le format (n,q) de AB est obtenu à partir des formats (n,p) de A et (p,q) de B "comme par la relation de Chasles".

Proposition 6.2.5

1. *Pseudo-distributivité à gauche :*
$$\forall A \in \mathcal{M}_{n,p}(K),\ \forall B,C \in \mathcal{M}_{p,q}(K),\ A(B+C) = AB + AC,$$
2. *Pseudo-distributivité à droite :*
$$\forall A,B \in \mathcal{M}_{n,p}(K),\ \forall C \in \mathcal{M}_{p,q}(K),\ (A+B)C = AC + BC,$$
3. $\forall \lambda \in K,\ \forall A \in \mathcal{M}_{n,p}(K),\ \forall B \in \mathcal{M}_{p,q}(K)$
$$(\lambda A)B = \lambda(AB) = A(\lambda B),$$
4. *Pseudo-associativité :*
$$\forall A \in \mathcal{M}_{n,p}(K),\ \forall B \in \mathcal{M}_{p,q}(K),\ \forall C \in \mathcal{M}_{q,r}(K),\ (AB)C = A(BC).$$

Proposition 6.2.6

1. $(\mathcal{M}_n(K), +, ., \times)$ *est une K-algèbre associative et unitaire.*
2. *Pour tout K-ev E de dimension n et toute base $\mathcal{B}$ de E, l'application* $\begin{array}{rcl} Mat_{\mathcal{B}} : \mathcal{L}(E) & \to & \mathcal{M}_n(K) \\ f & \mapsto & Mat_{\mathcal{B}}(f) \end{array}$
est un isomorphisme de K-algèbres unitaires.

Preuve : On a déja vu que $(\mathcal{M}_n(K), +)$ est un K-ev et que la multiplication est interne dans $\mathcal{M}_n(K)$. Comme $Mat_{\mathcal{B}}$ est bijective, que $\forall (f,g) \in (\mathcal{L}(E))^2$, $Mat_{\mathcal{B}}(g \circ f) = Mat_{\mathcal{B}}(g)Mat_{\mathcal{B}}(f)$, et que $(\mathcal{L}(E), +, ., \circ)$ est une K-algèbre associative et unitaire, par transport de structure, $(\mathcal{M}_n(K), +, ., \circ)$ est aussi une K-algèbre associative et unitaire, et $Mat_{\mathcal{B}}$ est un isomorphisme de K-algèbres unitaires. ■

Notation 6.2.3 On note $I_n = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \in \mathcal{M}_n(K)$, qui est l'élément neutre de la multiplication dans $\mathcal{M}_n(K)$.

Remarque 6.2.4

1. Si $n \geq 2$, l'algèbre $\mathcal{M}_n(K)$ n'est pas commutative, comme le montre (pour $n = 2$) l'exemple :
$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$
2. Si $n \geq 2$, il se peut que le produit de deux matrices de $\mathcal{M}_n(K)$ soit nul sans qu'aucune des deux matrices ne soit nulle, comme le montre (pour $n = 2$) l'exemple :
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$
3. On confond souvent un élément x de K et la matrice (x) de $\mathcal{M}_1(K)$.
   - Soit $A \in \mathcal{M}_{n,1}(K)$, on a $A(x) = xA$, mais $(x)A$ n'est pas définie (si $n \geq 2$).
   - Soit $B \in \mathcal{M}_{1,n}(K)$, on a $(x)B = xB$, mais $B(x)$ n'est pas définie (si $n \geq 2$).

Définition 6.2.7 *Une matrice carrée A de $\mathcal{M}_n(K)$ est dite **nilpotente** si et seulement s'il existe $k \in \mathbb{N}^\star$ tel que $A^k = 0$.*

Exemple 6.2.1

1. $A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$ est nilpotente car $A^2 = 0$.
2. $B = \begin{pmatrix} -9 & 7 & 3 \\ -13 & 10 & 4 \\ 4 & -3 & -1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$ est nilpotente car $A^3 = 0$.

Proposition 6.2.7 *Soit $A \in \mathcal{M}_n(K)$ nilpotente. L'ensemble $\{k \in \mathbb{N}^\star, A^k = 0\}$ admet un plus petit élément $\nu(A)$ appelé **indice de nilpotence** de A et on a :*
$$\forall k \in \mathbb{N}^\star,\ k \geq \nu(A) \Rightarrow A^k = 0.$$

Preuve :

- $\{k \in \mathbb{N}^\star, A^k = 0\}$ est une partie non vide de $\mathbb{N}^\star$ donc admet un plus petit élément $\nu(A)$.
- Pour tout k tel que $k \geq \nu(A)$: $A^k = A^{k-\nu(A)}A^{\nu(A)} = 0$. ■

Définition 6.2.8 *Soit $A \in \mathcal{M}_{n,p}(K)$.*

1. *On appelle **noyau** de A le sev de $\mathcal{M}_{p,1}(K)$ noté $Ker(A)$, défini par :*
$$Ker(A) = \{X \in \mathcal{M}_{p,1}(K), AX = 0\}$$
2. *On appelle **image** de A le sev de $\mathcal{M}_{n,1}(K)$ noté $Im(A)$ défini par :*
$$Im(A) = \{Y \in \mathcal{M}_{n,1}(K), \exists X \in \mathcal{M}_{p,1}(K), Y = AX\} = \{AX, X \in \mathcal{M}_{p,1}(K)\}.$$

Soit $A \in \mathcal{M}_{n,p}(K)$. En notant $\begin{array}{rccc} f : & \mathcal{M}_{p,1}(K) & \to & \mathcal{M}_{n,1}(K) \\ & X & \mapsto & AX \end{array}$, f est linéaire et $Ker(f) = Ker(A)$ et $Im(f) = Im(A)$. Les notations $Ker(A)$ et $Im(A)$ incitent à considérer A comme une application linéaire.

