

# Algèbre Linéaire Avancée I

## Math 110 (b)

Dr. Aline Zanardini  
aline.zanardini@epfl.ch

Automne 2025

AZ: Ces notes contiennent tout le contenu du cours et sont basées sur le cours de Donna Testerman durant l'année académique 2024-2025, ainsi que sur des extraits des ouvrages de Hoffman & Kunze et d'Axler. Les sections non traitées lors de l'année 2024-2025 sont annotées par (\*). Ces notes peuvent contenir des erreurs, et vous êtes libre de me signaler toute coquille ou toute erreur par e-mail. J'ai déjà les personnes suivantes à remercier : R. Blondel, M. Delorenzi, E. Pizzaia et M. Yurchenko.

## Table des matières

---

<b>1</b>	<b>Cours 1</b>	<b>3</b>
1.1	Que comprend l'algèbre linéaire et pourquoi l'étudie-t-on ? . . . . .	3
1.2	Lois de composition . . . . .	5
<b>2</b>	<b>Cours 2 &amp; 3</b>	<b>8</b>
2.1	Groupes . . . . .	8
2.2	Sous-groupes . . . . .	13
2.3	Morphismes de groupes . . . . .	15
<b>3</b>	<b>Cours 4 &amp; 5</b>	<b>17</b>
3.1	Anneaux . . . . .	17
3.2	Corps . . . . .	20
3.3	Anneaux de polynômes . . . . .	21
3.4	Pour réfléchir chez vous . . . . .	23
<b>4</b>	<b>Cours 6</b>	<b>25</b>
4.1	Espaces vectoriels . . . . .	25

<b>5 Cours 7</b>	<b>28</b>
5.1 De nouveaux sous-espaces à partir d'autres sous-espaces . . . . .	28
5.2 (In)dépendance linéaire . . . . .	31
<b>6 Cours 8</b>	<b>33</b>
6.1 Base et dimension . . . . .	33
6.2 Quelques exemples . . . . .	36
<b>7 Cours 9</b>	<b>37</b>
7.1 Applications linéaires : définitions et exemples . . . . .	37
7.2 Opérations sur les applications linéaires . . . . .	40
7.3 Pour réfléchir chez vous . . . . .	41
<b>8 Cours 10</b>	<b>41</b>
8.1 Noyau, image et le théorème du rang . . . . .	42
8.2 Pour réfléchir chez vous . . . . .	44
<b>9 Cours 11</b>	<b>45</b>
9.1 La matrice d'une application linéaire . . . . .	46
9.2 Changement de base et des matrices semblables . . . . .	47
<b>10 (*) Cours 12 (non examinable)</b>	<b>49</b>
10.1 Forme linéaires (covecteurs) . . . . .	49
10.2 Pour réfléchir chez vous . . . . .	52
<b>11 Cours 13</b>	<b>52</b>
11.1 Opérations élémentaires et forme échelonnée réduite . . . . .	53
11.2 Pour réfléchir chez vous . . . . .	55
<b>12 Cours 14</b>	<b>56</b>
12.1 La méthode de Gauss . . . . .	56
12.2 Pour réfléchir chez vous . . . . .	59
<b>13 Cours 15</b>	<b>59</b>
13.1 Applications de la méthode de Gauss . . . . .	59
<b>14 Cours 16</b>	<b>65</b>
14.1 Le noyau et l'image d'une application linéaire . . . . .	65
14.2 Le rang d'une application linéaire . . . . .	68
14.3 Pour réfléchir chez vous . . . . .	69
<b>15 Cours 17</b>	<b>70</b>
15.1 Inversion de matrices carrées . . . . .	70
15.2 Matrice de changement de base . . . . .	72
15.3 Pour réfléchir chez vous . . . . .	73

<b>16 Cours 18</b>	<b>73</b>
16.1 Le groupe $S_n$ . . . . .	74
16.2 Le déterminant d'une matrice $2 \times 2$ . . . . .	76
16.3 Le déterminant d'une matrice $3 \times 3$ . . . . .	76
<b>17 (★) Cours 19</b>	<b>76</b>
17.1 Formes multilinéaires alternées . . . . .	76
<b>18 Cours 20</b>	<b>80</b>
18.1 Déterminants . . . . .	80
18.2 Quelques propriétés des déterminants en plus . . . . .	83
<b>19 Cours 21</b>	<b>84</b>
19.1 Vecteurs propres et valeurs propres . . . . .	84
<b>20 Cours 22</b>	<b>87</b>
20.1 Multiplicité géométrique et multiplicité algébrique . . . . .	87
20.2 (★) Polynôme minimal d'un endomorphisme (non examinable) . . . . .	88
<b>21 Cours 23</b>	<b>91</b>
21.1 Matrices triangulaires et endomorphismes trigonalisables . . . . .	91
<b>22 Cours 24</b>	<b>96</b>
22.1 Matrices diagonales et endomorphismes diagonalisables . . . . .	96
<b>23 Cours 25</b>	<b>99</b>
23.1 (★) Opérateurs commutatifs . . . . .	99
<b>24 Cours 26 &amp; 27</b>	<b>101</b>
24.1 (★) Espaces munis d'un produit scalaire (non examinable) . . . . .	101

## Cours 1

---

### 1.1 Que comprend l'algèbre linéaire et pourquoi l'étudie-t-on ?

L'algèbre est le domaine des mathématiques qui s'occupe d'étudier les **structures algébriques**, c.-à-d., les ensembles munis d'un certain nombre d'opérations sur leurs éléments, et parfois dépendant d'autres ensembles, qui satisfont quelques propriétés et qui sont liées. Dans l'univers de l'algèbre linéaire, c'est la structure **d'espace vectoriel** qui joue le rôle principal. En fait, le mot linéaire fait référence à deux **lois de composition** sur un ensemble (non vide), l'une interne et l'autre externe, qui sont compatibles entre elles et qui vérifient certains axiomes.

Cette structure nous permet de généraliser des concepts de géométrie (comme les droites, les plans, les volumes, . . .), des notions concrètes que nous pouvons visualiser, à une variété de cas beaucoup plus abstraits qui apparaissent dans différents domaines d'étude, notamment

la physique. Par exemple, en mécanique quantique, l'espace des états d'un système est un espace vectoriel, dit un espace de Hilbert. On peut également citer tous les problèmes de la physique qui consistent en la résolution d'une équation différentielle linéaire. De toute façon, il y a aussi des applications concrètes de l'algèbre linéaire en ingénierie, en informatique, en économie, en chimie, en biologie, ...

AZ: Je vous propose de lire cet article [↗](#) (en anglais).

### 1.1.1 Une introduction aux espaces vectoriels

AZ: Cette petite introduction est basée sur une vidéo de la chaîne *Les maths en finesse* avec le même nom que je vous propose également de regarder.

Des espaces vectoriels peuvent donc contenir par leurs éléments des suites, des polynômes, des matrices, des fonctions, ou alors plus simplement des « vecteurs numériques » ou des « vecteurs géométriques » qui représentent un point dans le plan  $\mathbb{R}^2$  ou dans l'espace  $\mathbb{R}^3$ , par exemple. Même si à première vue ces objets semblent très différents.

Pour introduire cette notion, considérons maintenant les ensembles suivants :

- $\mathbb{R}^2$ ,
- $\mathcal{S} := \{x = (x_n)_{n=0}^\infty \in \mathbb{R}^\mathbb{N} \mid x_{n+2} = x_{n+1} + x_n\}$ , et
- $\mathcal{F} := \{f \in C^2(\mathbb{R}, \mathbb{R}) \mid \forall t \in \mathbb{R}, f''(t) + f(t) = 0\}$ .

Quel est le lien entre ces trois ensembles? On vérifie que dans les trois cas, les affirmations suivantes sont vraies.

- (i) Les trois ensembles sont stables par **combinaisons linéaires** (réelles). Intuitivement, ça veut dire que si je prends deux éléments d'un de ces ensembles, il existe un moyen de les multiplier par des nombres réels et d'additionner le résultat de telle manière que nous obtenions un élément qui appartient au même ensemble. Plus précisément, nous avons que pour tous les nombres réels  $\alpha$  et  $\beta$

$$(x, y) \in \mathcal{S} \times \mathcal{S} \Rightarrow \alpha x + \beta y \in \mathcal{S},$$

où l'addition de deux suites est définie terme par terme, et la multiplication par les **scalaires** réels aussi. Le formalisme dans les deux autres cas est analogue.

- (ii) Chaque élément de  $\mathbb{R}^2$ , de  $\mathcal{S}$ , ou de  $\mathcal{F}$  est complètement déterminé par deux données. Par exemple, chaque point du plan est entièrement déterminé par son abscisse et par son ordonnée. Similairement, toute suite  $x = (x_n)$  dans  $\mathcal{S}$  est caractérisée par les termes  $x_0$  et  $x_1$ . Et, de la même manière, des fonctions  $f$  qui appartiennent à  $\mathcal{F}$  peuvent être reconstruites en utilisant les valeurs  $f(0)$  et  $f'(0)$ .

AZ: Dans ce dernier cas, il peut être utile pour vous de faire le lien avec des systèmes physiques qui sont modélisés comme des oscillateurs harmoniques.

- (iii) Tout élément de  $\mathbb{R}^2$  s'écrit de manière unique comme une combinaison linéaire de deux éléments quelconques qui n'appartiennent pas à la même droite passant par l'origine. Par exemple, si  $(x, y) \in \mathbb{R}^2$ , alors

$$(x, y) = x \cdot (1, 0) + y \cdot (0, 1),$$

et il est évident que les nombres réels  $x$  et  $y$  que nous permettent d'écrire  $(x, y)$  comme une combinaison linéaire des éléments  $(1, 0)$  et  $(0, 1)$  sont uniques. Des affirmations analogues sont également vraies pour les ensembles  $\mathcal{S}$  et  $\mathcal{F}$ .

### 1.1.2 Pour réfléchir chez vous

**Exercice 1.1.1.** Vérifiez la véracité de l'affirmation du point (i) ci-dessus. Comment sont définies les opérations d'addition et de multiplication par un nombre réel dans chaque cas ?

**Exercice 1.1.2.** Trouvez deux autres éléments  $u = (u_1, u_2)$  et  $v = (v_1, v_2)$  dans  $\mathbb{R}^2$  tels que tout autre point du plan  $(x, y) \in \mathbb{R}^2$  peut être écrit de manière unique comme une combinaison linéaire de ceux-ci, c'est-à-dire que de la façon suivante :

$$(x, y) = \alpha u + \beta v = \alpha \cdot (u_1, u_2) + \beta \cdot (v_1, v_2),$$

où  $\alpha$  et  $\beta$  sont des nombres réels. Que se passera-t-il si nous remplaçons  $\mathbb{R}^2$  par  $\mathbb{R}^3$  ? Et dans le cas des ensembles  $\mathcal{S}$  et  $\mathcal{F}$ , pouvez-vous trouver deux bons éléments « **générateurs** » ?

## 1.2 Lois de composition

Un ensemble est simplement une collection d'objets, sans condition particulière. Mais ils peuvent souvent être associés les uns aux autres (additionnés ou multipliés, par exemple), et on parle alors de lois de composition. Selon les règles que ces lois vérifient, elles permettent de définir des structures algébriques ; autrement dit, les ensembles correspondants portent des structures algébriques (de groupe, d'anneau, de corps, d'espace vectoriel, ...). Les définitions sont les suivantes.

**Définition 1.2.1.** Une **loi de composition interne**, ou loi interne, sur un ensemble  $E \neq \emptyset$  est une application (une fonction) de  $E \times E$  dans  $E$ .

AZ:  Dans ce cours, les mots application, fonction et transformation seront utilisés de manière interchangeable.

Autrement dit, une loi interne sur un ensemble  $E$  associe à deux éléments de  $E$  un élément de  $E$ . Donc, une loi de composition interne sur un ensemble  $E$  est une opération binaire par laquelle  $E$  est stable. Elle peut être notée par  $*$ , par  $\circ$ , par  $\otimes$ , ... L'addition et la multiplication usuelles dans les ensembles  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  ou  $\mathbb{C}$  sont des exemples classiques de lois de composition internes.

Il est important de noter que pour que la fonction considérée soit effectivement une loi de composition interne, il faut qu'elle soit définie partout. À deux éléments quelconques de  $E$  la fonction associe un troisième (élément), unique, et toujours dans  $E$ .

**Définition 1.2.2.** Une **loi de composition externe**, ou loi externe, sur un ensemble  $E \neq \emptyset$  est une application de  $F \times E$  dans  $E$ , où  $F$  est un autre ensemble a priori différent de  $E$ . Les éléments de  $F$  sont appelés des opérateurs ou des scalaires.

L'exemple typique est la multiplication d'un point du plan, un élément de  $E = \mathbb{R}^2$ , par un nombre réel ( $F = \mathbb{R}$ ). Géométriquement, on peut considérer les points du plan comme des vecteurs géométriques, c'est-à-dire représentés par un segment orienté (une flèche) dont les extrémités sont un point de départ, l'origine, et un point d'arrivée. L'opération dont nous parlons consiste à étirer ou à rétrécir un vecteur, ou bien évidemment à ne rien faire.

**Remarque 1.** Si  $F = E$  dans la Définition 1.2.2, on a une loi interne. Donc, une loi interne, c'est un cas particulier d'une loi externe.

### 1.2.1 Quelques propriétés

Soit  $E$  un ensemble non vide et soit  $*$  :  $E \times E \rightarrow E$  une loi interne sur  $E$ . On dit que la loi  $*$  est

(P1) associative si

$$(a * b) * c = a * (b * c) \quad \forall (a, b, c) \in E^3 = E \times E \times E,$$

(P2) commutative si

$$a * b = b * a \quad \forall (a, b) \in E^2 = E \times E,$$

De plus,

- si  $\circ : E \times E \rightarrow E$  est une autre loi sur  $E$ , on dit que  $*$  est distributive à gauche sur  $\circ$  si :

$$\forall (a, b, c) \in E^3; a * (b \circ c) = (a * b) \circ (a * c).$$

Similairement, on dit que  $*$  est distributive à droite sur  $\circ$  si :

$$\forall (a, b, c) \in E^3; (b \circ c) * a = (b * a) \circ (c * a).$$

- Un **élément neutre** pour  $*$  est un élément  $e \in E$  tel que :

$$\boxed{e * a = a * e = a} \quad \forall a \in E.$$

- Si  $E$  possède un élément neutre  $e$  pour  $*$ , on dit qu'un élément  $b \in E$  est un **inverse** de  $a \in E$  si  $\boxed{a * b = b * a = e}$ . Un élément  $a \in E$  qui admet un inverse est dit **inversible** (pour  $*$ ).

**Remarque 2.** On peut parler aussi d'éléments neutres à gauche ou à droite et également des inverses à droite et à gauche. Lorsque la loi  $*$  en considération est associative, l'existence d'un implique l'existence de l'autre. On va laisser tout ça de côté dans ce cours, cf. Section 2.1 ci-dessous.

AZ: **▲** Lorsque la loi en question est associative et commutative, on adopte souvent la notation additive : on la désigne par  $+$ , l'inverse d'un élément  $a \in E$  devient  $-a$ , et on parle d'élément opposé. On parle également d'élément nul, plutôt que d'élément neutre, généralement noté  $O_E$  ou simplement  $0$ . Même si  $0$  n'est pas forcément le nombre zéro. D'un autre côté, il est aussi parfois utile d'adopter la notation multiplicative. . . Je voudrais donc vous avertir que je ferai probablement tout cela très souvent pendant ce cours, car c'est quelque chose de très naturel pour moi. Il faut toujours faire attention.

Nous pouvons prouver ce qui suit à propos de ces notions.

**Proposition 1.2.3.** *Soit  $E$  un ensemble non vide et  $\star : E \times E \rightarrow E$  une loi de composition interne. Si  $E$  possède un élément neutre pour la loi  $\star$ , alors cet élément est unique. Par ailleurs, si  $\star$  est associative et  $E$  possède un élément neutre, alors chaque élément inversible de  $E$  a un unique inverse.*

*Démonstration.* Soient  $E$  et  $\star$  comme dans l'énoncé du théorème. Supposons que  $E$  possède un élément neutre  $e \in E$  (pour  $\star$ ). Si  $\tilde{e} \in E$  est un autre élément neutre, alors

$$e = e \star \tilde{e} = \tilde{e}. \quad (1)$$

AZ: Notez que dans la première égalité dans (1) ci-dessus nous avons utilisé le fait que  $\tilde{e}$  est un élément neutre, et la deuxième égalité découle du fait que  $e$  est un élément neutre.

Supposons maintenant que  $\star$  est associative et choisissons un élément  $a$  qui appartient à  $E$  et qui est inversible. Soient  $b$  et  $\tilde{b}$  deux inverses de  $a$ . Alors,

$$\begin{aligned} \tilde{b} &= \tilde{b} \star e && (e \text{ est élément neutre}) \\ &= \tilde{b} \star (a \star b) && (b \text{ est un inverse de } a) \\ &= (\tilde{b} \star a) \star b && (\star \text{ est associative}) \\ &= e \star b && (\tilde{b} \text{ est un inverse de } a) \\ &= b. && (e \text{ est élément neutre}) \end{aligned}$$

□

## 1.2.2 Quelques exemples

**Exemple 1.2.4** (Réunion et intersection). Si  $X$  est un ensemble non vide quelconque, la réunion  $(A, B) \mapsto A \cup B$  et l'intersection  $(A, B) \mapsto A \cap B$  sont des lois de composition interne sur l'ensemble  $\mathcal{P}(X)$  de toutes les parties de  $X$ .

**Exemple 1.2.5** (Composition de fonctions). Si  $X$  est un ensemble non vide quelconque, nous pouvons considérer l'ensemble  $\mathcal{F}(X, X)$  de toutes les applications de  $X$  dans  $X$ . La composition usuelle  $(f, g) \mapsto f \circ g$  est une loi de composition sur cet ensemble.

**Exemple 1.2.6** (Produit vectoriel). Sur l'ensemble  $\mathbb{R}^3$  nous pouvons considérer une loi  $\wedge : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}^3$  qui est définie par

$$(a, b, c) \wedge (d, e, f) = \begin{vmatrix} \hat{\mathbf{i}} & \hat{\mathbf{j}} & \hat{\mathbf{k}} \\ a & b & c \\ d & e & f \end{vmatrix} = (bf - ce, cd - af, ae - bd).$$

### 1.2.3 Pour réfléchir chez vous

**Exercice 1.2.7.** Les lois des exemples ci-dessus sont-elles commutatives? Sont-elles associatives? Est-ce qu'elles admettent un élément neutre?

**Exercice 1.2.8.** Donnez un exemple<sup>1</sup> d'un ensemble  $E$  et d'une loi interne  $*$  :  $E \times E \rightarrow E$  qui n'est pas commutative. Est-ce que vous connaissez un exemple de loi qui n'est pas associative?

AZ: Je vous invite à lire cet article [↗](#) (en français).

**Exercice 1.2.9.** Si  $*$  est une loi associative/commutative, sur un ensemble  $E$ , et  $A \subset E$  est stable par  $*$ , alors convainquez-vous que la loi  $*$ , vue comme une loi interne sur  $A$ , est bien sûr encore associative/commutative.

**Exercice 1.2.10.** Soit  $E \neq \emptyset$  un ensemble et  $\clubsuit : E \times E \rightarrow E$  une loi de composition sur  $E$  qui est associative. Supposons que  $E$  possède un élément neutre  $e \in E$  (pour  $\clubsuit$ ). Démontrez que le sous-ensemble

$$A = \{a \in E \mid a \text{ est inversible}\}$$

est stable par  $\clubsuit$ . Si  $a, b \in A$ , quel est l'inverse de  $a \clubsuit b$ ?

La définition de partie stable est la suivante.

**Définition 1.2.11.** Soit  $E$  un ensemble non vide, soit  $A \subset E$  un sous-ensemble (une partie) et soit  $\diamond : E \times E \rightarrow E$  une loi interne sur  $E$ . On dit que  $A$  est **stable** par  $\diamond$  si pour chaque couple  $(x, y)$  d'éléments de  $A$  on a  $x \diamond y \in A$ . On dit aussi que  $\diamond$  induit une loi interne sur la partie  $A$ .

## Cours 2 & 3

---

### 2.1 Groupes

La structure de groupe est fondamentale en mathématiques et dans ce cours nous l'utiliserons pour définir les espaces vectoriels de manière rigoureuse.

**Définition 2.1.1.** Un **groupe** est un ensemble muni d'une loi de composition interne associative, admettant un élément neutre et telle que tout élément est inversible. Autrement dit, un groupe est un ensemble  $G$  muni d'une application  $*$  :  $G \times G \rightarrow G$ , qui envoie  $(a, b) \mapsto a * b$ , tel que les axiomes suivants sont vérifiés :

(G1) (**associativité**) On a  $a * (b * c) = (a * b) * c$  pour tous  $a, b, c \in G$ ;

(G2) (**existence de l'élément neutre**) il existe  $e \in G$  tel que  $e * g = g * e = g$  pour tout  $g \in G$  ;  
et

(G3) (**existence des inverses**) pour tout  $g \in G$ , il existe  $g^{-1} \in G$  tel que  $g^{-1} * g = g * g^{-1} = e$ .

---

1. Différent des exemples ci-dessus.

**Définition 2.1.2.** Un groupe  $(G, *)$  dans lequel la loi de composition  $*$  est commutative est appelé **groupe abélien**.

AZ: **▲** On écrira souvent  $ab$  pour  $a * b$  dans un groupe où la loi n'est pas précisée.

AZ: **▲** Si le groupe  $G$  est abélien j'utiliserai parfois la notation additive :  $+$  pour désigner la loi de composition,  $0$  pour l'élément neutre, et  $-g$  pour l'inverse/opposé de  $g \in G$ .

**Remarque 3.** Notez que dans un groupe  $G$ , les inverses sont uniques. Nous avons prouvé ce fait dans la Proposition 1.2.3. C'est pour ça qu'on utilise la notation  $g^{-1}$  pour désigner l'inverse d'un élément  $g \in G$ .

Voici quelques conséquences directes de la définition de groupe.

**Proposition 2.1.3.** Soit  $(G, *)$  un groupe avec élément neutre  $e \in G$ . Les affirmations suivantes sont vraies.

(i) Pour tous  $a, b, c \in G$ , on a

$$a * b = a * c \Rightarrow b = c. \quad (\text{simplification à gauche})$$

De même,

$$a * b = c * b \Rightarrow a = c \quad (\text{simplification à droite})$$

(ii) Pour tous  $a, b \in G$ , on a

$$(a * b)^{-1} = b^{-1} * a^{-1} \quad \text{et} \quad (a^{-1})^{-1} = a.$$

*Démonstration.*

(i) Pour tous  $a, b, c \in G$  on a

$$\begin{aligned} a * b = a * c &\Rightarrow a^{-1} * (a * b) = a^{-1} * (a * c) \\ &\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c && (\text{Associativité}) \\ &\Rightarrow e * b = e * c && (\text{Définition de l'inverse}) \\ &\Rightarrow b = c && (e \text{ est élément neutre}) \end{aligned}$$

et de même,

$$\begin{aligned} a * b = c * b &\Rightarrow (a * b) * b^{-1} = (c * b) * b^{-1} \\ &\Rightarrow a * (b * b^{-1}) = c * (b * b^{-1}) && (\text{Associativité}) \\ &\Rightarrow a * e = c * e && (\text{Définition d'inverse}) \\ &\Rightarrow a = c && (e \text{ est élément neutre}) \end{aligned}$$

(ii) Pour tous  $a, b \in G$ , on a

$$\begin{aligned}
 (a * b) * (b^{-1} * a^{-1}) &= ((a * b) * b^{-1}) * a^{-1} && \text{(Associativité)} \\
 &= (a * (b * b^{-1})) * a^{-1} && \text{(Associativité)} \\
 &= (a * e) * a^{-1} && \text{(Définition de l'inverse)} \\
 &= a * a^{-1} && (e \text{ est élément neutre}) \\
 &= e. && \text{(Définition de l'inverse)}
 \end{aligned}$$

AZ: Notez qu'à ce moment, nous venons de prouver que  $b^{-1} * a^{-1}$  est un inverse à droite de  $a * b$  et la preuve n'est pas finie. Pourquoi ?

De la même façon, nous pouvons montrer que  $(b^{-1} * a^{-1}) * (a * b) = e$ . Donc, par définition de l'inverse, on a  $b^{-1} * a^{-1} = (a * b)^{-1}$ .

Enfin, l'égalité  $(a^{-1})^{-1} = a$  est une tautologie. Comme dans un groupe des inverses sont uniques (regardez Remarque 3 et Proposition 1.2.3), on a que  $(a^{-1})^{-1}$  est le seul élément de  $G$  satisfaisant les égalités suivantes :

$$(a^{-1})^{-1} * (a^{-1}) = (a^{-1}) * (a^{-1})^{-1} = e.$$

Donc ça suffit de noter que

$$a * (a^{-1}) = (a^{-1}) * a = e.$$

En tout cas, nous pouvons également argumenter comme suit (comparez avec la preuve de la Proposition 1.2.3).

$$\begin{aligned}
 (a^{-1})^{-1} &= (a^{-1})^{-1} * e && (e \text{ est élément neutre}) \\
 &= (a^{-1})^{-1} * (a^{-1} * a) && (a^{-1} \text{ est l'inverse de } a) \\
 &= ((a^{-1})^{-1} * a^{-1}) * a && (* \text{ est associative}) \\
 &= e * a && ((a^{-1})^{-1} \text{ est l'inverse de } a^{-1}) \\
 &= a && (e \text{ est élément neutre})
 \end{aligned}$$

□

### 2.1.1 Exemples

Il existe une variété d'exemples de groupes. En fait, vous connaissez déjà, par exemple,  $(\mathbb{Z}, +)$  (ou  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$ , ...) et  $(\mathbb{R} \setminus \{0\}, \cdot)$ . Nous listons ici quelques autres qui sont pertinents pour ce cours.

AZ: Je vous invite à parcourir cet article [☞](#) (en français) pour trouver plus d'exemples qui sont relevant pour les physicien.ne.s.

Notez que l'ensemble  $\mathbb{N}$  muni de l'addition usuelle n'est pas un groupe. Pourquoi ?

**Exemple 2.1.4** (Le plus petit groupe). Soit  $G$  un ensemble quelconque avec un seul élément noté  $e$ . Si on définit une loi interne  $*$  :  $G \times G \rightarrow G$  sur  $G$ , alors nécessairement  $e * e = e$  et  $(G, *)$  est un groupe.

**Exemple 2.1.5.** Nous verrons qu'un espace vectoriel est, en particulier, un groupe abélien avec l'addition vectorielle. Nous reviendrons sur cette affirmation lors de la troisième semaine du cours.

**Exemple 2.1.6.** Soit  $X$  un ensemble non vide et considérez l'ensemble  $:= \text{Bij}(X)$  de toutes les applications bijectives de  $X$  dans  $X$ . Si  $\circ : \text{Bij}(X) \times \text{Bij}(X) \rightarrow \text{Bij}(X)$  note la composition de fonctions, alors on peut vérifier que  $(\text{Bij}(X), \circ)$  est un groupe.

AZ: On appelle ce groupe le groupe des permutations de l'ensemble  $X$  ou le groupe symétrique de  $X$ .

Un cas particulier qui est très important, c'est celui où  $X$  est fini. Si  $X = \{1, 2, \dots, n\}$ ,  $n$  étant un entier naturel positif, on appelle  $\text{Bij}(X)$  le **groupe symétrique de degré  $n$** , noté  $\mathfrak{S}_n, \text{Sym}_n$ , ou simplement  $S_n$ . Pour  $\sigma \in S_n$  on écrit souvent

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}.$$

Par exemple, si  $n = 3$  et  $\sigma : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$  est la bijection telle que  $1 \mapsto 2, 2 \mapsto 1$  et  $3 \mapsto 3$ , on écrit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

**Exemple 2.1.7** (Les entiers modulo  $n$ ). Fixons un nombre naturel  $n$  non nul. On définit une relation d'équivalence sur  $\mathbb{Z}$  de la façon suivante : pour tous  $a, b \in \mathbb{Z}$ , on dit que  $a \sim b$  si et seulement si  $n$  divise  $b - a$ , c'est-à-dire qu'il existe  $k \in \mathbb{Z}$  tel que  $b - a = k \cdot n$ . On écrit  $\mathbb{Z}/n\mathbb{Z}$  pour désigner l'ensemble des classes d'équivalence de  $\mathbb{Z}$  par rapport à cette relation et on munit  $\mathbb{Z}/n\mathbb{Z}$  d'une loi de composition qui lui donnera la structure de groupe abélien. Si on note  $\bar{a}$  la classe d'équivalence de  $a \in \mathbb{Z}$ , c.-à-d.  $\bar{a} := \{b \in \mathbb{Z} \mid a \sim b\}$ , alors pour  $(x, y) \in \mathbb{Z} \times \mathbb{Z}$  on pose  $\bar{x} + \bar{y} := \overline{x + y}$ .

**Exemple 2.1.8** (Matrices). Une matrice  $n \times m$  à coefficients dans  $\mathbb{R}$  (ou plus généralement dans un corps  $K$ ) est un tableau à  $n$  lignes et  $m$  colonnes constituées d'éléments de  $\mathbb{R}$  (ou  $K$ ) :

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}.$$

On va voir la définition dans la Section 3.2.

On appelle des  $a_{ij}$  les coefficients de la matrice  $A$ . On écrit  $A = (a_{ij})$  et on note  $\mathbb{M}_{n \times m}(\mathbb{R})$  (ou  $\mathbb{M}_{n \times m}(K)$ ) l'ensemble des matrices  $n \times m$  à coefficients dans  $\mathbb{R}$  (ou  $K$ ). Sur cet ensemble, on peut définir une loi interne  $+$  :  $\mathbb{M}_{n \times m}(\mathbb{R}) \times \mathbb{M}_{n \times m}(\mathbb{R}) \rightarrow \mathbb{M}_{n \times m}(\mathbb{R})$  donnée par  $(A = (a_{ij}), B = (b_{ij})) \mapsto A + B$ , où la matrice  $(A + B)$  est telle que son coefficient trouvé dans la ligne  $i$  et la colonne  $j$  est égal à  $a_{ij} + b_{ij}$  pour tous  $1 \leq i \leq n$  et  $1 \leq j \leq m$ . On vérifie que  $(\mathbb{M}_{n \times m}(\mathbb{R}), +)$  est un groupe abélien. Quel est l'élément neutre ?

**Exemple 2.1.9** (Matrices inversibles).

**Définition 2.1.10.**

- (i) Soient  $A \in \mathbb{M}_{n \times m}(\mathbb{R})$  et  $B \in \mathbb{M}_{m \times \ell}(\mathbb{R})$ . On définit le produit  $AB$  comme étant la matrice  $C \in \mathbb{M}_{n \times \ell}(\mathbb{R})$  avec  $C = (c_{ij})$  et telle que  $c_{ij} = \sum_{k=1}^m a_{ik}b_{kj}$  pour tous  $1 \leq i \leq n$  et  $1 \leq j \leq \ell$ .

Il faut faire attention ici car le produit est défini uniquement lorsque le nombre de colonnes de  $A$  est égal au nombre de lignes de  $B$ .

- (ii) Une matrice  $A \in \mathbb{M}_{n \times n}(\mathbb{R})$  est dite inversible s'il existe  $B \in \mathbb{M}_{n \times n}(\mathbb{R})$  telle que

$$AB = \underbrace{\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}}{:=I_n} = BA.$$

- (iii) On note  $\text{GL}(n, \mathbb{R})$  l'ensemble des matrices  $n \times n$  (à coefficients dans  $\mathbb{R}$ ) qui sont inversibles. Avec la multiplication de matrices,  $\text{GL}(n, \mathbb{R})$  est un groupe.

AZ: Ce dernier exemple est fondamental. En fait, beaucoup d'autres exemples intéressants sont des sous-groupes (Définition 2.2.1) de  $\text{GL}(n, \mathbb{R})$ . On verra aussi que dans l'algèbre linéaire le calcul matriciel est très important. Je vous propose de regarder la vidéo « But what is a neural network? » sur la chaîne *3Blue1Brown*. Je vous invite aussi à lire cet article [↗](#) (en anglais).

**Remarque 4** (▲ À lire en fin de semestre). Soit  $K$  un corps et considérons le groupe  $\text{GL}(n, K)$ . On peut définir une loi de composition externe sur l'ensemble  $\mathbb{M}_{n \times n}(K)$  de la façon suivante :

$$\begin{aligned} \text{GL}(n, K) \times \mathbb{M}_{n \times n}(K) &\rightarrow \mathbb{M}_{n \times n}(K) \\ (P, A) &\mapsto PAP^{-1} \end{aligned}$$

Notez qu'en utilisant la notation de l'Exemple 1.2.5 on peut aussi considérer cette loi comme une application

$$\begin{aligned} \text{GL}(n, K) &\rightarrow \mathcal{F}(\mathbb{M}_{n \times n}(K), \mathbb{M}_{n \times n}(K)) \\ P &\mapsto (f_P : A \mapsto PAP^{-1}) \end{aligned}$$

telle que pour chaque  $P \in \text{GL}(n, K)$  la fonction  $f_P : \mathbb{M}_{n \times n}(K) \rightarrow \mathbb{M}_{n \times n}(K)$  est bijective. Pouvez-vous voir pourquoi? Ceci est donc un exemple d'action de groupe. Alors, on peut utiliser cette loi-là pour définir une relation d'équivalence sur l'ensemble  $\mathbb{M}_{n \times n}(K)$ . Pouvez-vous décrire les classes d'équivalence lorsque  $n = 2$  et  $K = \mathbb{R}$  ou  $\mathbb{C}$ ?

### 2.1.2 Pour réfléchir chez vous

**Exercice 2.1.11.** Si  $(G, *)$  est un groupe fini (c.-à-d. que l'ensemble  $G$  est fini) on peut décrire  $*$  à travers un tableau (ou matrix) : on place les éléments de  $G$  dans un ordre fixe  $g_1 = e, g_2, \dots, g_n$  et on pose que l'entrée  $a_{ij}$  du tableau soit l'élément  $g_i g_j \in G$  (et que doit être l'un des  $g_k$ ), cf. Exemple 2.2.6. Montrez que dans ce cas  $G$  est abélien si et seulement si le tableau donne une matrice symétrique (la transposée est égale à la matrice originale).

**Exercice 2.1.12.** Soit  $(G, *)$  un groupe avec élément neutre  $e$  et tel que  $g^2 = g * g = e$  pour tout  $g \in G$ . Montrez que  $G$  est abélien.

**Exercice 2.1.13.** Considérez l'ensemble  $\mathcal{H}$  de toutes les matrices  $H \in \mathbb{M}_{3 \times 3}(\mathbb{R})$  de la forme :

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

Montrez que  $\mathcal{H}$  est un groupe avec le produit des matrices. Ce groupe est appelé le groupe de Heisenberg et son origine est trouvée dans la mécanique quantique.

la matrice transposée (ou la transposée) d'une matrice  $A \in \mathbb{M}_{n \times m}(K)$  est la matrice  $A^t \in \mathbb{M}_{m \times n}(K)$ , obtenue en échangeant les lignes et les colonnes de  $A$ .

## 2.2 Sous-groupes

**Définition 2.2.1.** Soit  $(G, *)$  un groupe. Un sous-ensemble  $H \subset G$  est un **sous-groupe** de  $G$  si la loi  $*$  restreinte à  $H$  munit  $H$  d'une structure de groupe. Si tel est le cas, on écrit  $H \leq G$ .

Nous constatons que cette définition n'est pas très pratique. Nous démontrons donc ce qui suit.

**Proposition 2.2.2.** Soit  $(G, *)$  un groupe et  $H \subset G$  un sous-ensemble. Alors  $H$  est un sous-groupe de  $G$  si et seulement si les trois conditions suivantes sont vérifiées.

- (i)  $H$  est non vide,
- (ii) pour tous  $a, b \in H$ , on a  $a * b \in H$ , et
- (iii) pour tout  $h \in H$ , on a  $h^{-1} \in H$ .

*Démonstration.*

$\Rightarrow$  Tout d'abord, supposons que  $H$  soit un sous-groupe de  $G$ . Alors,  $H$  possède un élément neutre  $e_H$  et est donc non vide. En plus, (ii) s'ensuit, puisque la loi de composition sur  $G$  se restreint à une loi sur  $H$ . On a aussi que l'élément neutre de  $H$ ,  $e_H$ , est égal à  $e$ , l'élément neutre de  $G$ . En effet,

$$\begin{array}{ccc}
 & e_H \in H & \\
 & \downarrow e_H \text{ est élément neutre de } H & \\
 e_H * e = e_H & = & e_H * e_H \\
 \uparrow e_H \in G & & \uparrow \\
 e \text{ est élément neutre de } G & & \Rightarrow \boxed{e = e_H} \\
 & & \uparrow \text{simplification à gauche}
 \end{array}$$

Maintenant, montrons que (iii) est valide. Si  $h \in H$ , il existe  $\tilde{h} \in H$  tel que  $h * \tilde{h} = \tilde{h} * h = e_H$ . Alors, puisque  $e_H = e$ , par l'unicité des inverses, on obtient que  $\tilde{h} = h^{-1}$  et donc  $h^{-1} \in H$ .

⊞ Supposons maintenant que les conditions (i), (ii) et (iii) soient vérifiées. Alors, (ii) nous dit que l'image de tout couple  $(a, b) \in H \times H$  sous la loi  $*$  appartient à  $H$ , c.-à-d. que la restriction de  $*$  à  $H \times H$  définit bien une loi de composition sur  $H$ . La loi est associative car elle est déjà dans  $G$  (cf. Exercice 1.2.9). En plus, par (i) il existe  $h \in H$  et par la combinaison de (iii) et (ii) on a  $h * h^{-1} = e \in H$ . Autrement dit,  $H$  possède un élément neutre, notamment  $e$ , l'élément neutre de  $G$ . Enfin, il résulte de (iii) que tout élément de  $H$  possède un inverse. En conclusion, les conditions (G1), (G2) et (G3) dans la Définition 2.1.1 sont vérifiées et  $(H, *)$  est un groupe.  $\square$

### 2.2.1 Exemples

**Exemple 2.2.3.** Si  $G$  est un groupe quelconque, alors  $H = \{e\}$  et  $H = G$  sont des sous-groupes de  $G$ .

**Exemple 2.2.4.**  $\{1, -1\} \leq (\mathbb{R} \setminus \{0\}, \cdot)$ .

**Exemple 2.2.5.** Si  $G = \mathbb{Z}/6\mathbb{Z}$ , alors  $H = \{\bar{0}, \bar{2}, \bar{4}\}$  est un sous-groupe.

**Exemple 2.2.6.** Le groupe  $G = S_3$  a six éléments : l'élément neutre  $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ ,  $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ ,  $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ ,  $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ ,  $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$  et  $\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ .

On note que  $\sigma_1 \sigma_2 = \sigma_4 \neq \sigma_5 = \sigma_2 \sigma_1$ , et donc  $S_3$  n'est pas abélien. En plus,  $H = \{e, \sigma_4, \sigma_5\} \leq S_3$ . En effet, on a

o	e	$\sigma_4$	$\sigma_5$
e	e	$\sigma_4$	$\sigma_5$
$\sigma_4$	$\sigma_4$	$\sigma_5$	e
$\sigma_5$	$\sigma_5$	e	$\sigma_4$

### 2.2.2 Pour réfléchir chez vous

**Exercice 2.2.7.** Soit  $(G, *)$  un groupe abélien avec élément neutre  $e$  et posons

$$G_2 = \{g \in G \mid g^2 = g * g = e\}.$$

Montrer que  $G_2$  est un sous-groupe de  $G$ . Dans le cas particulier du groupe  $(\mathbb{Z}/4\mathbb{Z}, +)$ , trouver  $G_2$ .

**Exercice 2.2.8.** Plus généralement, soient  $(G, *)$  un groupe abélien et  $n \in \mathbb{N}$  un nombre naturel supérieur ou égal à deux. Montrez que  $H := \{g \in G \mid g^n = e\}$  est un sous-groupe de  $G$ . Ici  $g^n = \underbrace{g * \dots * g}_n$ . Est-ce que vous pouvez décrire  $H$  lorsque  $(G, *) = (\mathbb{C} \setminus \{0\}, \cdot)$ ?