Exercice 105 On considère l'endomorphisme f de $\mathbb{R}^3$ dont la matrice dans la base canonique est :
$$\begin{pmatrix} 1 & 1 & 1 \\ -1 & 2 & -2 \\ 0 & 3 & -1 \end{pmatrix}.$$

Donner une base de $Ker(f)$ et de $Im(f)$.
Correction : Le noyau de f est l'ensemble des triplets (x, y, z) tels que

$$f(x,y,z) = 0 \Leftrightarrow \left\{ \begin{array}{rcl} x+y+z & = & 0 \\ -x+2y-2z & = & 0 \\ 3y-z & = & 0 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} x & = & -4y \\ y & = & y \\ z & = & 3y \end{array} \right. .$$

Le noyau de f est donc la droite vectorielle de vecteur directeur $(-4, 1, 3)$. Déterminer $Ker(A)$ revient donc à trouver $X = (x, y, z) \neq 0$ tel que $AX = 0$.
Par le théorème du rang, $Im(f)$ est de dimension 2. De plus, $f(e_1) = (1, -1, 0)$ et $f(e_2) = (1, 2, 3)$ sont clairement indépendants. Donc $(f(e_1), f(e_2))$ est une base de $Im(f) = Im(A)$.

Exercice 106 On considère l'endomorphisme f de $\mathbb{R}^3$ dont la matrice dans la base canonique est :

$$\begin{pmatrix} 1 & 1 & -1 \\ -3 & -3 & 3 \\ -2 & -2 & 2 \end{pmatrix}.$$

Donner une base de $Ker(f)$ et de $Im(f)$. En déduire que $M^n = 0$ pour tout $n \geq 2$.
Correction : On a

$$f(x,y,z) = 0 \Leftrightarrow x+y-z = 0 \Leftrightarrow \left\{ \begin{array}{rcl} x & = & x \\ y & = & y \\ z & = & x+y \end{array} \right. .$$

$Ker(f)$ est donc un plan vectoriel de base (u, v) avec $u = (1, 0, 1)$ et $v = (0, 1, 1)$. D'après le théorème du rang, on sait que $Im(u)$ est de dimension 1. Il est engendré par exemple par le vecteur non nul $w = f(e_1) = (1, -3, -2)$.
On remarque que $w = u - 3v$ est élément de $Ker(f)$. Ainsi, $Im(f) \subset Ker(f)$ et donc $f^2 = 0$. Ensuite, $f^n = 0$ pour tout $n \geq 2$ et la matrice de f dans la base canonique de $\mathbb{R}^3$ est elle aussi nulle. Donc $M^n = 0$ pour tout $n \geq 2$.

6.2.5 Le groupe $GL_n(K)$

Soit $n \in \mathbb{N}^\star$.

Définition 6.2.9 *Une matrice A de $\mathcal{M}_n(K)$ est dite **inversible** si et seulement s'il existe $A' \in \mathcal{M}_n(K)$ telle que $AA' = A'A = I_n$.*
Si A est inversible alors A' est unique et appelée inverse de A et est notée A^{-1}.
On note $GL_n(K)$ l'ensemble des matrices inversibles de $\mathcal{M}_n(K)$.

Proposition 6.2.8

1. *La multiplication est interne dans $GL_n(K)$ et $(GL_n(K), .)$ est un groupe appelé **groupe linéaire**.*
2. *Pour tout K-ev E de dimension n et toute base $\mathcal{B}$ de E, l'application $f \mapsto Mat_{\mathcal{B}}(f)$ est un isomorphisme du groupe $(\mathcal{GL}(E), \circ)$ sur le groupe $(GL_n(K), .)$.*

Preuve :

1. – Pour tout (A, B) de $(GL_n(K))^2$, $(A, B)(B^{-1}A^{-1}) = I_n$ et $(B^{-1}A^{-1})(AB) = I_n$ donc $AB \in GL_n(K)$.
   – $I_n \in GL_n(K)$.
2. – Pour toute f de $\mathcal{GL}(E)$ comme $Mat_{\mathcal{B}}(f)Mat_{\mathcal{B}}(f^{-1}) = Mat_{\mathcal{B}}(f^{-1})Mat_{\mathcal{B}}(f) = Mat_{\mathcal{B}}(Id_E) = I_n$, on a $Mat_{\mathcal{B}}(f) \in GL_n(K)$.

– Réciproquement, pour toute matrice $A \in GL_n(K)$, il existe $(f,g) \in (\mathcal{L}(E))^2$ unique tel que $Mat_{\mathcal{B}}(f) = A$ et $Mat_{\mathcal{B}}(g) = A^{-1}$ et on a
$$\begin{cases} Mat_{\mathcal{B}}(g \circ f) = Mat_{\mathcal{B}}(g)Mat_{\mathcal{B}}(f) = A^{-1}A = I_n, \\ Mat_{\mathcal{B}}(f \circ g) = Mat_{\mathcal{B}}(f)Mat_{\mathcal{B}}(g) = AA^{-1} = I_n, \end{cases}$$
donc $g \circ f = f \circ g = Id_E$ d'où $f \in \mathcal{GL}(E)$.
– Enfin, $\forall (f,g) \in (\mathcal{GL}(E))^2$, $Mat_{\mathcal{B}}(g \circ f) = Mat_{\mathcal{B}}(g)Mat_{\mathcal{B}}(f)$. ■