**Exercice 2.2.9.** On dit qu'une matrice  $A \in \mathbb{M}_{n \times n}(\mathbb{R})$  est orthogonale si  $A^t = A^{-1}$ , c'est-à-dire que  $A^t A = I_n = A A^t$ . L'ensemble de toutes ces matrices orthogonales est noté  $O(n, \mathbb{R})$ . Montrez que  $O(n, \mathbb{R}) \leq \text{GL}(n, \mathbb{R})$ .

Ici  $A^t$  note la transposée de  $A$ .

## 2.3 Morphismes de groupes

Il n'est pas très utile de définir de nouveaux objets mathématiques si on ne sait pas comment les comparer entre eux. La notion qui permet de le faire pour les groupes est celle d'homomorphisme des groupes.

**Définition 2.3.1.** Soient  $(A, *)$  et  $(B, \circ)$  des groupes.

- (i) Un **homomorphisme** (ou simplement **morphisme**) de groupes de  $A$  dans  $B$  est une application  $\varphi : A \rightarrow B$ , telle que pour tous  $x, y \in A$  on a

$$\varphi(x * y) = \varphi(x) \circ \varphi(y).$$

$\uparrow$  loi sur  $A$                        $\uparrow$  loi sur  $B$

- (ii) Un **isomorphisme**, s'il existe, entre  $A$  et  $B$  est un homomorphisme bijectif. Si tel est le cas, nous disons que  $A$  et  $B$  sont isomorphes, ou que  $A$  est isomorphe à  $B$  (et vice versa), et on écrit  $A \simeq B$ .

Voici quelques propriétés qui suivent directement de la Définition 2.3.1.

**Lemme 2.3.2.** Soit  $\varphi : A \rightarrow B$  un morphisme de groupes de  $(A, *)$  dans  $(B, \star)$ , et soit encore  $a \in A$ . Alors

- (i)  $\varphi(e_A) = e_B$ ,
- (ii)  $\varphi(a^{-1}) = \varphi(a)^{-1}$
- (iii) et plus généralement pour tout  $n \in \mathbb{Z}$  on a  $\varphi(a^n) = \varphi(a)^n$ .

*Démonstration.* Comme déjà mentionné, la preuve découle directement de la Définition 2.3.1 (i) et est laissée en exercice.  $\square$

La notion de morphisme de groupes nous permet aussi d'introduire deux autres exemples de sous-groupes qui sont très importants.

**Définition 2.3.3.** Le **noyau** d'un homomorphisme de groupes  $\varphi : A \rightarrow B$  est l'ensemble

$$\ker(\varphi) := \{a \in A \mid \varphi(a) = e_B\} \subset A.$$

$\uparrow$  l'élément neutre de  $B$

On désigne l'image de  $\varphi$  par  $\text{im}(\varphi) := \{\varphi(a) \mid a \in A\} \subset B$ .

**Proposition 2.3.4.** Si  $\varphi : A \rightarrow B$  est un morphisme de groupes de  $(A, *)$  dans  $(B, \star)$ , alors  $\ker(\varphi) \leq A$  et  $\text{im}(\varphi) \leq B$ .

*Démonstration.*

- Montrons que  $\ker(\varphi) \leq A$  en utilisant la Proposition 2.2.2. Par Lemme 2.3.2 (i),  $e_A \in \ker(\varphi)$  et donc  $\ker(\varphi)$  est non vide. Maintenant, prenons  $x, y \in \ker(\varphi)$ . Alors

$$\varphi(x * y) = \varphi(x) \star \varphi(y) \stackrel{x, y \in \ker(\varphi)}{\downarrow} e_B \star e_B = e_B \stackrel{\text{Définition 2.3.3}}{\Rightarrow} x * y \in \ker(\varphi)$$

$\uparrow$  Définition 2.3.1 (i)                       $\uparrow$  Définition 2.3.3

et, également, par Lemme 2.3.2 (ii) on a

$$\varphi(a^{-1}) = \underbrace{\varphi(a)^{-1}}_{=e_B} = e_B.$$

- Je vous laisse comme exercice de montrer que  $\text{im}(\varphi) \leq B$ .

□

### 2.3.1 Exemples

**Exemple 2.3.5.** Soit  $G$  un groupe quelconque. Alors l'application identité  $\text{id} : G \rightarrow G$  est un morphisme de groupes, tout comme l'application constante  $\varphi : G \rightarrow \{e\}$ .

**Exemple 2.3.6.** Soit  $H = \{e, \sigma_4, \sigma_5\} \leq S_3$  comme dans l'Exemple 2.2.6. On définit  $\varphi : \mathbb{Z}/3\mathbb{Z} \rightarrow H$  par  $\varphi(\bar{0}) = e, \varphi(\bar{1}) = \sigma_4$  et  $\varphi(\bar{2}) = \sigma_5$ . On vérifie que  $\varphi$  est un isomorphisme de groupes.

**Exemple 2.3.7.** Soit  $n \in \mathbb{N}, n \geq 1$  et soit  $\varphi : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/n\mathbb{Z}, +)$  le morphisme défini par  $a \mapsto \bar{a}$ . Alors  $\ker(\varphi) = \{a \in \mathbb{Z} \mid \bar{a} = \bar{0}\} = \{a \in \mathbb{Z} \mid n \text{ divise } a\} = n\mathbb{Z}$ . Est-ce qu'il y a d'autres sous-groupes de  $(\mathbb{Z}, +)$  ?

**Exemple 2.3.8.** Soit  $H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \right\} \leq \text{GL}(2, \mathbb{R})$  et considérons l'application  $\varphi : H \rightarrow \mathbb{R}$  donnée par  $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mapsto a$ . On peut vérifier que  $\varphi$  est un isomorphisme de groupes de  $H$  (avec la multiplication des matrices) dans  $(\mathbb{R}, +)$ .

### 2.3.2 Pour réfléchir chez vous

**Exercice 2.3.9.** Trouvez un sous-groupe  $H \leq S_3$  tel qu'il existe un isomorphisme de groupes  $\mathbb{Z}/2\mathbb{Z} \rightarrow H$ . Décrivez explicitement l'isomorphisme. Combien de sous-groupes de ce type existe-t-il ?

**Exercice 2.3.10.** Soit  $S^1$  le cercle unité dans  $\mathbb{R}^2$ , i.e.  $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ . On définit la loi de composition  $*$  sur  $S^1$  par

$$(a, b) * (c, d) = (ac - bd, ad + bc)$$

pour  $a, b, c, d \in \mathbb{R}$ . On sait que  $(S^1, *)$  est un groupe. Soit  $f : \mathbb{R} \rightarrow S^1$  l'application définie par  $f(x) = (\cos(2\pi x), \sin(2\pi x))$  pour  $x \in \mathbb{R}$ .

- Montrer que  $f$  est un homomorphisme de groupes entre  $(\mathbb{R}, +)$  et  $(S^1, *)$ .
- Montrer que  $f$  est surjective et déterminer son noyau  $\ker(f)$ . L'application  $f$  est-elle un isomorphisme de groupes ?

### 3.1 Anneaux


**Définition 3.1.1.** Un **anneau unitaire**  $(A, +, \cdot)$  est un ensemble (non vide) muni de deux lois de composition

$$\begin{aligned} + : A \times A &\rightarrow A & \text{et} & & \cdot : A \times A &\rightarrow A \\ (x, y) &\mapsto x + y & & & (x, y) &\mapsto x \cdot y \end{aligned}$$

satisfaisant les axiomes suivants :

- (A1)  $(A, +)$  est un groupe abélien,
- (A2)  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  pour tous  $a, b, c \in A$  (la loi  $\cdot$  est associative)
- (A3) il existe  $1_A \in A$  tel que  $1_A \cdot a = a \cdot 1_A = a$  pour chaque  $a \in A$  ( $1_A$  est élément neutre pour  $\cdot$ )
- (A4) la loi  $\cdot$  est distributive à droite et à gauche sur la loi  $+$ .

AZ:  Notez que cachée dans la définition ci-dessus se trouve la stabilité de  $A$  par rapport aux deux lois.

AZ:  Pour moi un anneau est toujours unitaire, c'est-à-dire que (A3) est toujours vrai pour les triplets  $(A, +, \cdot)$  qui m'intéressent, donc je me permettrai de parler simplement d'anneaux. Par contre, pour moi, il existe des anneaux très intéressants qui ne sont pas commutatifs, c'est-à-dire, dans lesquels  $a \cdot b \neq b \cdot a$  !

**Remarque 5.** Si  $(A, +, \cdot)$  est un anneau (unitaire), on écrira souvent  $ab$  à la place de  $a \cdot b$  et on parlera de la multiplication dans  $A$ . Notez que les inverses multiplicatifs n'existent pas nécessairement. En plus, on suppose que  $1_A \neq 0$ , et donc que  $A \neq \{0\}$ .

#### 3.1.1 Exemples

**Exemple 3.1.2.** Les ensembles  $\mathbb{Z}, \mathbb{Q}$  ou  $\mathbb{R}$  munis des opérations usuelles d'addition et de multiplication sont des anneaux commutatifs.

**Exemple 3.1.3.** Soit  $n \in \mathbb{N}$  avec  $n \geq 2$ . On peut munir l'ensemble  $\mathbb{Z}/n\mathbb{Z}$  des entiers modulo  $n$  d'une deuxième loi de composition. On peut associer à chaque paire  $(\bar{a}, \bar{b})$  l'élément  $\overline{ab} \in \mathbb{Z}/n\mathbb{Z}$ . Je vous laisse comme exercice de vérifier que les axiomes (A1), ..., (A4) dans la Définition 3.1.1 sont valables.

**Exemple 3.1.4.** Soit  $I$  un intervalle ouvert de la droite réelle et soit encore  $\mathcal{F}(I, \mathbb{R})$  l'ensemble de toutes les fonctions de  $I$  dans  $\mathbb{R}$ . Considérez les opérations d'addition et de multiplication de fonctions :

$$(f + g)(x) := f(x) + g(x), \quad (f \cdot g)(x) := f(x) \cdot g(x).$$

Alors,  $(\mathcal{F}(I, \mathbb{R}), +, \cdot)$  est un anneau avec ces lois. En fait, on peut considérer tout ensemble  $E$  non vide et tout anneau  $(A, +, \cdot)$ , et il est toujours vrai que  $\mathcal{F}(E, A)$  est un anneau avec l'addition et la multiplication usuelles.

**Exemple 3.1.5** (Des matrices revisitées). Si  $A$  est un anneau, on peut considérer l'ensemble  $\mathbb{M}_{n \times n}(A)$  des matrices  $n \times n$  à coefficients dans  $A$ . Avec les mêmes définitions de l'addition et de la multiplication que pour les matrices réelles, cet ensemble est un anneau.

### 3.1.2 Quelques propriétés

**Lemme 3.1.6.** Soit  $(A, +, \cdot)$  un anneau (unitaire). Alors,

- (i)  $0 \cdot a = a \cdot 0 = 0$  pour tout  $a \in A$ ,
- (ii)  $(-a)b = a(-b) = -(ab)$  pour tous  $a, b \in A$ , et
- (iii)  $(-a)(-b) = ab$  pour tous  $a, b \in A$ .

*Démonstration.*

- (i) Pour tout  $a \in A$  on a

$$0 \cdot a = (0 + 0) \cdot a \quad (0 \text{ est l'élément neutre pour } +)$$

$$= 0 \cdot a + 0 \cdot a. \quad (\cdot \text{ est distributive à droite sur } +)$$

Notez maintenant que nous pouvons également écrire  $0 \cdot a = 0 \cdot a + 0$ . Donc, en utilisant la simplification à gauche (Proposition 2.1.3), il s'ensuit que  $0 \cdot a = 0$ . Pour démontrer que  $a \cdot 0 = 0$  nous pouvons utiliser un argument symétrique complètement analogue :

car 0 est l'élément neutre pour +

$$a \cdot 0 + 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

- (ii) Il suffit d'observer que pour tous  $a, b \in A$  nous avons que

$$ab + (-a)b \stackrel{\cdot \text{ est distributive à droite sur } +}{=} (a + (-a)) \cdot b \stackrel{\text{Lemme 3.1.6 (i)}}{=} 0 \cdot b \stackrel{\downarrow}{=} 0$$

↑  
définition d'inverse et 0 est l'élément neutre pour +

et, similairement,

$$ab + a(-b) \stackrel{\cdot \text{ est distributive à gauche sur } +}{=} a \cdot (b + (-b)) = a \cdot 0 = 0.$$

Donc, par l'unicité des inverses additifs (c.-à-d. par rapport à +), on a que  $(-a)b = a(-b) = -(ab)$ .

- (iii) En utilisant (ii) deux fois et le fait que  $-(-a) = a$  (Proposition 2.1.3 (ii)), nous obtenons que

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$$

pour tous  $a, b \in A$ .

□

### 3.1.3 Morphismes et sous-anneaux

**Définition 3.1.7** (Morphisme d'anneaux). Soient  $(A, +, \cdot)$  et  $(B, \oplus, \times)$  deux anneaux, avec unités (des éléments neutres multiplicatifs)  $1_A$  et  $1_B$ , respectivement. Un **morphisme d'anneaux** est une application  $\varphi : A \rightarrow B$  telle que pour tous  $a, b \in A$  on a

- $\varphi(a + b) = \varphi(a) \oplus \varphi(b)$ ,
- $\varphi(a \cdot b) = \varphi(a) \times \varphi(b)$ , et
- $\varphi(1_A) = 1_B$ .

En algèbre, il est toujours intéressant de considérer les sous-structures. Par exemple, nous avons vu que de nombreux exemples de groupes proviennent de l'étude des sous-groupes de  $\text{GL}(n, \mathbb{R})$ . Pour les anneaux, le concept de sous-anneau est le suivant.

**Définition 3.1.8** (Sous-anneau). Soient  $(A, +, \cdot)$  un anneau et  $S \subset A$ . On dit que  $(S, +, \cdot)$  est un **sous-anneau** de  $A$  si

- (S1)  $(S, +)$  est un sous-groupe de  $(A, +)$  – en particulier,  $S$  est non vide ;
- (S2) nous avons que  $a \cdot b$  appartient à  $S$  pour tous  $a, b \in S$  ;
- (S3) et l'élément neutre multiplicatif  $1_A$  de  $A$  appartient à  $S$ .

AZ: Notez que le point (ii) dans la définition ci-dessus nous dit que  $S$  est unitaire et que  $1_S = 1_A$ .

**Lemme 3.1.9.** Soient  $(A, +, \cdot)$  un anneau et  $S \subset A$ . Alors, les affirmations suivantes sont équivalentes :

- (i)  $(S, +, \cdot)$  est un sous-anneau de  $(A, +, \cdot)$ ,
- (ii)  $1_A \in S$  et pour tous  $a, b \in S$ , on a  $a - b \in S$  et  $a \cdot b \in S$ .

*Démonstration.*

(i)  $\Rightarrow$  (ii) Cela découle directement de la définition d'un sous-anneau.

(ii)  $\Rightarrow$  (i) Tout d'abord on note que (S2) et (S3) sont valides d'après (ii). Maintenant, on montre que (S1) est valide. On utilise la Proposition 2.2.2. Comme  $1_A \in S$ ,  $S$  est non vide et comme  $1_A - 1_A = 0$  on a que  $0 \in S$ . Donc on a aussi que

- $b \in S \Rightarrow 0 - b = -b \in S$ , et, par conséquent, que
- $a, b \in S \Rightarrow a - (-b) = a + b \in S$ .

C'est-à-dire que  $(S, +)$  est un groupe.

□

### 3.1.4 Plus d'exemples

Il découle de la définition de sous-anneau que si  $(S, +, \cdot)$  est un sous-anneau de  $(A, +, \cdot)$ , alors  $S$  est un anneau. Nous pouvons donc examiner d'autres exemples d'anneaux.

**Exemple 3.1.10.** Soit  $m \geq 2$  un nombre entier naturel qui n'est pas un carré parfait. Considérez l'ensemble

$$\mathbb{Z}[\sqrt{m}] := \{a + b \cdot \sqrt{m} \mid a, b \in \mathbb{Z}\}.$$

Alors,  $(\mathbb{Z}[\sqrt{m}], +, \cdot)$  est un sous-anneau de  $(\mathbb{R}, +, \cdot)$ .

**Exemple 3.1.11.** Soit  $I$  un intervalle ouvert de la droite réelle et soit encore  $\mathcal{C}(I, \mathbb{R})$  l'ensemble de toutes les fonctions de  $I$  dans  $\mathbb{R}$  qui sont continues. Alors,  $\mathcal{C}(I, \mathbb{R})$  est un sous-anneau de l'anneau  $\mathcal{F}(I, \mathbb{R})$  décrit dans l'Exemple 3.1.4 et, par conséquent, il est lui-même un anneau. De même, les règles de dérivation montrent que l'ensemble de toutes les fonctions  $f : I \rightarrow \mathbb{R}$  qui sont dérivables/différentiables sur l'intervalle  $I$  est aussi un anneau. Pourquoi? Après avoir appris ces concepts, essayez de bien comprendre cet exemple.

▲ Les notions de fonction continue et de fonction dérivable seront étudiées dans le cours d'analyse.

## 3.2 Corps

Un corps est un anneau unitaire commutatif dans lequel tout élément non nul (c.-à-d.  $\neq 0$ ) est inversible par rapport à la multiplication :

**Définition 3.2.1.** Soit  $(K, +, \cdot)$  un anneau unitaire. On dit que  $K$  est un **corps** si et seulement si  $K \neq \{0\}$ , la loi  $\cdot$  est commutative, et pour tout  $a \in K \setminus \{0\}$ , il existe  $a^{-1} \in K$  tel que  $a \cdot a^{-1} = a^{-1} \cdot a = 1$ .

On peut prouver qu'un anneau  $(K, +, \cdot)$  est un corps si et seulement si  $(K, +)$  et  $(K \setminus \{0\}, \cdot)$  sont des groupes abéliens et, en plus, on a que  $(a + b) \cdot c = a \cdot c + b \cdot c$  pour tous  $a, b, c \in K$ . Notez que la commutativité de la loi  $\cdot$  implique que la distributivité à gauche est équivalente à la distributivité à droite.

Les anneaux  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$  et  $(\mathbb{C}, +, \cdot)$ , où  $+$  et  $\cdot$  sont les opérations usuelles, sont des corps. Par contre,  $(\mathbb{Z}, +, \cdot)$  n'est pas un corps. Pourquoi?

Pourquoi? Essayez de prouver que cette affirmation est vraie.

Voir aussi Section 3.2.2 ci-dessous.

### 3.2.1 Corps finis

**Proposition 3.2.2.** Soit  $p \in \mathbb{N}$  un nombre premier. Alors, tout élément de  $\mathbb{Z}/p\mathbb{Z}$  différent de  $\bar{0}$  est inversible.

*Démonstration.* Soit  $a \in \mathbb{Z}$  tel que  $\bar{a} \neq \bar{0}$ . Comme  $a$  n'est pas un multiple de  $p$  et  $p$  est un nombre premier, on a que  $\text{pgcd}(a, p) = 1$ . Donc, par l'identité de Bézout, il existe  $b, c \in \mathbb{Z}$  tels que  $ab + pc = 1$ . Donc  $ab - 1 = -pc$  et  $p$  divise  $ab - 1$ . Par conséquent,  $\overline{ab} = \bar{1}$  et on déduit que  $\bar{a}$  est inversible.  $\square$

**Corollaire 3.2.3.** Soit  $p \in \mathbb{N}$  un nombre premier. Alors,  $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$  est un corps. Souvent, on écrit  $\mathbb{F}_p$  pour désigner le corps fini  $\mathbb{Z}/p\mathbb{Z}$ .

### 3.2.2 Le corps de nombres complexes

Le corps de nombres complexes est l'ensemble  $\mathbb{C}$  des nombres qui peuvent être écrits comme  $a + b \cdot i$ , où  $a, b \in \mathbb{R}$  et  $i$  satisfait  $i^2 = -1$  (c'est l'une des racines de  $p = x^2 + 1 \in \mathbb{R}[x]$ ); et qui est équipé des opérations :

$$(a + b \cdot i) + (c + d \cdot i) := (a + c) + (b + d) \cdot i$$

et

$$(a + b \cdot i) \cdot (c + d \cdot i) := (ac - bd) + (ad + bc) \cdot i.$$

La partie réelle du nombre complexe  $z = a + b \cdot i$  est  $\Re(z) = a$ , et la partie imaginaire est  $\Im(z) = b$ . En plus, nous définissons le conjugué d'un nombre complexe  $z = a + b \cdot i$  comme étant le nombre complexe  $\bar{z} := a - b \cdot i$ . Finalement, notez qu'on peut construire une bijection  $\mathbb{C} \rightarrow \mathbb{R}^2$  définie par  $a + b \cdot i \mapsto (a, b)$ . Le module d'un nombre complexe  $z = a + b \cdot i$  est le nombre réel noté  $|z|$  défini par  $\sqrt{a^2 + b^2}$ . Autrement dit,  $|z|$  est égal à la distance (euclidienne) entre les points  $(a, b)$  et  $(0, 0)$ .