Remarque 6.2.5 Pour $n \geq 2$ le groupe $GL_n(K)$ n'est pas commutatif, comme le montre (pour $n = 2$) l'exemple suivant :
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

Du théorème 5.4.2 (Chapitre 5 - Applications linéaires), on déduit le théorème suivant :

Théorème 6.2.1 *Soient $A \in \mathcal{M}_n(K)$ et f un endomorphisme représenté par A dans une base. Les propriétés suivantes sont deux à deux équivalentes :*

1. *f est bijective,*
2. *A est inversible à gauche,*
3. *A est inversible à droite,*
4. *A est inversible,*
5. *A est régulière à gauche,*
6. *A est régulière à droite,*
7. *A est régulière.*

Rappelons que A est dite :
– **régulière à gauche** si et seulement si :
$$\forall (B,C) \in (\mathcal{M}_n(K))^2,\ AB = AC \Rightarrow B = C,$$
– **régulière à droite** si et seulement si :
$$\forall (B,C) \in (\mathcal{M}_n(K))^2,\ BA = CA \Rightarrow B = C,$$
– **régulière** si et seulement si A est régulière à gauche et régulière à droite.

Remarque 6.2.6 Une matrice A de $\mathcal{M}_n(K)$ est inversible si et seulement si :
$$\forall X \in \mathcal{M}_{n,1}(K),\ AX = 0 \Rightarrow X = 0$$
On verra plus loin (plus tard) d'autres caractérisations de l'inversibilité d'une matrice carrée faisant intervenir le rang, le déterminant, les valeurs propres.
Le calcul pratique de A^{-1} se fait de la manière suivante : en notant $AX = Y$ où $X, Y \in \mathcal{M}_{n,1}(K)$, on exprime X en fonction de Y par résolution d'un système linéaire (car si A est inversible, $AX = Y \Leftrightarrow X = A^{-1}Y$). Cependant, pour des matrices carrées de grande taille, on utilisera un logiciel de calcul d'inverse des matrices inversibles (Matlab, Mathematica, Maple, Scilab, Octave,...)

6.2.6 Rang d'une matrice

Définition 6.2.10 *Soit $A \in \mathcal{M}_{n,p}(K)$. On appelle **rang** de A et on note $rg(A)$ le rang de la famille des colonnes de A dans $\mathcal{M}_{n,1}(K)$.*

Ainsi en notant $A = \begin{pmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{np} \end{pmatrix}$ et $C_1 = \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \dots, C_p = \begin{pmatrix} a_{1p} \\ \vdots \\ a_{np} \end{pmatrix}$ les colonnes de A, on a $rg(A) = rg(C_1, \dots, C_p)$.

Proposition 6.2.9 *Soient E, F deux K-ev, $\mathcal{B}$ et $\mathcal{C}$ des bases de E et F respectivement, $f \in \mathcal{L}(E,F)$, $A = Mat_{\mathcal{B},\mathcal{C}}(f)$. On a $rg(f) = rg(A)$.*

Preuve : Notons $\mathcal{B} = (e_1, \ldots, e_n)$, $\mathcal{C} = (f_1, \ldots, f_n)$, $A = (a_{ij})_{ij}$, $C_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}$ pour $1 \leq j \leq p$. On a $\forall j \in \{1, \ldots, p\}$, $f(e_j) = \sum_{i=1}^{n} a_{ij} f_i$. Puisque $\theta : \mathcal{M}_{n,1}(K) \to F$, $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \sum_{i=1}^{n} x_i f_i$ est un isomorphisme de K-ev, on a $rg(A) = dim(Vect(C_1, \ldots, C_p)) = dim(Vect(\theta(C_1), \ldots, \theta(C_p))) = dim(Vect(f(e_1), \ldots, f(e_p))) = rg(f)$. ■

Ainsi,
- le rang d'une matrice A est le rang de n'importe quelle application linéaire représentée par A,
- le rang d'une application linéaire f est le rang de n'importe quelle matrice représentant f,
- le rang d'une famille finie $\mathcal{F}$ de vecteurs d'un K-ev E est le rang de $\mathcal{F}$ dans n'importe quelle base de E.

Proposition 6.2.10 $\forall A \in \mathcal{M}_{n,p}(K)$, $rg(A) \leq \min(n,p)$

Preuve : Avec les notations précédentes :
- $rg(A) = rg(C_1, \ldots, C_p) \leq p$,
- $rg(A) = dim(Vect(C_1, \ldots, C_p)) \leq dim(\mathcal{M}_{n,1}(K)) = n$. ■

Proposition 6.2.11 $\forall A \in \mathcal{M}_n(K)$, $rg(A) = n \Leftrightarrow A \in GL_n(K)$.