**Plan complexe et forme polaire** Par définition, tout nombre complexe correspond uniquement à un vecteur dans le plan  $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ . La somme des nombres complexes correspond à la somme des vecteurs, et la conjugaison correspond à la réflexion par rapport à l'axe réel, c-à-d.  $\mathbb{R} \times \{0\} \simeq \{a + b \cdot i \in \mathbb{C} \mid b = 0\}$ . Alors, si  $z = a + b \cdot i \in \mathbb{C} \setminus \{0\}$ , en notant  $r = |z| > 0$  le module et  $\theta = \arctan(b/a) \in (-\pi, \pi]$  l'argument, on peut écrire  $a + b \cdot i = \underset{=a}{r \cos \theta} + \underset{=b}{(r \sin \theta)} \cdot i$ .

En fait, on considère  $\theta$  modulo  $2\pi$

**Forme matricielle** Soit  $\mathcal{C}$  l'ensemble de toutes les matrices  $2 \times 2$  à coefficients réels qui ont la forme :

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

On peut prouver que  $\mathcal{C}$  est un sous-anneau de  $\mathbb{M}_{2 \times 2}(\mathbb{R})$  et que l'application

$$\begin{aligned} \varphi : \mathbb{C} &\rightarrow \mathcal{C} \\ a + b \cdot i &\mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{aligned}$$

est un isomorphisme (= morphisme bijectif) d'anneaux.

### 3.3 Anneaux de polynômes

Soit  $(A, +, \cdot)$  un anneau et considérons  $A^{\mathbb{N}}$ , l'ensemble des suites ordonnées  $(a_0, a_1, a_2, \dots)$  d'éléments de  $A$  avec  $a_i \neq 0$  pour un nombre fini de  $i$ . On peut définir deux lois de composition interne sur  $A^{\mathbb{N}}$  :

- $(a_0, a_1, \dots) \oplus (b_0, b_1, \dots) := (a_0 + b_0, a_1 + b_1, \dots)$ , et
- $(a_0, a_1, \dots) \odot (b_0, b_1, \dots) := (c_0, c_1, \dots)$ , où  $c_k := \sum_{i+j=k} a_i b_j$  pour chaque  $k \in \mathbb{N}$ .

Ça veut dire qu'il existe  $n \in \mathbb{N}$  tel que  $a_i = 0$  pour tous  $i > n$

On note tout de suite que  $(A^{\mathbb{N}}, \oplus)$  est un groupe abélien avec élément neutre  $(0, 0, 0, \dots)$ , l'inverse de  $(a_0, a_1, \dots)$  est  $(-a_0, -a_1, \dots)$ , et l'associativité et la commutativité de la loi  $\oplus$  sont héritées de celles de  $+$  (dans  $A$ ). On note aussi que  $\odot$  est également associative et que son élément neutre est la suite  $(1_A, 0, 0, \dots)$ .

En ce qui concerne  $A^{\mathbb{N}}$ , nous adoptons les notations suivantes. On écrit :

$$(N1) \quad 0 = (0, 0, \dots),$$

$$(N2) \quad x := (0, 1_A, 0, 0, \dots),$$

$$(N3) \quad 1 = (1_A, 0, 0, \dots), \text{ et}$$

$$(N4) \quad \text{pour } a \in A, a = (a, 0, 0, \dots).$$

En plus, on remplace  $\oplus$  par  $+$  et  $\odot$  par  $\cdot$  (ou par la juxtaposition d'éléments), et on désigne  $(A^{\mathbb{N}}, \oplus, \odot)$  par  $(A[x], +, \cdot)$ . On appelle ce triple **l'anneau des polynômes à coefficients dans  $A$**  (voir Proposition 3.3.1 ci-dessous). Les affirmations suivantes sont des conséquences directes de ces nouvelles notations.

- Pour  $a \in A$ , on a que  $a = a \cdot 1$ .
- Pour  $a \in A$ , on a que  $(0, a, 0, \dots) = (a, 0, 0, \dots) \odot (0, 1_A, 0, \dots) = a \cdot x$ .
- Pour  $n \in \mathbb{N}, n \geq 1$ , on a que  $(0, 0, \dots, 1_A, 0, \dots) = x^n = \underbrace{x \cdot \dots \cdot x}_n$ , où le terme  $1_A$  est à la  $(n + 1)$ -ième place.
- Pour  $a_i \in A, i \in \mathbb{N}$ , si  $a_k = 0$  pour tout  $k > n$ , on a que

$$(a_0, a_1, \dots, a_n, 0, 0, \dots) = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n.$$

**Proposition 3.3.1.** *L'ensemble  $A[x]$ , avec  $+$  et  $\cdot$ , est un anneau. Si  $A$  est commutatif, alors  $A[x]$  est commutatif. L'application  $\varphi : A \rightarrow A[x]$  définie par  $\varphi(a) = (a, 0, 0, \dots)$  est un morphisme d'anneaux qui, par ailleurs, est injectif.*

AZ: Notez qu'étant donné le morphisme  $\varphi$  de la Proposition 3.3.1, on identifie  $A$  avec  $\varphi(A)$ , et  $A$  devient un sous-anneau de l'anneau de polynômes  $A[x]$ .

**Définition 3.3.2.** Soit  $(A, +, \cdot)$  un anneau.

- (i) Soit  $p = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n \in A[x]$ , avec  $a_n \neq 0$ . On dit que  $p$  est de degré  $n$ , et on écrit  $\deg(p) = n$ . On pose  $\deg(0) = -\infty$ .
- (ii) Pour  $p \in A[x]$ , si  $\deg(p) = n$  et  $a_n = 1_A$  (le coefficient du terme de plus haut degré), on dit que  $p$  est unitaire.
- (iii) Si  $\deg(p) = 0$ , ou si  $p = 0$ , on dit que  $p$  est un polynôme constant.

### 3.3.1 Polynômes à coefficients dans un corps

Si  $K$  est un corps, nous savons d'après la Proposition 3.3.1 que l'ensemble des polynômes à coefficients dans  $K$ , muni de l'addition et de la multiplication des polynômes, est un anneau commutatif. En plus, dans le cas où  $K$  est un sous-anneau d'un anneau  $A$ , il est utile de considérer les morphismes d'évaluation en un élément  $a \in A$ .

**Définition 3.3.3.** Soit  $K$  un corps qui est sous-anneau d'un anneau  $A$ . Soit encore  $p \in K[x] \subset A[x]$  avec  $p = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n$ .

(i) L'évaluation de  $p$  en  $\alpha \in A$ , notée  $p(\alpha)$ , est l'élément de  $A$  suivant :

$$a_0 + a_1\alpha + \dots + a_n\alpha^n.$$

- Pour chaque  $\alpha \in A$  fixé, on peut donc considérer le morphisme d'anneaux  $ev_\alpha : K[x] \rightarrow A$  défini par  $p \mapsto p(\alpha)$ .
- On peut également considérer le morphisme d'anneaux  $\varepsilon : K[x] \rightarrow \mathcal{F}(A, A)$  défini par

$$p \mapsto (\alpha \mapsto ev_\alpha(p) = p(\alpha)).$$

(ii) Un élément  $\alpha \in A$  s'appelle une **racine** de  $p \in K[x]$  si  $p(\alpha) = 0_A$ .

**Théorème 3.3.4** (division euclidienne des polynômes). Soient  $p, q \in K[x]$  avec  $q \neq 0$ . Alors, il existe un unique couple de polynômes  $g, r \in K[x]$  avec  $\deg(r) < \deg(q)$  et tels que  $p = g \cdot q + r$

*Démonstration.* Admis sans preuve. □

**Corollaire 3.3.5.** Soit  $K$  un corps et soient encore  $p \in K[x]$  et  $\alpha \in K$ . Alors,  $\alpha$  est une racine de  $p$  si et seulement si  $x - \alpha$  divise  $p$ , c-à-d.  $p = g(x - \alpha)$  pour un certain  $g \in K[x]$ .

*Démonstration.* L'assertion découle du théorème précédent en posant  $q = x - \alpha$  et en utilisant le fait que  $ev_\alpha : K[x] \rightarrow K$  est un morphisme d'anneaux. □

### 3.3.2 Théorème fondamental de l'algèbre

**Définition 3.3.6.** Soit  $K$  un corps. On dit qu'un polynôme  $p \in K[x]$  est scindé s'il existe  $\beta, b_1, \dots, b_n \in K$  tels que

$$p = \beta(x - b_1) \cdot (x - b_2) \cdot \dots \cdot (x - b_n)$$

**Théorème 3.3.7** (Théorème fondamental de l'algèbre). Tout polynôme à coefficients dans  $\mathbb{C}$  est scindé.

*Démonstration.* Admis sans preuve. □

## 3.4 Pour réfléchir chez vous

**Exercice 3.4.1.** Comprenez bien l'exemple suivant. Soit  $\alpha \in \mathbb{C}$  une racine d'un polynôme du second degré avec des coefficients réels. Par exemple, on peut considérer  $\alpha = \sqrt{2}$  et le polynôme  $p(x) = x^2 - 2$ . Alors, l'ensemble

$$\mathbb{R}[\alpha] := \{a + b \cdot \alpha \mid a, b \in \mathbb{R}\}$$

est un sous-anneau de  $(\mathbb{C}, +, \cdot)$ .

**Exercice 3.4.2.** Soit  $m \geq 2$  un nombre entier naturel qui n'est pas un carré, par exemple, on peut considérer  $m = 2$ . Considérez l'ensemble

$$\mathbb{Q}[\sqrt{m}] := \{a + b \cdot \sqrt{m} \mid a, b \in \mathbb{Q}\}.$$

Prouvez que les affirmations suivantes sont vraies.

- (i) L'application  $\varphi : \mathbb{Q} \rightarrow \mathbb{Q}[\sqrt{m}]$  définie par  $a \mapsto a$  (l'inclusion) est un morphisme d'anneaux injectif.
- (ii)  $(\mathbb{Q}[\sqrt{m}], +, \cdot)$  est un corps.

**Exercice 3.4.3.** Considérez l'ensemble  $\mathbb{Q}[\sqrt{2}]$  (comme dans l'Exercice 3.4.2) et le sous-anneau  $(A, +, \cdot)$  de  $\mathbb{M}_{2 \times 2}(\mathbb{Q})$  de toutes les matrices qui ont la forme

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \quad a, b \in \mathbb{Q}.$$

Prouvez que l'application  $\varphi : \mathbb{Q}[\sqrt{2}] \mapsto A$  définie par  $a + b \cdot \sqrt{2} \mapsto \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$  est un isomorphisme d'anneaux, c.-à-d. un morphisme qui est bijectif.

**Exercice 3.4.4.** Trouvez un morphisme d'anneaux  $\varphi : (\mathbb{Z}, +, \cdot) \rightarrow (\mathbb{Z}, +, \cdot)$ . Existent-ils? Si oui, combien? Et si plutôt nous considérons des morphismes  $\varphi : (\mathbb{Q}[\sqrt{2}], +, \cdot) \rightarrow (\mathbb{Q}[\sqrt{2}], +, \cdot)$ ? Je prétends que dans ce dernier cas, il n'y en a que deux, et que tous deux sont des isomorphismes. Pourquoi? Pouvez-vous les décrire?

## 4.1 Espaces vectoriels

**Définition 4.1.1.** Soit  $K$  un corps. Un  $K$ -espace vectoriel est un ensemble non vide  $V$  munis de deux lois :

- (E1) une loi interne  $+$  :  $V \times V \rightarrow V$  telle que  $(V, +)$  est un groupe abélien ; et  
 (E2) une loi externe  $\cdot$  :  $K \times V \rightarrow V$  telle que pour tous  $u, v \in V$  et pour tous  $\lambda, \mu \in K$  on a que
- $1_K \cdot v = v$ ,
  - $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$ ,
  - $(\lambda\mu) \cdot v = \lambda \cdot (\mu \cdot v)$ , et
  - $\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v$ .

Si  $V$  est un  $K$ -espace vectoriel, ses éléments s'appellent les vecteurs et les éléments de  $K$  s'appellent les scalaires. On parle de l'addition de vecteurs et de la multiplication par un scalaire. On notera l'élément neutre du groupe  $(V, +)$  par  $0$  (ou  $0_V$  si nécessaire) et l'inverse de  $v \in V$  par  $-v$ .

on peut aussi dire espace vectoriel sur  $K$

### 4.1.1 Premières propriétés

**Proposition 4.1.2.** Soit  $V$  un  $K$ -espace vectoriel et soient encore  $\lambda \in K$  et  $v \in V$ . Alors,

- (i)  $\lambda \cdot 0_V = 0_V$ ,  
 (ii)  $0_K \cdot v = 0_V$ ,  
 (iii)  $\lambda \cdot v = 0_V \Rightarrow (\lambda = 0_K) \vee (v = 0_V)$ , et  
 (iv)  $(-\lambda) \cdot v = \lambda \cdot (-v) = -(\lambda \cdot v)$ .

*Démonstration.* Soient  $\lambda \in K$  et  $v \in V$ .

- (i)  $0_V + \lambda \cdot 0_V = \lambda \cdot 0_V = \lambda \cdot (0_V + 0_V) = \lambda \cdot 0_V + \lambda \cdot 0_V$  et en simplifiant à droite on obtient  $\lambda \cdot 0_V = 0_V$ .  
 (ii)  $0_V + 0 \cdot v = 0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v$  et on conclut comme dans (i).  
 (iii) Si  $\lambda = 0$  il n'y a rien à prouver, donc supposons que  $\lambda \neq 0$ . Alors, il existe  $\lambda^{-1} \in K$  et on a que

$$\begin{aligned} \lambda \cdot v = 0_V &\Rightarrow \lambda^{-1} \cdot (\lambda \cdot v) = \lambda^{-1} \cdot 0_V \\ &\Rightarrow (\lambda^{-1} \cdot \lambda) \cdot v = 0_V \\ &\Rightarrow 1 \cdot v = 0_V \\ &\Rightarrow v = 0_V \end{aligned}$$

- (iv) On observe que

$$(-\lambda) \cdot v + \lambda \cdot v = (-\lambda + \lambda) \cdot v = 0 \cdot v = 0_V$$

et que

$$\lambda \cdot (-v) + \lambda \cdot v = \lambda \cdot (-v + v) = \lambda \cdot 0_V = 0_V.$$

Donc, par l'unicité des inverses, on a  $(-\lambda) \cdot v = \lambda \cdot (-v) = -(\lambda \cdot v)$ . Notez que, par définition,  $(V, +)$  est un groupe abélien. □

### 4.1.2 Exemples

**Exemple 4.1.3** (Le plus petit). L'exemple le plus simple d'espace vectoriel est l'espace nul  $V = \{0\}$ , qui ne contient que le vecteur nul. On va voir que tout  $K$ -espace vectoriel contient un sous-espace vectoriel isomorphe à celui-ci.

**Exemple 4.1.4** (Espace des  $n$ -uplets). Soit  $K$  un corps et  $V$  le produit cartésien  $K \times \dots \times K$  ( $n$  fois) qu'on notera  $K^n$ . Nous pouvons munir  $V$  d'une structure d'espace vectoriel comme suit. Si  $u = (u_1, \dots, u_n)$  et  $v = (v_1, \dots, v_n)$  appartiennent à  $K^n$ , et  $\lambda \in K$ , les deux lois sont définies par :

- $u + v := (u_1 + v_1, \dots, u_n + v_n)$ , et
- $\lambda \cdot v = (\lambda v_1, \dots, \lambda v_n)$ .

En particulier, tout corps peut être considéré comme un espace vectoriel sur lui-même.

**Exemple 4.1.5** (Espace des polynômes). Soit  $K[x]$  l'anneau de polynômes à coefficients dans un corps  $K$ . Alors  $(K[x], +)$  est un groupe abélien et on peut définir une loi externe, la multiplication par un scalaire, comme suit. Si  $\lambda \in K$  et  $f = a_0 + a_1x + \dots + a_nx^n \in K[x]$ , on pose

$$\lambda \cdot f := \lambda a_0 + \lambda a_1x + \dots + \lambda a_nx^n.$$

Avec ces opérations,  $K[x]$  devient un espace vectoriel sur  $K$ .

**Exemple 4.1.6** (Espace des fonctions). Soit  $E$  un ensemble non vide quelconque. Si  $K$  est un corps, l'ensemble  $\mathcal{F}(E, K)$  de toutes les applications de  $E$  dans  $K$  est un anneau. En particulier,  $(\mathcal{F}(E, K), +)$  est un groupe abélien et on définit une loi externe par : pour tout  $\lambda \in K$  et pour tout  $f \in \mathcal{F}(E, K)$  on pose

$$\lambda \cdot f := E \ni x \mapsto \underbrace{\lambda \cdot f(x)}_{\in K} \in K.$$

Je vous laisse comme exercice de vérifier que  $\mathcal{F}(E, K)$  muni de ces opérations est un  $K$ -espace vectoriel.

**Exemple 4.1.7** (Espace des matrices). Rappelez-vous qu'une matrice  $n \times m$  à coefficients dans un corps  $K$  est un tableau à  $n$ -lignes et  $m$  colonnes constituées d'éléments de  $K$  :

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}.$$

L'ensemble  $\mathbb{M}_{n \times m}(K)$  de toutes ces matrices peut être muni d'une loi interne  $+$  et d'une loi externe  $\cdot$  comme suit. Soient  $A, B \in \mathbb{M}_{n \times m}(K)$ , avec  $A = (a_{ij})$  et  $B = (b_{ij})$  et soit encore  $\lambda \in K$ . On définit

- $A + B = (a_{ij} + b_{ij})$ , et
- $\lambda \cdot A = (\lambda a_{ij})$ .

On peut vérifier que  $\mathbb{M}_{n \times m}(K)$  muni de ces opérations est un  $K$ -espace vectoriel.

**Exemple 4.1.8** (Espace des solutions d'un système linéaire). Soit  $K$  un corps et  $A = (a_{ij}) \in \mathbb{M}_{n \times m}(K)$ . Considérez le système de  $n$  équations dans les variables  $x_1, \dots, x_m$  :

$$(*) \begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_m = 0 \\ \qquad \qquad \qquad \vdots \qquad \qquad \qquad \vdots \qquad \qquad \qquad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nm}x_m = 0 \end{cases}$$

On dit que  $(v_1, \dots, v_m) \in K^m$  est une solution du système si pour tout  $1 \leq i \leq n$  on a que

$$\sum_{j=1}^m a_{ij}v_j = a_{i1}v_1 + \dots + a_{im}v_m = 0.$$

Les restrictions des deux lois  $+$  et  $\cdot$  (sur  $K^m$ ) au sous-ensemble

$$W_A := \{(v_1, \dots, v_m) \in K^m \mid (v_1, \dots, v_m) \text{ est solution de } (*)\}$$

font de  $W_A$  un  $K$ -espace vectoriel. Autrement dit,  $W_A \subset K^m$  est un sous-espace vectoriel.

AZ: On peut prouver que le choix d'une matrice  $A \in \mathbb{M}_{n \times m}$  comme dans le dernier exemple définit un morphisme de groupes :

$$\begin{aligned} \varphi_A : (\mathbb{M}_{m \times 1}(K), +) &\rightarrow (\mathbb{M}_{n \times 1}(K), +) \\ \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} &\mapsto \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}. \end{aligned}$$

En utilisant ce langage, nous avons que  $W_A = \ker(\varphi_A)$ .

### 4.1.3 Sous-espaces vectoriels

**Définition 4.1.9.** Soit  $V$  un  $K$ -espace vectoriel. Une partie  $W \subset V$  s'appelle un **sous-espace vectoriel** (ou simplement sous-espace) de  $V$  si les restrictions des deux lois  $+$  et  $\cdot$  à  $W$  font de  $W$  un  $K$ -espace vectoriel. On écrit  $W \leq V$ .