Preuve : Soit f l'endomorphisme de $\mathcal{M}_{n,1}(K)$ représenté par A dans la base canonique de $\mathcal{M}_{n,1}(K)$. Comme $(C_1, \ldots, C_n)$ est une base de $\mathcal{M}_{n,1}(K)$ si et seulement si f est bijective, on conclut que $rg(A) = n \Leftrightarrow A \in GL_n(K)$. ■

Proposition 6.2.12 $\forall A \in \mathcal{M}_{n,p}(K)$, $\begin{cases} \forall P \in GL_p(K) & rg(AP) = rg(A) \\ \forall Q \in GL_n(K) & rg(QA) = rg(A) \end{cases}$

Preuve :

1. Il est clair que $Im(AP) \subset Im(A)$ d'où $rg(AP) \leq rg(A)$. En remplaçant (A, P) par (AP, P^{-1}), on déduit $rg(A) = rg((AP)P^{-1}) \leq rg(AP)$.
2. Il est clair que $Ker(A) \subset Ker(QA)$ d'où, d'après le théorème du rang, $rg(A) = p - dim(Ker(A)) \geq p - dim(Ker(Q(A)) = rg(QA)$. En remplaçant (A, Q) par (QA, Q^{-1}), on déduit $rg(QA) \geq rg(Q^{-1}(QA)) = rg(A)$. ■

Remarque 6.2.7 On montre de façon analogue : $\forall (A, B, C) \in \mathcal{M}_{n,p}(K) \times \mathcal{M}_{p,q}(K) \times \mathcal{M}_{q,r}(K)$, $rg(ABC) \leq rg(B)$.

6.2.7 Transposition

Définition 6.2.11 *Pour toute matrice $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} = \begin{pmatrix} a_{11} & \ldots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{np} \end{pmatrix}$ de $\mathcal{M}_n(K)$, on appelle* ***transposée*** *de A la matrice, notée ${}^tA$, de $\mathcal{M}_{p,n}(K)$ définie par :*

$$ {}^tA = (a_{ji})_{\substack{1 \le j \le p \\ 1 \le i \le n}} = \begin{pmatrix} a_{11} & \dots & a_{n1} \\ \vdots & & \vdots \\ a_{1p} & \dots & a_{np} \end{pmatrix}. $$

Exemple 6.2.2 Si $A = \begin{pmatrix} a & b & c \\ \alpha & \beta & \gamma \end{pmatrix}$ alors ${}^tA = \begin{pmatrix} a & \alpha \\ b & \beta \\ c & \gamma \end{pmatrix}$.

En particulier, la transposée d'une matrice ligne est une matrice colonne et réciproquement :

$$ {}^t(x_1, \dots, x_n) = {}^t\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (x_1 \dots x_n), \quad {}^t(x_1 \dots x_n) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (x_1, \dots, x_n). $$

Proposition 6.2.13

1. $\forall A \in \mathcal{M}_{n,p}(K),\ {}^t({}^tA) = A.$
2. $\forall \alpha \in K,\ \forall (A,B) \in (\mathcal{M}_{n,p}(K))^2,\ {}^t(\alpha A + B) = \alpha\, {}^tA + {}^tB.$
3. $\forall A \in \mathcal{M}_{n,p}(K),\ \forall B \in \mathcal{M}_{p,q}(K),\ {}^t(AB) = {}^tB\, {}^tA.$
4. $\forall A \in GL_n(K),\ {}^tA \in GL_n(K)$ *et* $({}^tA)^{-1} = {}^t(A^{-1}).$

Preuve :

1. Immédiat.
2. En notant $A = (a_{ij})_{ij}$, $B = (b_{ij})_{ij}$, on a $\alpha A + B = (\alpha a_{ij} + b_{ij})_{ij}$ donc ${}^t(\alpha A + B) = (\alpha a_{ij} + b_{ij})_{ji}$ et $\alpha\, {}^tA + {}^tB = \alpha (a_{ij})_{ji} + (b_{ij})_{ji} = (\alpha a_{ij} + b_{ij})_{ji}$, d'où ${}^t(\alpha A + B) = \alpha\, {}^tA + {}^tB$.
3. En notant $A = (a_{ij})_{ij}$, $B = (b_{jk})_{jk}$, on a ${}^tA = (\alpha_{ji})_{ji}$, ${}^tB = (\beta_{kj})_{kj}$ où $\alpha_{ji} = a_{ij}$ et $\beta_{kj} = b_{jk}$, et $AB = (c_{ik})_{ik}$, ${}^tB\, {}^tA = (\gamma_{ki})_{ki}$ où $c_{ik} = \sum_{j=1}^{p} \beta_{kj}\alpha_{ji} = \sum_{j=1}^{p} b_{jk}a_{ij} = c_{ik}$. Ainsi, ${}^tB\, {}^tA = {}^t(AB)$.
4. Soit $A \in GL_n(K)$. Puisque ${}^tA\, {}^t(A^{-1}) = {}^t(A^{-1}A) = {}^tI_n = I_n$, ${}^tA$ est inversible et $({}^tA)^{-1} = {}^t(A^{-1})$. ■

6.2.8 Trace d'une matrice carrée

Définition 6.2.12 *Pour toute matrice carrée $A = (a_{ij})_{ij} \in \mathcal{M}_n(K)$, on définit la* ***trace*** *de A, notée $tr(A)$ par : $tr(A) = \sum_{i=1}^{n} a_{ii}$.*

Proposition 6.2.14

1. *L'application* $tr : \begin{array}{ccc} \mathcal{M}_n(K) & \to & K \\ A & \mapsto & tr(A) \end{array}$ *est une forme linéaire.*
2. $\forall A \in \mathcal{M}_{n,p}(K),\ \forall B \in \mathcal{M}_{p,n}(K),\ {}^t(AB) = {}^t(BA).$

Preuve :

1. En notant $A = (a_{ij})_{ij}$, $B = (b_{ij})_{ij}$, ${}^t(\alpha A + B) = \sum_{i=1}^{n} \alpha a_{ii} + \sum_{i=1}^{n} b_{ii} = \alpha\, {}^tA + {}^tB$.
2. On remarque tout d'abord que AB et BA sont carrées. En notant $A = (a_{ij})_{ij}$, $B = (b_{jk})_{jk}$, on a ${}^t(AB) = \sum_{i=1}^{n} \left(\sum_{j=1}^{p} a_{ij}b_{ij} \right) = \sum_{j=1}^{p} \left(\sum_{i=1}^{n} b_{ij}a_{ij} \right) = {}^t(BA)$. ■

6.3 Changement de bases

6.3.1 Matrices de passage

Définition 6.3.1 *Soient E un K-ev de dimension n, $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E. On appelle* ***matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$****, qu'on note $Pass(\mathcal{B},\mathcal{B}')$ la matrice de $\mathcal{M}_n(K)$ dont les colonnes sont formées des composantes des vecteurs de $\mathcal{B}'$ exprimés dans la base $\mathcal{B}$ c'est-à-dire :*

$$Pass(\mathcal{B},\mathcal{B}') = Mat_{\mathcal{B}}(\mathcal{B}').$$

Exemple 6.3.1 Soient $\mathcal{B} = (e_1, e_2)$ la base canonique de K^2 c'est-à-dire $e_1 = (1,0)$ et $e_2 = (0,1)$, et $u = (2,4)$, $v = (3,-1)$. Alors $\mathcal{B}' = (u,v)$ est une base de K^2 et la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$ est $\begin{pmatrix} 2 & 3 \\ 4 & -1 \end{pmatrix}$, puisque $u = 2e_1 + 4e_2$ et $v = 3e_1 - e_2$.

Proposition 6.3.1 *Pour toutes bases $\mathcal{B}$, $\mathcal{B}'$ de E, $Pass(\mathcal{B},\mathcal{B}') = Mat_{\mathcal{B},\mathcal{B}'}(Id_E)$.*

Preuve : Notons $\mathcal{B}' = (e'_1, \ldots, e'_n)$. Pour chaque $j \in \{1, \ldots, n\}$, la j-ième colonne de $Mat_{\mathcal{B}',\mathcal{B}}(Id_E)$ est formée par les composantes de $Id_E(e'_j)$, c'est-à-dire e'_j dans la base $\mathcal{B}$. ■

Proposition 6.3.2 *Soient E un K-ev, $\mathcal{B},\mathcal{B}',\mathcal{B}''$ des bases de E. On a :*

1. $Pass(\mathcal{B},\mathcal{B}') = Pass(\mathcal{B},\mathcal{B}')Pass(\mathcal{B}',\mathcal{B}'')$.
2. $Pass(\mathcal{B},\mathcal{B}) = I_n$.
3. $Pass(\mathcal{B},\mathcal{B}')$ *est inversible et* $(Pass(\mathcal{B},\mathcal{B}'))^{-1} = Pass(\mathcal{B}',\mathcal{B})$.

Preuve :

1. $Pass(\mathcal{B},\mathcal{B}'') = Mat_{\mathcal{B}'',\mathcal{B}}(Id_E) = Mat_{\mathcal{B}',\mathcal{B}}(Id_E)Mat_{\mathcal{B}'',\mathcal{B}'}(Id_E) = Pass(\mathcal{B},\mathcal{B}')Pass(\mathcal{B}',\mathcal{B}'')$.
2. $Pass(\mathcal{B},\mathcal{B}) = Pat_{\mathcal{B},\mathcal{B}}(Id_E) = I_n$
3. $Pass(\mathcal{B},\mathcal{B}')Pass(\mathcal{B}',\mathcal{B}) = Pass(\mathcal{B},\mathcal{B}) = I_n$. ■

Remarque 6.3.1 Soient E un K-ev de dimension n, $\mathcal{B}$ une base de E. L'application $\mathcal{B}' \to Pass(\mathcal{B},\mathcal{B}')$ est clairement une bijection de l'ensemble des bases de E sur $GL_n(K)$. Ainsi :

- Toute matrice de passage est inversible.
- Toute matrice inversible peut être considérée comme matrice de passage.

6.3.2 Changement de base pour un vecteur

Proposition 6.3.3 *Soient E un K-ev, $\mathcal{B},\mathcal{B}'$ deux bases de E, $P = Pass(\mathcal{B},\mathcal{B}')$, $x \in E$, $X = Mat_g(x)$, $X' = Mat_{\mathcal{B}'}(x)$, alors :*

$$X = PX'.$$

Preuve : $X = Mat_{\mathcal{B}}(x) = Mat_{\mathcal{B}',\mathcal{B}}(Id_E)Mat_{\mathcal{B}'}(x) = PX'$. ■

Exemple 6.3.2 Dans K^2, soient (e_1, e_2) la base canonique, $u_1 = (-2,1)$, $u_2 = (3,-2)$, $x = (x_1, x_2) \in K^2$. Il est clair que (u_1, u_2) est une base de K^2. En notant X_1, X_2 les composantes de x dans la base (u_1, u_2), on a :

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -2 & 3 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} -2X_1 + 3X_2 \\ X_1 - 2X_2 \end{pmatrix}.$$

Remarque 6.3.2 Dans un changement de base pour un vecteur, on exprime donc naturellement les anciennes coordonnées (coordonnées de x dans $\mathcal{B}$) en fonction des nouvelles coordonnées (coordonnées de x dans $\mathcal{B}'$). Si on veut exprimer les nouvelles coordonnées de x en fonction des anciennes coordonnées de x, on dispose de la formule $X' = P^{-1}X$, dont l'emploi nécessite le calcul (souvent implicite) de l'inverse de P.