La proposition suivante nous dit qu'il faut et qu'il suffit de vérifier une seule condition pour assurer qu'une partie non vide de  $V$  est un sous-espace.

**Proposition 4.1.10.** Soient  $V$  un  $K$ -espace vectoriel et  $\emptyset \neq W \subset V$ . Alors  $W$  est un sous-espace de  $V$  si et seulement si pour tout  $\lambda \in K$  et pour tous  $u, v \in W$  on a que  $\lambda u + v \in W$ .

*Démonstration.* Tout d'abord, c'est clair que si  $\emptyset \neq W \subset V$  est un sous-espace,  $\lambda \in K$ , et  $u, v \in W$ , alors  $\lambda u + v \in W$ .

À l'inverse, comme  $W$  est non vide, il existe  $w \in W$  et en prenant  $\lambda = -1 \in K$  on trouve que  $(-1) \cdot w + w = -w + w = 0_V \in W$ . Donc,  $W$  possède le vecteur nul. Mais alors il contiendra aussi des inverses. Comme  $0_V \in W$  en prenant  $\lambda = -1 \in K$  encore une fois on déduit que

$$w \in W \Rightarrow -w = (-1) \cdot w + 0_V \in W.$$

Nous pouvons également montrer que  $W$  est stable par  $+$  et par  $\cdot$  :

- $u, v \in W \Rightarrow 1 \cdot u + v = u + v \in W$  (prenez  $\lambda = 1$ )
- $\lambda \in K, u \in W \Rightarrow \lambda \cdot u + 0_V = \lambda \cdot u \in W$  (prenez  $v = 0_V$ ).

Et enfin, les propriétés restantes sont vérifiées car elles étaient déjà dans  $V$ .  $\square$

**Exemple 4.1.11** (Sous-espace engendré). Soit  $V$  un  $K$ -espace vectoriel et soient  $v_1, \dots, v_k \in V$ . Posons

$$\text{Vect}(v_1, \dots, v_k) := \{\lambda_1 \cdot v_1 + \dots + \lambda_k \cdot v_k \mid \lambda_i \in K \text{ pour tous } 1 \leq i \leq k\}.$$

On peut vérifier que  $\text{Vect}(v_1, \dots, v_k)$  est un sous-espace de  $V$ , appelé le sous-espace de  $V$  engendré par  $v_1, \dots, v_k$ . Cet espace est le plus petit sous-espace vectoriel de  $V$  contenant le sous-ensemble  $\{v_1, \dots, v_n\}$ .

**Exemple 4.1.12** (Matrices symétriques). Une matrice carrée  $A = (a_{ij}) \in \mathbb{M}_{n \times n}(K)$  est dite symétrique si  $a_{ij} = a_{ji}$  pour chaque  $i$  et  $j$ . L'ensemble de toutes les matrices symétriques forme un sous-espace de  $\mathbb{M}_{n \times n}(K)$ .

**Exemple 4.1.13.** Toute droite du plan passant par l'origine forme un sous-espace vectoriel de  $\mathbb{R}^2$ . De même, tout plan passant par l'origine dans  $\mathbb{R}^3$  et ainsi de suite.

#### 4.1.4 Pour réfléchir chez vous

**Exercice 4.1.14.** Soit  $\mathcal{P} := \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f(x) = f(-x) \forall x \in \mathbb{R}\}$ . Montrer que  $\mathcal{P}$  est un sous-espace de  $\mathcal{F}(\mathbb{R}, \mathbb{R})$ .

**Exercice 4.1.15.** Les ensembles suivants sont-ils des sous-espaces vectoriels de  $\mathbb{R}^3$ ? Vous devez justifier vos réponses.

- (a)  $W_1 = \{(x, y, z) \in \mathbb{R}^3 \mid x + 2y - 5z = 0\}$
- (b)  $W_2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 = 0\}$
- (c)  $W_3 = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 1\}$

## Cours 7

---

### 5.1 De nouveaux sous-espaces à partir d'autres sous-espaces

Si  $V$  est un  $K$ -espace vectoriel et  $U, W \leq V$  sont des sous-espaces, alors leur somme et leur intersection sont également des sous-espaces.

**Proposition 5.1.1.** Soient  $V$  un espace vectoriel sur un corps  $K$  et  $U, W \subset V$  deux sous-espaces. Alors

- (i)  $U \cap W$  est un sous-espace vectoriel de  $V$  et,
- (ii) également,  $U + W := \{u + w \mid u \in U, w \in W\}$  est un sous-espace vectoriel de  $V$ .
  - Dans le cas où  $U \cap W = \{0_V\}$  on parle de la **somme directe** de  $U$  et  $W$  et on écrit  $U \oplus W$ .

*Démonstration.*

- (i) Tout d'abord on observe que  $U \cap W \neq \emptyset$  car  $0_V \in U$  et  $0_V \in W$ . Il suffit donc de montrer que

$$\lambda \in K, a, b \in U \cap W \Rightarrow \lambda \cdot a + b \in U \cap W.$$

Prenons  $\lambda \in K$  et  $a, b \in U \cap W$ . Comme  $a, b \in U$  et  $U$  est un sous-espace vectoriel, nous savons que (Proposition 4.1.10, cours 6)  $\lambda \cdot a + b \in U$ . Similairement, comme  $a, b \in W$  et  $W$  est un sous-espace vectoriel, on a que  $\lambda \cdot a + b \in W$ . Mais alors, ça implique que  $\lambda \cdot a + b \in U \cap W$  et, en utilisant Proposition 4.1.10 (cours 6) encore une fois, on déduit que  $U \cap W$  est un sous-espace vectoriel.

- (ii) Nous observons également que  $U + W \neq \emptyset$  car  $0_V \in U \cap W$  et donc  $0_V = 0_V + 0_V \in U + W$ . Or, si  $\lambda \in K$  et  $a, b \in U + W$  alors il existe  $u_1, u_2 \in U$  et  $w_1, w_2 \in W$  tels que

$$\begin{aligned} \lambda \cdot a + b &= \lambda \cdot \underbrace{(u_1 + w_1)}_{=a} + \underbrace{(u_2 + w_2)}_{=b} \\ &= (\lambda \cdot u_1 + u_2) + (\lambda \cdot w_1 + w_2), \end{aligned}$$

mais comme  $U$  et  $W$  sont des sous-espaces vectoriels, on a que  $\lambda \cdot u_1 + u_2 \in U$  et que  $\lambda \cdot w_1 + w_2 \in W$ , et donc ce qui précède signifie que  $\lambda \cdot a + b \in U + W$ . □

**Exemple 5.1.2.** Soient  $V$  un  $K$ -espace vectoriel et  $X \subset V$  une partie de  $V$ . Considérons l'intersection de tous les sous-espaces de  $V$  qui contiennent le sous-ensemble  $X$ . On pose  $\mathcal{S} := \{U \leq V \mid X \subset U\}$  et on considère :

$$\text{Vect}(X) := \bigcap_{U \in \mathcal{S}} U.$$

On vérifie que  $\text{Vect}(X)$  est bien un sous-espace de  $V$ , appelé le sous-espace engendré par la partie  $X$ . En fait, on peut montrer que  $\text{Vect}(X)$  est l'ensemble de toutes les combinaisons linéaires (Définition 5.2.1 (D1) ci-dessous) de vecteurs de  $X$ .

AZ: ▲ Notez que  $\text{Vect}(\emptyset) = \{0\}$ .

**Exemple 5.1.3.** Soient  $K$  un corps et  $V$  l'espace de toutes les matrices  $2 \times 2$  à coefficients dans  $K$ . Soient  $U = \left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \right\} \leq V$  et  $W = \left\{ \begin{pmatrix} d & 0 \\ 0 & e \end{pmatrix} \right\} \leq V$ . Alors,  $U \cap W = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \right\} \leq V$  et  $U + W = V$ .

**Exemple 5.1.4.** Soit  $V = \mathcal{F}(\mathbb{R}, \mathbb{R})$  et considère les sous-espaces  $V_p = \{f \in V \mid f(x) = f(-x)\}$  (fonctions paires) et  $V_i = \{f \in V \mid f(x) = -f(-x)\}$  (fonctions impaires). Alors,  $V = V_p \oplus V_i$ .

On peut bien sûr généraliser aussi la définition de somme et de somme directe au cas de plus de deux sous-espaces. Plus généralement, la définition est la suivante.

**Définition 5.1.5.** Soient  $V$  un  $K$ -espace vectoriel et  $W_1, \dots, W_k$  des sous-espaces vectoriels de  $V$ .

- (i) On dénote par  $W_1 + \dots + W_k$  l'ensemble  $\{w_1 + \dots + w_k \mid w_i \in W_i, \forall 1 \leq i \leq k\}$ .
- (ii) On dit qu'un sous-espace  $U$  de  $V$  est la somme directe de  $W_1, \dots, W_k$  et on écrit  $U = W_1 \oplus \dots \oplus W_k$  si
  - (ii-a)  $U = W_1 + \dots + W_k$ , et
  - (ii-b)  $W_i \cap \left( \sum_{j \neq i} W_j \right) = \{0_V\}$  pour tout  $1 \leq i \leq k$ .

Le résultat suivant caractérise les sommes directes.

**Théorème 5.1.6.** Soient  $W_1, \dots, W_k, U$  des sous-espaces vectoriels d'un  $K$ -espace vectoriel  $V$  avec  $W_i \subset U$  pour tout  $1 \leq i \leq k$ . Les conditions suivantes sont équivalentes :

- (i)  $U = W_1 \oplus \dots \oplus W_k$ .
- (ii) Chaque vecteur  $u \in U$  peut être écrit de façon unique comme  $u = w_1 + \dots + w_k$ , avec  $w_i \in W_i$  pour tout  $1 \leq i \leq k$ .

*Démonstration.*

- (i)  $\Rightarrow$  (ii) Par définition, chaque  $u \in U$  s'écrit comme  $u = w_1 + \dots + w_k$ , il faut vérifier l'unicité d'une telle décomposition. Supposons qu'on peut écrire

$$u = w_1 + \dots + w_k = \tilde{w}_1 + \dots + \tilde{w}_k,$$

pour certains  $w_i, \tilde{w}_i \in W_i, 1 \leq i \leq k$ . Alors, pour chaque  $i$  on a que

$$w_i - \tilde{w}_i = \sum_{j \neq i} (\tilde{w}_j - w_j).$$

Or, ce vecteur appartient à la fois à  $W_i$  et à la somme  $\sum_{j \neq i} W_j$ , donc à l'intersection

$W_i \cap \left( \sum_{j \neq i} W_j \right)$ . On en déduit que  $w_i - \tilde{w}_i = 0_V$  pour tout  $1 \leq i \leq k$  et que l'écriture est unique.

- (ii)  $\Rightarrow$  (i) Par hypothèse,  $U \subset W_1 + \dots + W_k$ . De plus, comme  $W_i \subset U$  pour tout  $i$  et  $U \leq V$  on a aussi que  $W_1 + \dots + W_k \subset U$ . Montrons que  $W_i \cap \left( \sum_{j \neq i} W_j \right) = \{0_V\}$  pour tout

$1 \leq i \leq k$ . Fixons  $1 \leq i \leq k$  quelconque et prenons  $v \in W_i \cap \left( \sum_{j \neq i} W_j \right) \subset W_1 + \dots + W_n$ .

Alors, d'une part

$$v = 0 + \dots + 0 + \underbrace{v}_{\in W_i} + 0 + \dots + 0,$$

et d'autre part

$$v = w_1 + \dots + w_{i-1} + 0 + w_{i+1} + \dots + w_k,$$

pour certains  $w_j \in W_j$ . Comme l'écriture est unique, on déduit que  $v = 0$ .

□

## 5.2 (In)dépendance linéaire

On fixe un corps  $K$  et un  $K$ -espace vectoriel  $V$ .

### Définition 5.2.1.

(D1) Soient  $v_1, \dots, v_k \in V$  des vecteurs. Une **combinaison linéaire** de  $v_1, \dots, v_k$  est un vecteur  $v \in V$  qui peut être écrit comme  $v = \sum_{i=1}^k \lambda_i \cdot v_i = \lambda_1 \cdot v_1 + \dots + \lambda_k \cdot v_k$  pour certains scalaires  $\lambda_i \in K$ .

(D2)  $X \subset V$  s'appelle un système générateur, ou une **partie génératrice** de  $V$  si  $V = \text{Vect}(X)$  (voir l'Exemple 5.1.2).

Autrement dit,  $\emptyset \neq X \subset V$  est une partie génératrice de  $V$  si et seulement si tout  $v \in V$  est une combinaison linéaire de vecteurs dans  $X$ .

(D3) Soient  $v_1, \dots, v_k \in V$ . On dit que  $v_1, \dots, v_k$  sont liés, ou **linéairement dépendants**, s'il existe  $\lambda_1, \dots, \lambda_k \in K$ , non tous nuls, tels que

$$\lambda_1 \cdot v_1 + \dots + \lambda_k \cdot v_k = 0_V.$$

Cela signifie donc que l'un des  $v_i$  est une combinaison linéaire de toutes les autres  $v_j$ ,  $j \neq i$ .

(D4) Par contre, si  $v_1, \dots, v_k$  sont distincts et on ne peut pas trouver des scalaires  $\lambda_i$  comme ci-dessus, on dit que ces vecteurs sont libres, ou **linéairement indépendants**.

Autrement dit,  $v_1, \dots, v_k$  sont libres s'ils ne sont pas liés. Ce qui signifie que toute égalité

$$\lambda_1 \cdot v_1 + \dots + \lambda_k \cdot v_k = 0_V$$

implique que  $\lambda_i = 0$  pour tout  $i$ .

(D5) Une partie  $X \subset V$  est dite liée, ou linéairement dépendante, s'il existe  $v_1, \dots, v_k \in X$  distincts qui sont liés. Sinon, la partie est dite libre ou linéairement indépendante.

AZ: Je vous propose de regarder la vidéo « Linear combinations, span, and basis vectors » sur la chaîne [3Blue1Brown](#).

Voici quelques conséquences directes de ces définitions.

- Tout ensemble contenant un ensemble linéairement dépendant est linéairement dépendant.
- Tout sous-ensemble d'un ensemble linéairement indépendant est linéairement indépendant.
- Tout ensemble contenant le vecteur nul est linéairement dépendant car  $1_K \cdot 0_V = 0_V$ . En particulier, chaque liste de vecteurs dans  $V$  contenant le vecteur nul est linéairement dépendante.
- Une partie  $X \subset V$  est linéairement indépendante si et seulement si chaque sous-ensemble fini de  $X$  est linéairement indépendant, c'est-à-dire si et seulement si pour tout vecteur distinct  $v_1, \dots, v_k$ , de  $X$ ,  $\lambda_1 \cdot v_1 + \dots + \lambda_k \cdot v_k = 0_V$  implique que chaque  $\lambda_i = 0$ .
- Des vecteurs  $v_1, \dots, v_k$  sont linéairement indépendants si et seulement si chaque vecteur de  $\text{Vect}(v_1, \dots, v_k)$  n'a qu'une seule représentation sous forme de combinaison linéaire de  $v_1, \dots, v_k$ .
- La partie vide est donc linéairement indépendante.

### Exemple 5.2.2.

- Pour chaque  $v \in V$ , le sous-ensemble  $\{v\}$  est linéairement indépendant si et seulement si le vecteur  $v$  n'est pas nul.
- Deux vecteurs distincts dans un espace vectoriel sont linéairement indépendants si et seulement si aucun des deux vecteurs n'est un multiple scalaire de l'autre.

### 5.2.1 Quelques exemples en plus de parties génératrices et de parties libres

- Dans l'espace vectoriel  $K[x]$ , l'ensemble  $\{1, x, x^2, x^3, \dots\}$  est un système générateur.
- Dans l'espace  $K^3$ ,  $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$  est une partie génératrice .
- Dans l'espace  $\mathbb{R}^2$ ,  $\{(1, -2), (3, 2), (1, 5), (-4, 1)\}$  est un système générateur.
- La partie vide  $\emptyset \subset V$  est libre.
- Dans  $\mathcal{F}(\mathbb{R}, \mathbb{R})$ , l'ensemble  $\{\sin x, \cos x\}$  est un ensemble de vecteurs linéairement indépendants.
- Dans  $\mathbb{R}^2$ , les vecteurs  $(1, -2)$  et  $(3, 2)$  sont libres et le sous-ensemble  $\{(1, -2), (3, 2)\}$  est donc libre aussi.

- $\left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right\}$  est un sous-ensemble de  $\mathbb{M}_{n \times 1}(K)$  qui est linéairement indépendant.

Ici 1 désigne  $1_K$  et 0 désigne  $0_K$

### 5.2.2 Pour réfléchir chez vous

- À quoi ressemblent les vecteurs linéairement dépendants dans  $\mathbb{R}^2$ ? Et dans  $\mathbb{R}^3$ ?

- Quelle est la plus petite cardinalité d'une partie génératrice de  $\mathbb{R}^4$  ?

## Cours 8

---

### 6.1 Base et dimension

Partout,  $K$  désignera un corps et  $V$  un  $K$ -espace vectoriel.

**Définition 6.1.1.** Une partie  $X \subset V$  s'appelle une **base** si les deux conditions suivantes sont satisfaites.

- (B1)  $X$  est une partie génératrice de  $V$ , et  
 (B2)  $X$  est une partie linéairement indépendante.

L'espace vectoriel  $V$  est dit de dimension finie si  $V$  possède un système générateur fini, ou de manière équivalente, si  $V$  possède une base finie (voir Théorème 6.1.5 ci-dessous).

AZ: **▲** Dans ce cours, on va admettre sans preuve que tout  $K$ -espace vectoriel possède une base. Si  $V = \{0\}$  la base est la partie  $\emptyset$ . Si  $V \neq \{0\}$ , il existe un sous-ensemble propre  $X \subset V$  qui est linéairement indépendant (par exemple, chaque sous-ensemble de la forme  $\{v\}$  avec  $v \neq 0$ ). On peut montrer qu'il existe un sous-ensemble maximal linéairement indépendant de  $V$  qui contient  $X$  et qu'en plus cette partie maximale sera forcément une base (voir aussi Lemme 6.1.8 ci-dessous).

**Proposition 6.1.2.** *Supposons  $V \neq \{0\}$ . Une partie  $X \subset V$  est une base de  $V$  si et seulement si pour tout  $v \in V \setminus \{0_V\}$  il existe un nombre fini de vecteurs  $v_1, \dots, v_n$  et des scalaires  $\lambda_1, \dots, \lambda_n \in K^\times$ , uniquement déterminés, tels que  $v = \lambda_1 \cdot v_1 + \dots + \lambda_n \cdot v_n$ .*

AZ: **▲** Ici, je suppose que des vecteurs  $v_1, \dots, v_n$  sont distincts.

*Démonstration.*

- ( $\Rightarrow$ ) Si  $X$  est une base, par définition  $X$  est une partie génératrice et donc tout  $v \in V$  est une combinaison linéaire de vecteurs dans  $X$ . Il suffit de vérifier l'unicité de l'expression. Supposons

$$0_V \neq v = \alpha_1 \cdot u_1 + \dots + \alpha_k \cdot u_k = \beta_1 \cdot w_1 + \dots + \beta_m \cdot w_m,$$

pour certains scalaires  $\alpha_i, \beta_j \in K$  et certains vecteurs  $u_i, w_j$ . En rajoutant des termes à coefficients nuls, on peut supposer que

$$v = \gamma_1 \cdot v_1 + \dots + \gamma_n \cdot v_n = \lambda_1 \cdot v_1 + \dots + \lambda_n \cdot v_n$$

Alors,  $\sum_{k=1}^n (\gamma_k - \lambda_k) \cdot v_k = 0_V$  et comme  $X$  est libre,  $\{v_1, \dots, v_n\}$  est libre aussi, et on déduit que  $\gamma_k = \lambda_k$  pour tout  $1 \leq k \leq n$ . Par conséquent, les  $\alpha$ s sont égaux aux  $\beta$ s et les  $u$ s sont égaux aux  $w$ s.

( $\Leftarrow$ ) Tout d'abord, notez que  $X$  est une partie génératrice et comme  $V \neq \{0\}$ ,  $X \neq \emptyset$ . Donc, il existe  $0_V \neq v \in X$ . En plus,  $0_V \notin X$  car sinon on a  $v = 1 \cdot v = 1 \cdot v + 1 \cdot 0_V$ , ce qui contredit l'unicité de l'expression. On doit juste montrer que  $X$  est libre.