6.3.3 Changement de bases pour une application linéaire

1. **Formule de changement de bases.**

Proposition 6.3.4 *Soient E, F deux K-ev, $\mathcal{B}, \mathcal{B}'$ deux bases de E, $P = Pass(\mathcal{B}, \mathcal{B}')$, $\mathcal{C}, \mathcal{C}'$ deux bases de F, $Q = Pass(\mathcal{C}, \mathcal{C}')$, $f \in \mathcal{L}(E, F)$, $A = Mat_{\mathcal{B},\mathcal{C}}(f)$, $A' = Mat_{\mathcal{B}',\mathcal{C}'}(f)$. Alors :*

$$A' = Q^{-1}AP.$$

Preuve : $A' = Mat_{\mathcal{B}',\mathcal{C}'}(f) = Mat_{\mathcal{B}',\mathcal{C}'}(Id_F \circ f \circ Id_E) = Mat_{\mathcal{C},\mathcal{C}'}(Id_F)Mat_{\mathcal{B},\mathcal{C}}(f)Mat_{\mathcal{B}',\mathcal{B}}(Id_E) = Q^{-1}AP.$ ■

2. **Matrices équivalentes.**

Définition 6.3.2 *Soient $A, B \in \mathcal{M}_{n,p}(K)$. On dit que A est **équivalente à** B, et on note $A \sim B$, si et seulement si :*

$$\exists (P, Q) \in GL_p(K) \times GL_n(K),\ B = Q^{-1}AP.$$

Proposition 6.3.5 *La relation $\sim$ est une relation d'équivalence dans $\mathcal{M}_{n,p}(K)$.*

Preuve :

(a) *Réflexivité* : $\forall A \in \mathcal{M}_{n,p}(K)$, $A = I_n A I_p$.

(b) *Symétrie* : S'il existe $(P, Q) \in GL_p(K) \times GL_n(K)$ tel que $B = Q^{-1}AP$, alors $A = (Q^{-1})^{-1}BP^{-1}$ et $(P^{-1}, Q^{-1}) \in GL_p(K) \times GL_n(K)$ donc $B \sim A$.

(c) *Transitivité* : Supposons $A \sim B$ et $B \sim C$. Il existe $P \in GL_p(K)$, $Q \in GL_n(K)$, $R \in GL_p(K)$, $S \in GL_n(K)$ telles que $B = Q^{-1}AP$ et $C = S^{-1}BR$. Alors $C = S^{-1}Q^{-1}APR = (QS)^{-1}A(PR)$ et $(PR, QS) \in GL_p(K) \times GL_n(K)$, d'où $A \sim C$. ■

Proposition 6.3.6 *Soient $A \in \mathcal{M}_{n,p}(K)$, $r = rg(A)$. Alors A est équivalente à la matrice $J_{n,p,r}$ définie par :*

$$J_{n,p,r} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & \dots & \dots & 0 & 0 & \dots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \dots & \dots & 0 & 0 & \dots & 0 \end{pmatrix} = \begin{pmatrix} I_r & O_{r,p-r} \\ O_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}.$$

(En particulier, $J_{n,p,0} = 0$.)

Preuve : Soient E, F deux K-ev de dimensions respectives p, n (il en existe), $\mathcal{B}$ et $\mathcal{C}$ des bases de E et F, respectivement (il en existe), $f \in \mathcal{L}(E, F)$ représentée par A dans les bases $\mathcal{B}$ et $\mathcal{C}$: $Mat_{\mathcal{B},\mathcal{C}}(f) = A$. D'après le théorème du rang, le sev $Ker(f)$ de E est de dimension $p - r$ donc admet au moins une base $(e_{r+1}, \dots, e_p)$. D'après le théorème de la base incomplète (forme faible), il existe $e_1, \dots, e_r$ de E tels que $\mathcal{B}' = (e_1, \dots, e_r, e_{r+1}, \dots e_p)$ soit une base de E. Notons $f_1 = f(e_1), \dots, f_r = f(e_r)$. La

famille $(f_1, \ldots, f_r)$ est libre ; en effet si $(\lambda_1, \ldots, \lambda_r) \in K^r$ est tel que $\sum_{i=1}^{r} \lambda_i f_i = 0$ alors $\sum_{i=1}^{r} \lambda_i e_i \in Ker(f) \cap Vect(e_1, \ldots, e_r) = \{0\}$, donc $\lambda_1 = \ldots = \lambda_r = 0$. D'après le théorème de la base incomplète (forme faible), il existe $f_{r+1}, \ldots, f_n \in F$ tels que $\mathcal{C}' = (f_1, \ldots, f_r, f_{r+1}, \ldots, f_n)$ soit une base de F. Puisque $f(e_1) = f_1, \ldots, f(e_r) = f_r, f(e_{r+1}) = 0, \ldots, f(e_p) = 0$, la matrice de f dans $\mathcal{B}'$ et $\mathcal{C}'$ est $J_{n,p,r}$ et donc $A \sim J_{n,p,r}$. ■

Corollaire 6.3.1 $\forall (A, B) \in (\mathcal{M}_{n,p}(K))^2$, $(A \sim B \Leftrightarrow rg(A) = rg(B))$.

Preuve :

(a) Si $A \sim B$, alors A et B représentent une même application linéaire (dans des bases) donc ont le même rang.