Supposons le contraire. Il existe donc une partie finie de vecteurs distincts  $\{v_1, \dots, v_n\} \subset X$  qui n'est pas libre. Donc, il existe aussi des scalaires  $\lambda_1, \dots, \lambda_n$  non tous nuls tels que  $\lambda_1 \cdot v_1 + \dots + \lambda_n \cdot v_n = 0_V$ . Sans perte de généralité, nous pouvons supposer que  $\lambda_1 \neq 0$  et on peut écrire

$$V \ni -\lambda_1 \cdot v_1 = \underbrace{-\lambda_1}_{\in K^\times} \cdot \underbrace{v_1}_{\in X} = \lambda_2 \cdot v_2 + \dots + \lambda_n \cdot v_n.$$

Ainsi, soit  $-\lambda_1 \cdot v_1 = 0_V$ , soit l'un des autres scalaires est également différent de zéro. Par l'unicité de l'écriture, on déduit que le vecteur  $-\lambda_1 \cdot v_1$  doit être le vecteur nul. Mais cela implique que  $v_1 = 0_V$  car  $\lambda_1 \neq 0$ , ce qui est contradictoire puisque  $0_V \notin X$ . □

**Corollaire 6.1.3.** *Supposons que  $\{v_1, \dots, v_n\}$  soit une base de  $V$ . Alors  $V = \text{Vect}(v_1) \oplus \dots \oplus \text{Vect}(v_n)$ .*

### 6.1.1 Quelques résultats en plus

**Lemme 6.1.4.** *Supposons que  $v_1, \dots, v_m$  soient linéairement dépendants. Alors, il existe  $k \in \{1, \dots, m\}$  tel que  $v_k \in \text{Vect}(v_1, \dots, v_{k-1})$ . De plus, pour tel  $k$ , si le  $k$ -ième vecteur  $v_k$  est supprimé de  $\{v_1, \dots, v_m\}$ , alors le sous-espace engendré par les vecteurs restants est égal à  $\text{Vect}(v_1, \dots, v_m)$ .*

*Démonstration.* Comme  $v_1, \dots, v_m$  sont linéairement dépendants, il existe des scalaires  $\alpha_1, \dots, \alpha_m \in K$ , non tous nuls, tels que  $\alpha_1 \cdot v_1 + \dots + \alpha_m \cdot v_m = 0$ . Soit  $k$  le plus grand élément de  $\{1, \dots, m\}$  tel que  $\alpha_k \neq 0$ . Alors  $v_k = \sum_{i=1}^{k-1} \beta_i \cdot v_i$ , où  $\beta_i := -\alpha_k^{-1} \alpha_i$  pour tout  $1 \leq i \leq k-1$ , ce qui prouve que  $v_k \in \text{Vect}(v_1, \dots, v_{k-1})$ .

Maintenant, supposons que  $v \in \text{Vect}(v_1, \dots, v_m)$ . Alors il existe  $\gamma_1, \dots, \gamma_m \in K$  tels que

$$v = \gamma_1 \cdot v_1 + \dots + \gamma_m \cdot v_m.$$

Dans cette équation, on peut remplacer  $v_k$  par  $\sum_{i=1}^{k-1} \beta_i \cdot v_i$ , ce qui montre que  $v$  est dans le sous-espace engendré par les vecteurs  $v_j$  avec  $j \neq k$ . □

**Théorème 6.1.5.** *Si  $V \neq \{0\}$  est engendré par une partie finie  $\{v_1, \dots, v_n\}$ , c.-à-d., s'il existe un nombre fini ( $> 0$ ) de vecteurs  $v_1, \dots, v_n \in V$  tels que  $V = \text{Vect}(v_1, \dots, v_n)$ , alors toute partie  $X \subset V$  linéairement indépendante est finie et ne contient pas plus de  $n$  éléments. (c.-à-d.,  $|X| \leq n$ ).*

*Preuve 1.* Soient  $w_1, \dots, w_k \in V$  des vecteurs linéairement indépendants quelconques. Il suffit de montrer que  $k \leq n$ . Comme  $w_1 \in \text{Vect}(v_1, \dots, v_n) = V$ , les vecteurs  $w_1, v_1, \dots, v_n$  sont linéairement dépendants. En utilisant le Lemme 6.1.4, on peut supposer, sans perte de généralité, que  $V = \text{Vect}(w_1, v_2, \dots, v_n)$ , c.-à-d. qu'on remplace  $v_1$  par  $w_1$ . Notez que  $w_1 \neq 0$ ! Maintenant, comme  $w_2 \in \text{Vect}(w_1, v_2, \dots, v_n) = V$ , les vecteurs  $w_1, w_2, v_2, \dots, v_n$  sont linéairement dépendants; et comme  $w_2 \notin \text{Vect}(w_1)$ , en utilisant le Lemme 6.1.4 encore une fois, on peut supposer que  $V = \text{Vect}(w_1, w_2, v_3, \dots, v_n)$ . En procédant ainsi, après l'étape  $k$  (éventuellement après avoir réorganisé les vecteurs) nous aurons remplacé  $v_1, \dots, v_k$  par  $w_1, \dots, w_k$ . À chaque étape, le Lemme 6.1.4 implique qu'il y a un certain  $v_j$  à supprimer. Il y a donc au moins autant de  $v$ s que de  $w$ s.  $\square$

*Preuve 2.* Pour démontrer le théorème, il suffit de montrer que tout sous-ensemble  $X$  de  $V$  contenant plus de  $n$  vecteurs est linéairement dépendant. Soit  $X$  un tel ensemble. Dans  $X$ , il existe donc des vecteurs distincts  $w_1, \dots, w_k$  avec  $k > n$ ; et comme  $V = \text{Vect}(v_1, \dots, v_n)$ , il existe aussi des scalaires  $\lambda_{ij} \in K$  tels que

$$w_j = \sum_{i=1}^n \lambda_{ij} v_i.$$

Prenons maintenant  $k$  scalaires  $\alpha_1, \dots, \alpha_k$  quelconques. Alors

$$\begin{aligned} \alpha_1 \cdot w_1 + \dots + \alpha_k \cdot w_k &= \sum_{j=1}^k \alpha_j \cdot w_j = \sum_{j=1}^k \left( \alpha_j \cdot \left( \sum_{i=1}^n \lambda_{ij} v_i \right) \right) \\ &= \sum_{i=1}^n \left( \sum_{j=1}^k \lambda_{ij} \alpha_j \right) \cdot v_i \end{aligned}$$

et il suffit de montrer que nous pouvons toujours trouver des scalaires  $\alpha_1, \dots, \alpha_k$ , non tous nuls, tels que  $\left( \sum_{j=1}^k \lambda_{ij} \alpha_j \right) = 0$  pour tout  $1 \leq i \leq n$ . Ceci est vrai car tout système homogène de  $n$  équations linéaires avec  $k > n$  inconnues a une solution non triviale.  $\square$

**Corollaire 6.1.6.** *Si  $V$  est de dimension finie, deux bases quelconques de  $V$  ont le même nombre (fini) d'éléments.*

Si  $V$  est de dimension finie, on peut donc parler de sa dimension. Si  $V$  possède une base avec  $n$  éléments on écrit  $\dim(V) = n$ .

**Corollaire 6.1.7.** *Si  $V$  est de dimension finie et  $\dim(V) = n$ , alors*

- (i) *chaque sous-ensemble de  $V$  contenant plus de  $n$  vecteurs est linéairement dépendant;*
- (ii) *aucun sous-ensemble de  $V$  contenant moins de  $n$  vecteurs ne peut engendrer  $V$ .*

Nous admettrons que le sous-espace nul a une dimension nulle.

**Lemme 6.1.8.** *Soit  $X \subset V$  un sous-ensemble linéairement indépendant. Supposons que  $w$  soit un vecteur de  $V$  qui ne soit pas dans le sous-espace engendré par  $X$ . Alors, l'ensemble  $X \cup \{w\}$  obtenu en adjoignant  $w$  à  $X$  est linéairement indépendant.*

*Démonstration.* Considérons  $v_1, \dots, v_n \in X$  distincts. Si

$$\alpha_1 \cdot v_1 + \dots + \alpha_n \cdot v_n + \beta \cdot w = 0,$$

alors  $\beta = 0$ . Sinon,

$$w = \sum_{i=1}^n (-\beta^{-1} \alpha_i) \cdot v_i \Rightarrow w \in \text{Vect}(v_1, \dots, v_n) \subset \text{Vect}(X).$$

Ainsi  $\alpha_1 \cdot v_1 + \dots + \alpha_n \cdot v_n = 0$ , et puisque  $X$  est une partie linéairement indépendante, chaque  $\alpha_i = 0$ . Par conséquent, puisque les vecteurs  $v_i$  étaient arbitraires, cela signifie que nous ne pouvons pas trouver un nombre fini de vecteurs (distincts) dans  $X \cup \{w\}$  qui soient linéairement dépendants. Par définition,  $X \cup \{w\}$  est donc linéairement indépendant.  $\square$

**Théorème 6.1.9** (de la base incomplète). *Supposons que  $V$  soit de dimension finie. Soit  $L \subset V$  une partie libre (= linéairement indépendante). Alors,  $L$  peut être complété en une base de  $V$ . En plus, si  $|L| = \dim V$ , alors  $L$  est une base.*

*Démonstration.* Nous complétons  $L$  en une base de  $V$  comme suit. Si  $V = \text{Vect}(L)$ , il n'y a rien à faire. Sinon, il existe  $w \in V \setminus \text{Vect}(L)$ . Maintenant, le Lemme 6.1.8 nous dit que  $L \cup \{w\}$  est linéairement indépendant. Si  $V = \text{Vect}(L \cup \{w\})$ , on s'arrête. Sinon on peut procéder de cette façon (en pas plus de  $\dim(V)$  étapes) jusqu'à obtenir une base pour  $V$ . Le processus doit nécessairement se terminer par le Théorème 6.1.5, voir aussi Corollaire 6.1.7.  $\square$

Notez que ceci est vrai si et seulement si  $|L| = \dim(V)$ , voir Corollaire 6.1.7

**Corollaire 6.1.10.** *Soit  $W \leq V$  un sous-espace propre. Alors,  $W$  est de dimension finie et  $\dim W < \dim V$ . En plus, toute base de  $W$  peut être complétée en une base de  $V$ . En particulier, il existe  $U \leq V$  tel que  $V = U \oplus W$  et  $\dim V = \dim U + \dim W$ .*

AZ: En général,  $\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W)$ .

## 6.2 Quelques exemples

**Exemple 6.2.1.** Dans l'espace  $V = K^n$  on peut considérer des vecteurs  $e_1, \dots, e_n$  défini par

$$e_1 := (1, 0, 0, \dots, 0)$$

$$e_2 := (0, 1, 0, \dots, 0)$$

$$\vdots$$

$$e_n := (0, 0, 0, \dots, 1).$$

La partie  $\{e_1, \dots, e_n\} \subset K^n$  est une base, appelée base canonique.

**Exemple 6.2.2.** Les parties  $\{(1, 2), (3, 5)\}$  et  $\{(7, 5), (-4, 9)\}$  sont des bases de  $\mathbb{R}^2$ .

**Exemple 6.2.3.** La partie  $\{(1, -1, 0), (1, 0, -1)\}$  est une base de

$$V = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\} \leq \mathbb{R}^3.$$

**Exemple 6.2.4.** Soit  $A \in \mathbb{M}_{n \times n}(K)$  une matrice inversible. Alors, les colonnes de la matrice  $A$  forment une base de  $V = \mathbb{M}_{n \times 1}$ . De manière similaire, les lignes forment une base de  $\mathbb{M}_{1 \times n}$ .

### 6.2.1 Pour réfléchir chez vous

**Exercice 6.2.5.** Montrer que les vecteurs  $v_1 = (1, 0, -1)$ ,  $v_2 = (1, 2, 1)$  et  $v_3 = (0, -3, 2)$  forment une base de  $\mathbb{R}^3$  et exprimer chacun des vecteurs dans la base canonique  $\{e_1, e_2, e_3\}$  comme une combinaison linéaire de  $v_1, v_2$  et  $v_3$ .

**Exercice 6.2.6.** Trouvez trois vecteurs dans  $\mathbb{R}^3$  qui sont linéairement dépendants et tels que deux d'entre eux, n'importe lesquels, soient linéairement indépendants.

**Exercice 6.2.7.** Soit  $V = \mathbb{M}_{2 \times 2}(K)$  et considérons des sous-espaces  $U = \left\{ \begin{pmatrix} a & -a \\ b & c \end{pmatrix} \right\} \leq V$  et  $W = \left\{ \begin{pmatrix} d & e \\ -d & f \end{pmatrix} \right\} \leq V$ . Trouver les dimensions de  $U$  et de  $W$  et des sous-espaces  $U + W$  et  $U \cap W$ .

**Exercice 6.2.8.**

- (i) Soit  $U = \{(a_1, a_2, a_3, a_4, a_5) \in \mathbb{R}^5 \mid a_1 = 3a_2 \text{ et } a_3 = 7a_4\} \leq \mathbb{R}^5$ . Trouver une base de  $U$ .
- (ii) Complétez la base de (i) en une base de  $\mathbb{R}^5$ .
- (iii) Trouver un sous-espace  $W \leq \mathbb{R}^5$  tel que  $\mathbb{R}^5 = U \oplus W$ .

## Cours 9

---

On fixe un corps  $K$  et on considère  $V$  et  $W$  deux espaces vectoriels sur  $K$ .

### 7.1 Applications linéaires : définitions et exemples

**Définition 7.1.1.** Une application  $\varphi : V \rightarrow W$  est dite  **$K$ -linéaire** si

(L1)  $\varphi$  est un morphisme de groupes (pour l'addition), et

(L2)  $\varphi(\lambda \cdot v) = \lambda \cdot \varphi(v)$ , pour tous  $\lambda \in K$  et  $v \in V$ .

En plus,

- Une application  $K$ -linéaire de  $V$  dans  $V$  est aussi appelée un endomorphisme de  $V$ .
- Une application  $K$ -linéaire de  $V$  dans  $W$  qui est bijective s'appelle un isomorphisme de  $V$  dans  $W$  ou bien entre  $V$  et  $W$ . Et s'il existe un isomorphisme,  $\varphi : V \rightarrow W$  on dit que les espaces  $V$  et  $W$  sont isomorphes.
- S'il est clair que nous parlons du corps  $K$ , on dit simplement une application linéaire.

Donc  $\varphi : V \rightarrow W$  est une application  $K$ -linéaire si et seulement si

(L1)  $\varphi(u + v) = \varphi(u) + \varphi(v)$ , pour tous  $u, v \in V$ , et

(L2)  $\varphi(\lambda \cdot v) = \lambda \cdot \varphi(v)$ , pour tous  $\lambda \in K$  et  $v \in V$ .

On observe que ces deux conditions se résument en une seule :

$\varphi : V \rightarrow W$  est  $K$ -linéaire  $\iff \varphi(\lambda \cdot u + v) = \lambda \cdot \varphi(u) + \varphi(v)$ , pour tous  $\lambda \in K$  et  $u, v \in V$ .

AZ: Notez qu'une transformation linéaire (non nulle) de  $\mathbb{R}$  dans  $\mathbb{R}$ , selon la définition ci-dessus, est tout simplement une fonction de  $\mathbb{R}$  dans  $\mathbb{R}$  dont le graphe est une droite passant par l'origine.

On a les propriétés suivantes :

**Proposition 7.1.2.** Soit  $\varphi; V \rightarrow W$  une application  $K$ -linéaire.

(P1) On  $\varphi(0_V) = 0_W$ , et

(P2)  $\varphi(\lambda_1 \cdot v_1 + \dots + \lambda_n \cdot v_n) = \lambda_1 \cdot \varphi(v_1) + \dots + \lambda_n \cdot \varphi(v_n)$ .

En particulier, comme chaque élément de  $V$  s'écrit de manière unique comme une combinaison linéaire des éléments d'une base de  $V$ , il suffit de connaître les valeurs de  $\varphi$  sur une base pour connaître l'application  $\varphi$ . En fait, on peut prouver le résultat suivant.

**Théorème 7.1.3.** Supposons que  $V$  soit un espace vectoriel de dimension finie sur le corps  $K$ . Soit  $\mathcal{B} = \{v_1, \dots, v_n\}$  une base ordonnée de  $V$ . Soit  $W$  un espace vectoriel sur le même corps  $K$  et soient  $w_1, \dots, w_n$  des vecteurs quelconques dans  $W$ . Alors, il existe exactement une application linéaire  $\varphi : V \rightarrow W$  telle que  $\varphi(v_i) = w_i$  pour tous  $1 \leq i \leq n$ .

*Démonstration.* Nous prouvons d'abord l'existence de l'application  $\varphi$ . Étant donné  $v \in V$ , il existe des scalaires  $\lambda_1, \dots, \lambda_n$ , déterminés de manière unique, tels que

$$v = \lambda_1 \cdot v_1 + \dots + \lambda_n \cdot v_n$$

Pour ce vecteur on peut donc définir  $\varphi(v) = \lambda_1 \cdot w_1 + \dots + \lambda_n \cdot w_n$ . Comme  $v$  était arbitraire, nous obtenons ainsi une fonction  $\varphi : V \rightarrow W$  qui est bien définie. Par définition,  $\varphi(v_i) = w_i$  pour tous  $1 \leq i \leq n$  et on doit juste vérifier que  $\varphi$  est linéaire. Prenons des vecteurs  $u = \alpha_1 \cdot v_1 + \dots + \alpha_n \cdot v_n$  et  $v = \beta_1 \cdot v_1 + \dots + \beta_n \cdot v_n$  dans  $V$  et de scalaire  $\lambda \in K$ . Alors,

$$\lambda u + v = (\lambda \alpha_1 + \beta_1) \cdot v_1 + \dots + (\lambda \alpha_n + \beta_n) \cdot v_n$$

et par définition on a que

$$\varphi(u) = \alpha_1 \cdot w_1 + \dots + \alpha_n \cdot w_n,$$

$$\varphi(v) = \beta_1 \cdot w_1 + \dots + \beta_n \cdot w_n.$$

Donc,

$$\begin{aligned} \varphi(\lambda u + v) &= (\lambda \alpha_1 + \beta_1) \cdot w_1 + \dots + (\lambda \alpha_n + \beta_n) \cdot w_n && \text{(par définition!)} \\ &= \lambda(\alpha_1 \cdot w_1 + \dots + \alpha_n \cdot w_n) + (\beta_1 \cdot w_1 + \dots + \beta_n \cdot w_n) \\ &= \lambda \varphi(u) + \varphi(v). \end{aligned}$$

Maintenant, nous montrons l'unicité. Soit  $\psi : V \rightarrow W$  une autre application linéaire telle que  $\psi(v_i) = w_i$  pour tous  $1 \leq i \leq n$ . Alors, si  $v = \lambda_1 \cdot v_1 + \dots + \lambda_n \cdot v_n$  est un vecteur dans  $V$  quelconque, il faut nécessairement avoir

$$\begin{aligned} \psi(v) &= \psi(\lambda_1 \cdot v_1 + \dots + \lambda_n \cdot v_n) \\ &= \lambda_1 \cdot \psi(v_1) + \dots + \lambda_n \cdot \psi(v_n) \\ &= \lambda_1 \cdot w_1 + \dots + \lambda_n \cdot w_n. \end{aligned}$$

Donc,  $\psi = \varphi$ . □

### 7.1.1 Quelques exemples

AZ: Je vous propose de regarder la vidéo « Linear transformations and matrices » sur la chaîne *3Blue1Brown*.

**Exemple 7.1.4.** Si  $V$  est un espace vectoriel quelconque, la transformation identité  $\text{id}_V : V \rightarrow V$  définie par  $\text{id}_V(v) = v$  (pour tous  $v \in V$ ) est une transformation linéaire de  $V$  dans  $V$ . Également, la transformation nulle, définie par  $v \mapsto 0_V$  (pour tous  $v \in V$ ) est aussi un endomorphisme de  $V$ .

**Exemple 7.1.5.** Si  $V = K[x]$ , l'application  $D : K[x] \rightarrow K[x]$  définie par

$$f(x) = a_0 + a_1x + \dots + a_nx^n \mapsto (D(f))(x) := a_1 + 2a_2x + \dots + na_nx^{n-1}$$

est une application linéaire.

**Exemple 7.1.6.** Si  $V = K[x]$  et nous fixons  $f(x) \in K[X]$ , l'application  $\varphi_f : K[x] \rightarrow K[x]$  définie par

$$g(x) \mapsto f(x)g(x)$$

est une application linéaire.

**Exemple 7.1.7.** Considérons  $\mathbb{C}$  et  $\mathcal{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \right\} \subset \mathbb{M}_{2 \times 2}(\mathbb{R})$  comme  $\mathbb{R}$ -espaces vectoriels. Le morphisme de groupes (pour l'addition)  $\varphi : \mathbb{C} \rightarrow \mathcal{C}$  définie par  $a + b \cdot i \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$  est un isomorphisme ( $\mathbb{R}$ -linéaire). En effet,

(1)  $\varphi$  est bijective.  $\psi : \mathcal{C} \rightarrow \mathbb{C}$  définie par  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mapsto a + b \cdot i$  est l'inverse.

(2) pour tous  $\lambda \in \mathbb{R}$  et  $z = a + b \cdot i \in \mathbb{C}$  on a que

$$\varphi(\lambda \cdot z) = \varphi(\lambda a + \lambda b i) = \begin{pmatrix} \lambda a & -\lambda b \\ \lambda b & \lambda a \end{pmatrix} = \lambda \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \lambda \cdot \varphi(z)$$

**Exemple 7.1.8.** Les applications suivantes sont des isomorphismes :

$$\begin{aligned} \varphi : \mathbb{M}_{n \times 1}(K) &\rightarrow K^n \\ \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix} &\mapsto (a_{11}, \dots, a_{n1}) \end{aligned}$$

et

$$\begin{aligned} \varphi : \mathbb{M}_{1 \times n}(K) &\rightarrow K^n \\ (a_{11} \quad \dots \quad a_{1n}) &\mapsto (a_{11}, \dots, a_{1n}) \end{aligned}$$

**Exemple 7.1.9.** Soit  $A \in \mathbb{M}_{m \times n}(K)$ . L'application  $\varphi_A : \mathbb{M}_{n \times 1}(K) \rightarrow \mathbb{M}_{m \times 1}(K)$  définie par  $X \mapsto AX$  est une application linéaire.

Également, l'application  $\psi_A : \mathbb{M}_{1 \times m}(K) \rightarrow \mathbb{M}_{1 \times n}(K)$  définie par  $v \mapsto vA$  est une application linéaire.

**Exemple 7.1.10.** Soit  $\varphi : K^m \rightarrow K^n$ . Le Théorème 7.1.3 nous dit que  $\varphi$  est uniquement déterminée par des vecteurs  $v_1, \dots, v_m \in K^n$  tels que  $v_i = \varphi(e_i)$  pour tous  $1 \leq i \leq m$ . En effet, si  $u = (x_1, \dots, x_m) \in K^m$ , alors  $\varphi(u) = x_1 \cdot v_1 + \dots + x_m \cdot v_m$ . En particulier, en écrivant  $v_i = (a_{i1}, \dots, a_{in})$ , on a que

$$\varphi(x_1, \dots, x_m) = \begin{pmatrix} x_1 & \dots & x_m \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Également, en écrivant  $v_j = (b_{1j}, \dots, b_{nj})$ , on a que

$$\varphi(x_1, \dots, x_m) = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1m} \\ b_{21} & b_{22} & \dots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nm} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}.$$

**Exemple 7.1.11.** Soient  $P \in \mathbb{M}_{m \times m}(K)$  et  $Q \in \mathbb{M}_{n \times n}(K)$ . L'application

$$\varphi : \mathbb{M}_{m \times n}(K) \rightarrow \mathbb{M}_{m \times n}(K)$$

définie par  $A \mapsto PAQ$  est un endomorphisme.

**Exemple 7.1.12.** Si  $V$  est un  $K$ -espace vectoriel avec sous-espaces  $U$  et  $W$  tels que  $V = U \oplus W$ , alors la projection sur  $W$  parallèlement à  $U$  est l'application linéaire  $\pi : V \rightarrow W$  définie par  $\pi(u + w) = w$ , pour tous  $u \in U$  et  $w \in W$ . Définie comme telle, l'application est un endomorphisme, idempotent (c.-à-d.,  $\pi \circ \pi = \pi$ ), d'image  $W$  et de noyau  $U$ .

## 7.2 Opérations sur les applications linéaires

**Définition 7.2.1.** On dénote par  $\mathcal{L}(V, W)$  l'ensemble des applications  $K$ -linéaires de  $V$  dans  $W$ . On munit  $\mathcal{L}(V, W)$  d'une addition et d'une multiplication par scalaire somme suit :

- Si  $\varphi, \psi \in \mathcal{L}(V, W)$ , alors  $\varphi + \psi \in \mathcal{L}(V, W)$  est la application

$$v \mapsto \varphi(v) + \psi(v).$$

- Si  $\varphi \in \mathcal{L}(V, W)$  et  $\lambda \in K$ , alors  $\lambda \cdot \varphi \in \mathcal{L}(V, W)$  est la application

$$v \mapsto \lambda \cdot \varphi(v).$$

Nous pouvons donc montrer ce qui suit.

**Proposition 7.2.2.** *L'ensemble  $\mathcal{L}(V, W)$  muni des opérations définies ci-dessus est un  $K$ -espace vectoriel. En plus, si  $\dim(V) = n < \infty$  et  $\dim(W) = m < \infty$ , alors  $\mathcal{L}(V, W)$  est de dimension finie et  $\dim(\mathcal{L}(V, W)) = mn$*

AZ: Il serait peut-être utile d'aborder ce résultat sous un autre angle. Si on définit l'addition et la multiplication par scalaire comme ci-dessus, alors l'ensemble de toutes les fonctions de  $V$  dans  $W$  devient un espace vectoriel sur le corps  $K$ . Cela n'a rien à voir avec le fait que  $V$  soit un espace vectoriel, mais seulement avec le fait que  $V$  est un ensemble non vide et que  $W$  est un  $K$ -espace vectoriel. Lorsque  $V$  est aussi un  $K$ -espace vectoriel, on peut parler des applications linéaires de  $V$  dans  $W$ , et la proposition stipule que les transformations linéaires forment un sous-espace de l'espace de toutes les fonctions de  $V$  dans  $W$ .

On peut également composer des applications linéaires, ce qui donne toujours une autre application linéaire. De plus, si une application linéaire est bijective, alors son inverse est également linéaire.

### 7.2.1 Le groupe linéaire général

**Définition 7.2.3.** On pose  $GL(V) = \mathcal{L}(V, V) \cap \text{Bij}(V)$ , l'ensemble de toutes les applications linéaires bijectives de  $V$  dans  $V$ . Alors  $GL(V)$  est un groupe avec la composition de fonctions comme opération binaire (= loi de composition interne). Ce groupe s'appelle le groupe général linéaire de  $V$

### 7.3 Pour réfléchir chez vous

**Exercice 7.3.1.** Soient  $V$  un  $K$ -espace vectoriel de dimension finie et  $\varphi \in \mathcal{L}(V, V)$  une involution, c.-à-d.,  $\varphi^2 = \varphi \circ \varphi = \text{id}_V$ . Prouvez que les affirmations suivantes sont vraies.

- (i)  $V_+ := \{v \in V \mid \varphi(v) = v\}$  et  $V_- := \{v \in V \mid \varphi(v) = -v\}$  sont des sous-espaces vectoriels de  $V$ .
- (ii)  $V = V_+ \oplus V_-$ .
- (iii) L'application linéaire définie par  $\frac{1}{2}(\varphi + \text{id}_V)$  est la projection sur  $V_+$  parallèlement à  $V_-$ .
- (iv) Quelle est l'interprétation géométrique si  $V = \mathbb{R}^2$ ? Et si  $V = \mathbb{R}^3$  et  $\dim(V_+) = 2$ ?

## Cours 10

---

Partout, soient  $K$  un corps,  $V$  et  $W$  des espaces vectoriels sur  $K$ , et  $\varphi : V \rightarrow W$  une application  $K$ -linéaire.

## 8.1 Noyau, image et le théorème du rang

**Définition 8.1.1** ((Rappel)).

(D1) L'image de  $\varphi$  est l'ensemble

$$\text{im}(\varphi) := \{w \in W \mid \exists v \in V \text{ avec } w = \varphi(v)\} \subset W.$$

On vérifie que  $\text{im}(\varphi)$  est un sous-espace vectoriel de  $W$ . Si  $\text{im}(\varphi)$  est de dimension finie, alors  $\dim(\text{im}(\varphi))$  s'appelle le rang de l'application  $\varphi$ .

(D2) Le noyau de  $\varphi$  est l'ensemble

$$\ker(\varphi) := \{v \in V \mid \varphi(v) = 0_W\} \subset V.$$

C'est exactement le même ensemble qu'on a défini pour un morphisme de groupes. On vérifie aussi que  $\ker(\varphi)$  est un sous-espace vectoriel de  $V$  (on sait déjà que c'est un sous-groupe du groupe  $(V, +)$ ).

La proposition suivante nous dit que le noyau de  $\varphi$  détermine si  $\varphi$  est injective.

**Proposition 8.1.2** (Critère d'injectivité). *L'application  $\varphi$  est injective si et seulement si  $\ker(\varphi) = \{0_V\}$ .*

*Démonstration.* On suppose tout d'abord que  $\varphi$  est injective. Alors si  $v \in \ker(\varphi)$ , par définition, on a que  $\varphi(v) = 0_W$ . Mais comme  $\varphi(0_V) = 0_W$  aussi, l'injectivité de  $\varphi$  implique que  $v = 0_V$ , et on conclut que  $\ker(\varphi) = \{0_V\}$ .

Supposons maintenant que  $\ker(\varphi) = \{0_V\}$ . Soient  $u, v \in V$  tels que  $\varphi(u) = \varphi(v)$ . On a que

$$\begin{aligned} \varphi(u - v) &= \varphi(u) - \varphi(v) \\ &= 0_W \\ &\Rightarrow u - v \in \ker(\varphi) \\ &\Rightarrow u - v = 0_V. \end{aligned}$$

Par conséquent,  $u = v$  et  $\varphi$  est bien injective. □

**Corollaire 8.1.3.** *L'application  $\varphi$  est injective si et seulement si  $\varphi$  envoie chaque sous-ensemble linéairement indépendant de  $V$  en un sous-ensemble linéairement indépendant de  $W$ .*

*Démonstration.* On utilise la Proposition 8.1.2. Supposons que  $\varphi$  soit injective. Alors,  $\ker(\varphi) = \{0_V\}$ . Prenons  $X \subset V$  linéairement indépendant. Si  $v_1, \dots, v_k \in X$  on a que

$$\begin{aligned} \alpha_1 \cdot \varphi(v_1) + \dots + \alpha_k \cdot \varphi(v_k) = 0_W &\Rightarrow \varphi(\alpha_1 \cdot v_1 + \dots + \alpha_k \cdot v_k) = 0_W \\ &\Rightarrow \alpha_1 \cdot v_1 + \dots + \alpha_k \cdot v_k = 0_V \\ &\Rightarrow \alpha_1 = \dots = \alpha_k = 0 \end{aligned}$$

et les vecteurs  $\varphi(v_1) + \dots + \varphi(v_k)$  sont donc linéairement indépendants. Cet argument montre que l'image de  $X$  sous  $\varphi$  est une partie libre. En effet, si  $w_1, \dots, w_k \in \text{im}(\varphi)$ , alors il existe  $v_1, \dots, v_k \in X$  tels que  $w_i = \varphi(v_i)$  pour chaque  $1 \leq i \leq k$  et nous avons prouvé que

$$v_1, \dots, v_k \text{ libres} \Rightarrow w_1 = \varphi(v_1), \dots, w_k = \varphi(v_k) \text{ libres.}$$

Maintenant, supposons que  $\varphi$  envoie chaque sous-ensemble linéairement indépendant de  $V$  en un sous-ensemble linéairement indépendant de  $W$ . Soit  $v$  un vecteur non nul dans  $V$ . Alors, l'ensemble  $X = \{v\}$  est libre. L'image de  $X$ , l'ensemble constitué du vecteur  $\varphi(v)$ , est donc libre. Par conséquent,  $\varphi(v) \neq 0_W$ . Ceci montre que  $\ker(\varphi) = \{0_V\}$  et il découle de la Proposition 8.1.2 que  $\varphi$  est injective.  $\square$

On aimerait un critère aussi clair pour déterminer si une application  $K$ -linéaire est surjective. Comme  $\text{im}(\varphi)$  est un sous-espace vectoriel, si  $W$  est de dimension finie,  $\varphi$  est surjective si et seulement si  $\dim(\text{im}(\varphi)) = \dim(W)$ . Le théorème suivant nous dit comment utiliser le noyau pour calculer le rang de l'application  $\varphi$ . C'est l'un des résultats les plus importants de l'algèbre linéaire.

**Théorème 8.1.4** (Théorème du rang). *Supposons que  $V$  soit de dimension finie. Alors*

$$\dim(\text{im}(\varphi)) + \dim(\ker(\varphi)) = \dim(V).$$

*Démonstration.* Soient  $n = \dim(V)$ ,  $k = \dim(\ker(\varphi))$  et  $\{v_1, \dots, v_k\}$  une base de  $\ker(\varphi) \leq V$ . Si  $k = n$ , alors  $\varphi$  est l'application nulle et il n'y a rien à prouver. Donc, on suppose  $n > k$ . Or, comme il s'agit de vecteurs linéairement indépendants dans  $V$ , nous savons que nous pouvons compléter cet ensemble en une base de  $V$ . Donc, il existe  $v_{k+1}, \dots, v_n$  tels que  $\{v_1, \dots, v_k, v_{k+1}, \dots, v_n\}$  est une base de  $V$ . Par conséquent, il suffit de démontrer que  $\{\varphi(v_{k+1}), \dots, \varphi(v_n)\}$  est une base de  $\text{im}(\varphi)$ . Certainement, on a que  $\text{im}(\varphi) \subset \text{Vect}(\varphi(v_1), \dots, \varphi(v_n))$  et comme  $\varphi(v_j) = 0_W$  pour  $j \leq k$  nous voyons que des vecteurs  $\varphi(v_{k+1}), \dots, \varphi(v_n)$  engendrent  $\text{im}(\varphi)$ . Ainsi, on va juste montrer que ces vecteurs sont libres. Prenons des scalaires  $\lambda_{k+1}, \dots, \lambda_n \in K$  tels que

$$\sum_{j=k+1}^n \lambda_j \cdot (\varphi(v_j)) = 0_W.$$

Alors,  $\varphi\left(\sum_{j=k+1}^n \lambda_j \cdot v_j\right) = 0_W$  et le vecteur  $v := \sum_{j=k+1}^n \lambda_j \cdot v_j$  appartient à  $\ker(\varphi)$ . Maintenant, comme des vecteurs  $v_1, \dots, v_k$  forment une base de  $\ker(\varphi)$ , il existe des scalaires  $\alpha_1, \dots, \alpha_k \in K$  tels que  $v = \alpha_1 \cdot v_1 + \dots + \alpha_k \cdot v_k$ . Mais alors on a que

$$v - v = \sum_{i=1}^k \alpha_i \cdot v_i - \sum_{j=k+1}^n \lambda_j \cdot v_j = 0_V,$$

et comme  $v_1, \dots, v_n$  sont linéairement indépendants, ça implique que

$$\alpha_1 = \dots = \alpha_k = -\lambda_{k+1} = \dots = -\lambda_n = 0.$$

Donc,  $\lambda_{k+1} = \dots = \lambda_n = 0$ ; et, par conséquent, on déduit que des vecteurs  $\varphi(v_{k+1}), \dots, \varphi(v_n)$  sont linéairement indépendants.  $\square$

Notez qu'on a déjà prouvé que  $k \leq n$

**Corollaire 8.1.5.** Si  $\dim(V) > \dim(W)$ , alors  $\varphi \in \mathcal{L}(V, W)$  n'est pas injective.

*Démonstration.* Puisque

$$\begin{aligned}\dim(\ker(\varphi)) &= \dim(V) - \dim(\operatorname{im}(\varphi)) \\ &\geq \dim(V) - \dim(W) \\ &> 0\end{aligned}$$

on déduit que  $\ker(\varphi) \neq \{0_V\}$ . □

**Corollaire 8.1.6.** Si  $\dim(V) < \dim(W)$ , alors  $\varphi \in \mathcal{L}(V, W)$  n'est pas surjective.

*Démonstration.* Puisque

$$\begin{aligned}\dim(\operatorname{im}(\varphi)) &= \dim(V) - \dim(\ker(\varphi)) \\ &\leq \dim(V) \\ &< \dim(W)\end{aligned}$$

on déduit que  $\operatorname{im}(\varphi) \neq \{W\}$ . □

**Corollaire 8.1.7** (Critère de bijectivité). Supposons que  $V$  soit de dimension finie.

(i) Si  $\varphi$  est bijective, alors  $W$  est aussi de dimension finie et  $\dim(V) = \dim(W)$ .

(ii) Si  $W$  est aussi de dimension finie et  $\dim(V) = \dim(W)$ , alors  $\varphi$  est bijective si et seulement si  $\varphi$  est injective si et seulement si  $\varphi$  est surjective.

**Corollaire 8.1.8.** Si  $V$  est de dimension finie avec  $\dim(V) = n$ , alors  $V$  est isomorphe à  $K^n$ .

*Démonstration.* Soit  $L = \{v_1, \dots, v_k\} \subset V$  une partie libre, complétons  $L$  (si nécessaire) en une base  $\{v_1, \dots, v_k, v_{k+1}, \dots, v_n\}$  de  $V$  et considérons la base canonique  $\mathcal{B}_{\text{can}} = \{e_1, \dots, e_n\}$  de  $K^n$ . Le Théorème 7.1.3 nous dit qu'il existe exactement une application linéaire  $\varphi : V \rightarrow K^n$  telle que  $\varphi(v_i) = e_i$  pour tous  $1 \leq i \leq n$ . Comme  $\operatorname{im}(L) \subset \mathcal{B}_{\text{can}}$  et  $\mathcal{B}_{\text{can}}$  est libre, on déduit que  $\operatorname{im}(L)$  est libre et que cette application est donc injective par le Corollaire 8.1.3, donc bijective par le Corollaire 8.1.7. □

AZ: Notez que la démonstration du dernier Corollaire nous dit que chaque choix de base de  $V$ , avec un ordre particulier des vecteurs, définit un isomorphisme  $V \xrightarrow{\cong} K^n$ . En fait, nous aurions pu également considérer n'importe quelle autre base de  $K^n$ ...

## 8.2 Pour réfléchir chez vous

**Exercice 8.2.1.** Prouvez que l'affirmation suivante est vraie : un système homogène d'équations linéaires avec plus de variables que d'équations possède des solutions non nulles.

**Exercice 8.2.2.** Considérez  $V := \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathbb{M}_{2 \times 2}(\mathbb{C}) \mid a_{ij} = \overline{a_{ji}} \right\}$  comme  $\mathbb{R}$ -espace vectoriel et l'application

$$\begin{aligned} \varphi : \mathbb{R}^4 &\rightarrow V \\ (a, b, c, d) &\mapsto \begin{pmatrix} a + d & b + ci \\ b - ci & d - a \end{pmatrix}. \end{aligned}$$

Prouvez que  $\varphi$  est une application linéaire bijective.

## Cours 11

---

Fixons  $K$ , un corps, et  $V$  et  $W$ , des espaces vectoriels sur  $K$ . Rappelez-vous que si  $\{v_1, \dots, v_n\}$  est une base de  $V$  et  $\varphi : V \rightarrow W$  est linéaire, alors les valeurs de  $\varphi(v_1), \dots, \varphi(v_n)$  déterminent les valeurs de  $\varphi$  sur des vecteurs arbitraires dans  $V$ . On va voir que les matrices constituent une méthode efficace pour enregistrer les valeurs des  $\varphi(v_1), \dots, \varphi(v_n)$  en termes d'une base de  $W$ .

**Définition 9.0.1.** Une **base ordonnée** d'un  $K$ -espace vectoriel  $V$  de dimension finie ( $= n$ ) est un  $n$ -uplet  $(v_1, \dots, v_n)$  ordonné, c'est-à-dire un élément du produit cartésien  $V \times \dots \times V$  ( $n$  copies), tel que  $\{v_1, \dots, v_n\}$  soit une base de  $V$ .