(b) Réciproquement, si $rg(A) = rg(B)$ alors A et B sont équivalentes à $J_{n,p,r}$ donc sont équivalentes entre elles. ■

Exercice 107 Soit u l'application linéaire de $\mathbb{R}^2$ dans $\mathbb{R}^3$ dont la matrice dans les bases canoniques respectives est $A = \begin{pmatrix} 2 & -1 & 1 \\ 3 & 2 & 3 \end{pmatrix}$. On appelle (e_1, e_2, e_3) la base canonique de $\mathbb{R}^3$ et (f_1, f_2) celle de $\mathbb{R}^2$. On pose

$$e'_1 = e_2 + e_3,\ e'_2 = e_3 + e_1,\ e'_3 = e_1 + e_2 \text{ et } f'_1 = \frac{1}{2}(f_1 + f_2),\ f'_2 = \frac{1}{2}(f_1 - f_2).$$

1. Montrer que (e'_1, e'_2, e'_3) est une base de $\mathbb{R}^3$ puis que (f'_1, f'_2) est une base de $\mathbb{R}^2$.
2. Quelle est la matrice de u dans ces nouvelles bases ?

Correction :

1. Puisqu'on a des familles de 3 (respectivement 2) vecteurs dans un espace de dimension 3 (respectivement 2), il suffit de prouver qu'on a des familles libres. Pour (f'_1, f'_2), c'est clair puisque les vecteurs ne sont pas colinéaires. Pour (e'_1, e'_2, e'_3), si on a une égalité du type $ae'_1 + be'_2 + ce'_3 = 0$, alors on obtient
$$(b+c)e_1 + (a+c)e_2 + (a+b)e_3 = 0 \Leftrightarrow \left\{ \begin{array}{rcl} b+c & = & 0 \\ a+c & = & 0 \\ a+b & = & 0 \end{array} \right. \Leftrightarrow a = b = c = 0.$$
Donc la famille (e'_1, e'_2, e'_3) est une base de $\mathbb{R}^3$.
2. Notons P la matrice de passage de (e_1, e_2, e_3) à (e'_1, e'_2, e'_3) et Q la matrice de passage de (f_1, f_2) à (f'_1, f'_2). On a alors
$$P = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \text{ et } Q = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$
Si B est la matrice de u dans les nouvelles bases, alors la formule du changement de bases affirme que $B = Q^{-1}AP$. Or, $Q^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ de sorte que $B = \begin{pmatrix} -1 & 3 & 6 \\ 1 & 3 & -4 \end{pmatrix}$.
3.

Exercice 108 Soient $u : \mathbb{R}^2 \to \mathbb{R}^3$ et $v : \mathbb{R}^3 \to \mathbb{R}^2$ définies par $u(x, y) = (x + 2y, 2x - y, 2x + 3y)$ et $v(x, y, z) = (x - 2y + z, 2x + y - 3z)$.

1. Montrer que u et v sont linéaires et donner les matrices de $u, v, u \circ v$ et $v \circ u$ dans les bases canoniques de leurs espaces de définition respectifs. En déduire les expressions de $u \circ v(x, y, z)$ et $v \circ u(x, y)$.

2. Soient $\mathcal{B}_2 = \{\epsilon_1, \epsilon_2\}$ et $\mathcal{B}_3 = \{\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3\}$ les bases canoniques de $\mathbb{R}^2$ et $\mathbb{R}^3$ respectivement. Montrer que $\mathcal{B}'_2 = \{\epsilon'_1, \epsilon'_2\}$ et $\mathcal{B}'_3 = \{\mathcal{F}'_1, \mathcal{F}'_2, \mathcal{F}'_3\}$ sont des bases de $\mathbb{R}^2$ et $\mathbb{R}^3$ respectivement, où $\epsilon'_1 = \epsilon_1$, $\epsilon'_2 = \epsilon_1 - \epsilon_2$, $\mathcal{F}'_1 = \mathcal{F}_1$, $\mathcal{F}'_2 = \mathcal{F}_1 + \mathcal{F}_2$ et $\mathcal{F}'_3 = \mathcal{F}_1 + \mathcal{F}_2 + \mathcal{F}_3$.
3. Donner la matrice de passage P de la base $\mathcal{B}_2$ à la base $\mathcal{B}'_2$ puis la matrice de passage Q de la base $\mathcal{B}_3$ à la base $\mathcal{B}'_3$.
4. Écrire la matrice de u dans les bases $\mathcal{B}'_2$ et $\mathcal{B}_3$ puis dans les bases $\mathcal{B}'_2$ et $\mathcal{B}'_3$ et enfin celle de v dans les bases $\mathcal{B}'_3$ et $\mathcal{B}'_2$.

Correction :

1. Remarquons d'abord que u et v sont linéaires. Notons A (respectivement B) la matrice de u (respectivement v) dans sa base canonique. On a :
$$A = \begin{pmatrix} 1 & 2 \\ 2 & -1 \\ 2 & 3 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & -2 & 1 \\ 2 & 1 & -3 \end{pmatrix}.$$
$u \circ v$ est une application linéaire de $\mathbb{R}^3$ dans $\mathbb{R}^3$. Sa matrice est donnée par le produit matriciel AB. $v \circ u$ est un endomorphisme de $\mathbb{R}^2$. Sa matrice est donnée par le produit matriciel BA. On trouve
$$AB = \begin{pmatrix} 5 & 0 & -5 \\ 0 & -5 & 5 \\ 8 & -1 & -7 \end{pmatrix} \text{ et } BA = \begin{pmatrix} -1 & 7 \\ -2 & -6 \end{pmatrix}.$$
On en déduit que $u \circ v(x, y, z) = (5x - 5z, -5y + 5z, 8x - y - 7z)$ et $v \circ u(x, y) = (-x + 7y, -2x - 6y)$.
2. Il suffit de vérifier que les deux familles sont libres, puisqu'elles comptent le même nombre de vecteurs que la dimension de l'espace. Pour $\mathcal{B}'_2$, c'est clair puisque les deux vecteurs ne sont pas colinéaires. Pour $\mathcal{B}'_3$, on traduit une égalité du type $a\mathcal{F}'_1 + b\mathcal{F}'_2 + c\mathcal{F}'_3 = 0$ par
$$(a+b+c)\mathcal{F}_1 + (b+c)\mathcal{F}_2 + c\mathcal{F}_3 = 0 \Leftrightarrow \begin{cases} a+b+c &= 0 \\ b+c &= 0 \\ c &= 0 \end{cases} \Leftrightarrow a = b = c = 0.$$
3. La matrice de passage est la matrice des coordonnées des nouveaux vecteurs exprimés en fonction des anciens vecteurs. On a donc :
$$P = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \text{ et } Q = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$
4. Notons C la matrice de u dans les bases $\mathcal{B}'_2$ et $\mathcal{B}_3$. Comme on ne change la base qu'au départ, la formule de changement de base donne $C = AP = \begin{pmatrix} 1 & -1 \\ 2 & 3 \\ 2 & -1 \end{pmatrix}$.
Notons D la matrice de u dans les bases $\mathcal{B}'_2$ et $\mathcal{B}'_3$. Cette fois, on change de base à la fois au départ et à l'arrivée. La formule de changement de base donne $D = Q^{-1}AP$. Après calculs, on trouve
$$Q^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } D = \begin{pmatrix} -1 & -4 \\ 0 & 4 \\ 2 & -1 \end{pmatrix}.$$
Notons enfin E la matrice de v dans les nouvelles bases. La formule de changement de base donne $E = P^{-1}BQ$. On obtient après calculs :
$$P^{-1} = P \text{ et } E = \begin{pmatrix} 3 & -4 & -1 \\ -2 & 1 & 4 \end{pmatrix}.$$

6.3.4 Changement de base pour un endomorphisme

Proposition 6.3.7 *Soient E un K-ev de dimension n, $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E, $P = Pass(\mathcal{B}, \mathcal{B}')$, $f \in \mathcal{L}(E)$, $A = Mat_{\mathcal{B}}(f)$, $A' = Mat_{\mathcal{B}'}(f)$. Alors*

$$A' = P^{-1}AP.$$

Cette proposition est un cas particulier de la proposition 6.3.4.

Définition 6.3.3 *Soient $A, B \in \mathcal{M}_n(K)$. On dit que A est **semblable à** B, et on note $A \sim B$ si et seulement s'il existe $P \in GL_n(K)$ telle que $B = P^{-1}AP$.*

Proposition 6.3.8 *La relation $\sim$ est une relation d'équivalence dans $\mathcal{M}_n(K)$.*

Preuve :

1. *Réflexivité* : $\forall A \in \mathcal{M}_n(K)$, $A = I_n A I_n$.
2. *Symétrie* : S'il existe $P \in GL_n(K)$ telle que $B = P^{-1}AP$ alors $A = (P^{-1})^{-1}BP^{-1}$ et $P^{-1} \in GL_n(K)$ donc $B \sim A$.
3. *Transitivité* : Supposons $A \sim B$ et $B \sim C$. Il existe $P, Q \in GL_n(K)$ telles que $B = P^{-1}AP$ et $C = Q^{-1}BQ$. Alors $C = Q^{-1}P^{-1}APQ = (PQ)^{-1}A(PQ)$ et $PQ \in GL_n(K)$ donc $A \sim C$. ■

Proposition 6.3.9 $\forall (A, B) \in (M_n(K))^2$, $A \sim B \Rightarrow tr(A) = tr(B)$.

Preuve : Supposons $A \sim B$. Il existe $P \in GL_n n(K)$ telle que $B = P^{-1}AP$ d'où $tr(B) = tr(P^{-1}(AP)) = tr((AP)P^{-1}) = tr(A)$. ■

Remarque 6.3.3

- Il est clair que si deux matrices carrées sont semblables alors elles sont équivalentes.
- Mais, si $n \geq 2$, deux matrices équivalentes peuvent ne pas être semblables. Par exemple, pour $n = 2$, les matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ sont équivalentes puisqu'elles sont de même rang 1, mais ne sont pas semblables puisqu'elles n'ont pas la même trace.
- Soit $A \in \mathcal{M}_n(K)$. S'il existe $\alpha \in K$ tel que $A \sim \alpha I_n$ alors $A = \alpha I_n$. En effet, pour toute matrice P de $GL_n(K)$, $P(\alpha I_n)P^{-1} = \alpha I_n$.
- Si $n \geq 2$, deux matrices carrées peuvent avoir la même trace, mais ne sont pas semblables puisqu'elles ne sont pas équivalentes (la première est de rang 0, la seconde est de rang 1).

Définition 6.3.4 *Soient E un K-ev de dimension finie, $f \in \mathcal{L}(E)$. On appelle **trace** de f, et on note $tr(f)$, la trace de n'importe quelle matrice représentant l'endomorphisme f.*

Proposition 6.3.10 *Soit E un K-ev.*

1. *L'application* $tr : \begin{array}{ccc} \mathcal{L}(E) & \to & K \\ f & \mapsto & tr(f) \end{array}$ *est une forme linéaire.*
2. $\forall (f, g) \in (\mathcal{L}(E))^2$, $tr(g \circ f) = tr(f \circ g)$.
3. $\forall f \in \mathcal{L}(E)$, $\forall h \in \mathcal{GL}(E)$, $tr(h^{-1} \circ f \circ h) = tr(f)$.