Notez que si  $\mathcal{B} = (v_1, \dots, v_n)$  est une base ordonnée de  $V$ , alors pour chaque  $v \in V$  il existe un unique  $n$ -uplet  $(x_1, \dots, x_n) \in K^n$  de scalaires tel que

$$v = \sum_{i=1}^n x_i \cdot v_i.$$

À partir de maintenant, nous allons appeler  $x_i$  la  $i$ -ème coordonnée de  $v$  par rapport à la base ordonnée  $\mathcal{B}$ . En plus, il sera souvent plus pratique d'utiliser la matrice de coordonnées de  $V$  :

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{M}_{n \times 1}(K)$$

plutôt que le  $n$ -uplet  $(x_1, \dots, x_n)$  de coordonnées. Pour indiquer la dépendance de cette matrice de coordonnées par rapport à la base, nous utiliserons le symbole  $[v]_{\mathcal{B}}$ .

**▲** Dans la suite, les espaces vectoriels seront de dimension finie et les bases seront des bases ordonnées.

AZ: En plus, j'utiliserai souvent l'isomorphisme  $V \rightarrow \mathbb{M}_{n \times 1}(K)$  déterminé par une base ordonnée  $\mathcal{B}$  de  $V$  et définie par  $v \mapsto [v]_{\mathcal{B}}$ .

## 9.1 La matrice d'une application linéaire

**Définition 9.1.1.** Supposons que  $\varphi \in \mathcal{L}(V, W)$ ,  $\mathcal{B} = (v_1, \dots, v_n)$  soit une base de  $V$  et  $\mathcal{C} = (w_1, \dots, w_m)$  soit une base de  $W$ . La matrice de  $\varphi$  par rapport à ces bases est la matrice dans  $\mathbb{M}_{m \times n}(K)$ , notée par  $[\varphi]_{\mathcal{B}, \mathcal{C}}$ , dont les coefficients  $a_{ij}$  sont définis par

$$\varphi(v_j) = a_{1,j} \cdot w_1 + \dots + a_{m,j} \cdot w_m.$$

Si  $V = W$  et  $\mathcal{B} = \mathcal{C}$  on écrit simplement  $[\varphi]_{\mathcal{B}}$ .

### 9.1.1 Pourquoi définissons-nous la matrice comme cela ?

Posez  $A = [\varphi]_{\mathcal{B}, \mathcal{C}}$  temporairement. Si  $X = [v]_{\mathcal{B}} \in \mathbb{M}_{n \times 1}(K)$  est la matrice de coordonnées de  $v$  dans la base ordonnée  $\mathcal{B}$ , alors  $AX$  est la matrice de coordonnées du vecteur  $\varphi(v)$  dans la base ordonnée  $\mathcal{C}$ , c'est-à-dire,  $AX = [\varphi(v)]_{\mathcal{C}}$ .

Pour mémoriser la construction de  $[\varphi]_{\mathcal{B}, \mathcal{C}} \in \mathbb{M}_{m \times n}(K)$  à partir de  $\varphi$ , vous pouvez écrire en haut de la matrice les vecteurs dans l'espace de départ et à gauche les vecteurs dans l'espace d'arrivée, comme suit :

$$[\varphi]_{\mathcal{B}, \mathcal{C}} = \begin{array}{c} w_1 \\ \vdots \\ w_m \end{array} \begin{pmatrix} v_1 & \dots & v_j & \dots & v_n \\ \dots & a_{1,j} & \dots & & \\ \vdots & \vdots & \vdots & \vdots & \\ \dots & a_{m,j} & \dots & & \end{pmatrix}$$

Ce qui est important à retenir, c'est que la  $j$ -ième colonne de  $[\varphi]_{\mathcal{B}, \mathcal{C}}$  est constituée des scalaires utilisés pour écrire  $\varphi(v_j)$  comme une combinaison linéaire de  $w_1, \dots, w_m$ .

Nous pouvons résumer notre discussion sous la forme d'un théorème.

**Théorème 9.1.2.** Soient  $\mathcal{B}$  une base ordonnée pour  $V$  et  $\mathcal{C}$  une base ordonnée pour  $W$ . Pour chaque transformation linéaire  $\varphi : V \rightarrow W$ , il existe une matrice  $A_\varphi = [\varphi]_{\mathcal{B}, \mathcal{C}} \in \mathbb{M}_{m \times n}(K)$  telle que

$$[\varphi(v)]_{\mathcal{C}} = A_\varphi \cdot [v]_{\mathcal{B}}.$$

De plus,  $\varphi \mapsto A_\varphi$  est un isomorphisme entre les espaces vectoriels  $\mathcal{L}(V, W)$  et  $\mathbb{M}_{m \times n}(K)$ .

AZ: **▲** Il faut cependant noter qu'un tel isomorphisme dépend fortement des bases choisies.

Une autre aide visuelle précieuse à retenir est le diagramme suivant.

$$\begin{array}{ccccc} [v]_{\mathcal{B}} & \mathbb{M}_{n \times 1}(K) \simeq K^n \xrightarrow[\text{par } A_\varphi]{\text{mult.}} \mathbb{M}_{m \times 1}(K) \simeq K^m & & & [\varphi(v)]_{\mathcal{C}} \\ \uparrow & \simeq_{\mathcal{B}} \uparrow & & & \uparrow \\ v & V \xrightarrow{\varphi} W & & & \varphi(v) \\ & & & & \simeq_{\mathcal{C}} \end{array}$$

### 9.1.2 Quelques exemples

**Exemple 9.1.3.** Supposons que  $\varphi \in \mathcal{L}(\mathbb{R}^2, \mathbb{R}^3)$  soit défini par

$$\varphi : (x, y) \mapsto (x + 3y, 2x + 5y, 7x + 9y).$$

Comme  $(1, 0) \mapsto (1, 2, 7)$  et  $(0, 1) \mapsto (3, 5, 9)$ , la matrice de  $\varphi$  par rapport aux bases canoniques est la matrice ci-dessous :

$$\begin{pmatrix} 1 & 3 \\ 2 & 5 \\ 7 & 9 \end{pmatrix}.$$

**Exemple 9.1.4.** Pour  $n \in \mathbb{N}$ ,  $K[x]_{\leq n}$  désigne l'ensemble de tous les polynômes à coefficients dans  $K$  et de degré au plus  $n$ . Considérons la base « standard »  $1, x, \dots, x^n$ . Supposons que  $D \in \mathcal{L}(K[x]_{\leq 3}, K[x]_{\leq 2})$  soit l'application de différentiation définie dans l'Exemple 7.1.5. La matrice de  $D$  par rapport aux bases « standard » est la matrice ci-dessous :

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

### 9.1.3 Pour réfléchir chez vous

**Exercice 9.1.5.** Soit  $V$  un  $K$ -espace vectoriel de dimension finie et soit encore  $\mathcal{B} = (v_1, \dots, v_n)$  une base ordonnée de  $V$ . Nous avons prouvé qu'il existe un unique endomorphisme  $\varphi : V \rightarrow V$  tel que  $\varphi(v_j) = v_{j+1}$  pour tous  $1 \leq j \leq n-1$  et  $\varphi(v_n) = 0_V$ . Quelle est la matrice  $A = [\varphi]_{\mathcal{B}}$  de  $\varphi$  par rapport à la base ordonnée? Montrez que  $\varphi^n = 0$  mais  $\varphi^{n-1} \neq 0$ .

## 9.2 Changement de base et des matrices semblables

AZ: Je vous propose de regarder la vidéo « Change of basis » sur la chaîne *3Blue1Brown*.

**Définition 9.2.1.** Soient  $\mathcal{B} = (v_1, \dots, v_n)$  et  $\tilde{\mathcal{B}} = (w_1, \dots, w_n)$  deux bases d'un  $K$ -espace vectoriel  $V$ . On exprime les  $v_i$  en termes de la base  $\tilde{\mathcal{B}}$  :

$$v_j = p_{1j}w_1 + p_{2j}w_2 + \dots + p_{nj}w_n.$$

On définit donc une matrice  $P = (p_{ij}) \in \mathbb{M}_{n \times n}(K)$  telle que la  $j$ -ième colonne de  $P$  est le vecteur colonne  $[v_j]_{\tilde{\mathcal{B}}}$ . Cette matrice  $P$  s'appelle **la matrice de changement de base entre la base  $\mathcal{B}$  et la base  $\tilde{\mathcal{B}}$** . On dit aussi que  $P$  est la matrice de passage entre la base  $\mathcal{B}$  et la base  $\tilde{\mathcal{B}}$ .

On note que  $P$  est la matrice de l'application identité  $\text{id} : V \rightarrow V$ , par rapport aux bases  $\mathcal{B}$  et  $\tilde{\mathcal{B}}$ ; c'est-à-dire  $P = [\text{id}]_{\mathcal{B}, \tilde{\mathcal{B}}}$ . En particulier,  $P$  est nécessairement inversible et on a que

- $[v]_{\tilde{\mathcal{B}}} = P \cdot [v]_{\mathcal{B}}$  et
- $[v]_{\mathcal{B}} = P^{-1} \cdot [v]_{\tilde{\mathcal{B}}}$ ,

pour chaque vecteur  $v \in V$ .

AZ: Parfois, il sera utile d'écrire  $P_{\mathcal{B} \rightarrow \tilde{\mathcal{B}}}$ .

En utilisant ce qui précède, nous pouvons maintenant prouver ce qui suit.

**Théorème 9.2.2.** Soit  $\varphi \in \mathcal{L}(V, W)$ , soient  $\mathcal{B}$  et  $\tilde{\mathcal{B}}$  deux bases de  $V$  et soient  $\mathcal{C}$  et  $\tilde{\mathcal{C}}$  deux bases de  $W$ . Posons,  $P = [\text{id}_V]_{\mathcal{B}, \tilde{\mathcal{B}}}$ ,  $Q = [\text{id}_W]_{\mathcal{C}, \tilde{\mathcal{C}}}$ ,  $A_\varphi = [\varphi]_{\mathcal{B}, \mathcal{C}}$  et  $\tilde{A}_\varphi = [\varphi]_{\tilde{\mathcal{B}}, \tilde{\mathcal{C}}}$ . Alors,

$$\tilde{A}_\varphi = Q \cdot A_\varphi \cdot P^{-1}.$$

*Démonstration.* Supposons  $\dim(V) = n$  et  $\dim(W) = m$ . La preuve découle du diagramme commutatif ci-dessous.

$$\begin{array}{ccccccc} \mathbb{M}_{n \times 1}(K) & \xrightarrow{P^{-1}} & \mathbb{M}_{n \times 1}(K) & \xrightarrow{A_\varphi} & \mathbb{M}_{m \times 1}(K) & \xrightarrow{Q} & \mathbb{M}_{m \times 1}(K) \\ \simeq_{\tilde{\mathcal{B}}} \uparrow & & \simeq_{\mathcal{B}} \uparrow & & \simeq_{\mathcal{C}} \uparrow & & \simeq_{\tilde{\mathcal{C}}} \uparrow \\ V & \xrightarrow{\text{id}_V} & V & \xrightarrow{\varphi} & W & \xrightarrow{\text{id}_W} & W \end{array}$$

□

**Définition 9.2.3.** Soient  $A, B \in \mathbb{M}_{n \times n}(K)$ . On dit que  $A$  et  $B$  sont semblables s'il existe une matrice inversible  $P \in \mathbb{M}_{n \times n}(K)$  telle que  $PAP^{-1} = B$ . On vérifie que « être semblable » est une relation d'équivalence sur l'ensemble  $\mathbb{M}_{n \times n}(K)$ .

Les exemples clés de ce cours proviendront de l'observation suivante.

**Remarque 6.** Soit  $\varphi \in \mathcal{L}(V, V)$  et supposons que  $\dim(V) = n$ . Soient  $\mathcal{B}$  et  $\tilde{\mathcal{B}}$  deux bases de  $V$ . Alors les matrices  $[\varphi]_{\mathcal{B}}$  et  $[\varphi]_{\tilde{\mathcal{B}}}$  sont semblables. Cela découle du théorème précédent.

Pouvez-vous voir pourquoi ?

### 9.2.1 Quelques exemples

**Exemple 9.2.4.** Considérons  $\mathcal{B} = ((4, 2), (5, 3))$  et  $\tilde{\mathcal{B}} = ((1, 0), (0, 1))$  deux bases (ordonnées) de  $\mathbb{R}^2$ . Alors,

$$[\text{id}]_{\mathcal{B}, \tilde{\mathcal{B}}} = \begin{pmatrix} 4 & 5 \\ 2 & 3 \end{pmatrix}$$

et

$$[\text{id}]_{\tilde{\mathcal{B}}, \mathcal{B}} = \frac{1}{2} \begin{pmatrix} 3 & -5 \\ -2 & 4 \end{pmatrix}.$$

**Exemple 9.2.5.** Considérons  $\mathcal{B} = ((2, 4), (6, 8))$  et  $\tilde{\mathcal{B}} = ((7, 3), (4, 2))$  deux bases (ordonnées) de  $\mathbb{R}^2$ . Alors,

$$[(2, 4)]_{\tilde{\mathcal{B}}} = \begin{pmatrix} -6 \\ 11 \end{pmatrix} \quad \text{et} \quad [(6, 8)]_{\tilde{\mathcal{B}}} = \begin{pmatrix} -10 \\ 19 \end{pmatrix}$$

car  $(2, 4) = -6 \cdot (7, 3) + 11 \cdot (4, 2)$  et  $(6, 8) = -10 \cdot (7, 3) + 19 \cdot (4, 2)$ . Donc,

$$P_{\mathcal{B} \rightarrow \tilde{\mathcal{B}}} = [\text{id}]_{\mathcal{B}, \tilde{\mathcal{B}}} = \begin{pmatrix} -6 & -10 \\ 11 & 19 \end{pmatrix}.$$

Mais nous avons aussi que

$$P_{\tilde{\mathcal{B}} \rightarrow \mathcal{B}} = [\text{id}]_{\tilde{\mathcal{B}}, \mathcal{B}} = \begin{pmatrix} -6 & -10 \\ 11 & 19 \end{pmatrix}^{-1} = -\frac{1}{4} \cdot \begin{pmatrix} 19 & 10 \\ -11 & -6 \end{pmatrix}.$$

Notez que pour trouver des scalaires  $x, y \in \mathbb{R}$  tels que  $(2, 4) = x \cdot (7, 3) + y \cdot (4, 2)$  il faut résoudre le système d'équations :

$$\begin{cases} 7x + 4y = 2 \\ 3x + 2y = 4 \end{cases},$$

ce qui nous donne  $x = -6$  et  $y = 11$ . Un raisonnement similaire s'applique aussi au deuxième vecteur de  $\mathcal{B}$ .

AZ: Avant de considérer des exemples plus intéressants dans des dimensions supérieures, nous devons donc apprendre à résoudre des systèmes linéaires avec nombreuses équations...

## (★) Cours 12 (non examinable)

---

### 10.1 Forme linéaires (covecteurs)

Si  $V$  est un espace vectoriel sur le corps  $K$ , on peut toujours considérer des transformations linéaires de  $V$  dans  $K$ . Une telle application  $\varphi \in \mathcal{L}(V, K)$  est également appelée une forme linéaire. Rappelez-vous que cela signifie que  $\varphi$  est une fonction de  $V$  dans  $K$  telle que

$$\varphi(\alpha \cdot u + v) = \alpha \cdot \varphi(u) + \varphi(v)$$

pour tous les vecteurs  $u$  et  $v$  dans  $V$  et tous les scalaires  $\alpha$  dans  $K$ . Le concept de forme linéaire est très important dans l'étude des espaces de dimension finie car il permet d'organiser et de clarifier la discussion sur les sous-espaces, les équations linéaires et les coordonnées.

**Définition 10.1.1.** Une forme linéaire sur  $V$  est un élément de  $\mathcal{L}(V, K)$ . On appelle  $\mathcal{L}(V, K)$  l'espace dual de  $V$  et on le note  $V^*$ .

**Exemple 10.1.2.** L'application

$$\begin{aligned} \varphi : \mathbb{R}^3 &\rightarrow \mathbb{R} \\ (x, y, z) &\mapsto x + y + z \end{aligned}$$

est une forme linéaire sur  $\mathbb{R}^3$ .

**Exemple 10.1.3.** Plus généralement, si  $\alpha_1, \dots, \alpha_n$  sont des scalaires dans  $K$ , alors

$$\begin{aligned} \varphi : K^n &\rightarrow K \\ (x_1, \dots, x_n) &\mapsto \alpha_1 \cdot x_1 + \dots + \alpha_n \cdot x_n \end{aligned}$$

est une forme linéaire sur  $K^n$ . Il s'agit de la forme linéaire représentée par la matrice  $(\alpha_1 \ \dots \ \alpha_n)$  relative à la base (ordonnée) canonique de  $K^n$  et à la base  $\{1\}$  pour  $K$ . En fait, toute forme linéaire sur  $K^n$  est de cette forme, pour certains scalaires  $\alpha_1, \dots, \alpha_n$ .

**Exemple 10.1.4.** Si  $A = (a_{ij}) \in \mathbb{M}_{n \times n}(K)$ , sa trace est le scalaire

$$\text{tr}(A) = a_{11} + a_{22} + \dots + a_{nn}.$$

Nous avons donc une forme linéaire  $\text{tr} : \mathbb{M}_{n \times n}(K) \rightarrow K$ .

**Exemple 10.1.5.** Soit  $[a, b]$  un intervalle fermé sur la droite réelle et soit  $\mathcal{C}([a, b])$  l'espace des fonctions réelles continues sur  $[a, b]$ . Alors

$$\begin{aligned} \varphi : \mathcal{C}([a, b]) &\rightarrow \mathbb{R} \\ f &\mapsto \int_a^b f(x) \, dx \end{aligned}$$

est une forme linéaire sur  $\mathcal{C}([a, b])$ .

### 10.1.1 Bases duales

Si  $V$  est de dimension finie, on peut obtenir une description assez explicite de l'espace dual  $V^*$ . Nous savons que  $\dim(V) = \dim(V^*)$ , alors les deux espaces sont isomorphes.

En effet, si  $\mathcal{B} = (v_1, \dots, v_n)$  est une base ordonnée de  $V$ , alors d'après le Théorème 7.1.3, il existe (pour tout  $i$ ) une unique forme linéaire  $\varphi_i \in V^*$  telle que  $\varphi_i(v_j) = \delta_{ij}$  (delta de Kroenecker). On obtient ainsi une base ordonnée  $(\varphi_1, \dots, \varphi_n)$  de  $V^*$ . Cette base est appelée la **base duale de  $\mathcal{B}$** . En plus,

- pour chaque forme linéaire  $\varphi \in V^*$  on a que

$$\varphi = \varphi(v_1) \cdot \varphi_1 + \dots + \varphi(v_n) \cdot \varphi_n,$$

- et pour chaque vecteur  $v \in V$  on a que

$$v = \varphi_1(v) \cdot v_1 + \dots + \varphi_n(v) \cdot v_n.$$

Autrement dit, si  $\mathcal{B} = (v_1, \dots, v_n)$  est une base ordonnée de  $V$  et  $\mathcal{B}^* = (\varphi_1, \dots, \varphi_n)$  est la base duale, alors chaque  $\varphi_i$  est précisément la fonction qui assigne à chaque vecteur  $v \in V$  la  $i$ -ème coordonnée de  $v$  par rapport à la base ordonnée  $\mathcal{B}$ .

AZ: Les formes linéaires  $\varphi_1, \dots, \varphi_n$  sont parfois appelées fonctions coordonnées. Elles sont aussi souvent notées  $v_1^*, \dots, v_n^*$ .

### 10.1.2 Application transposée

Étant donnés deux espaces vectoriels  $V$  et  $W$  sur  $K$  et une application linéaire  $T : V \rightarrow W$ , nous allons maintenant introduire la notion d'application transposée qui nous permet de faire commuter le diagramme suivant :

$$\begin{array}{ccc} V & \xrightarrow{T} & W \\ & \searrow T^t(\psi) & \downarrow \varphi \\ & & K \end{array}$$

**Définition 10.1.6.** Soit  $T \in \mathcal{L}(V, W)$ , on appelle la transposée de  $T$ , noté  $T^t$ , l'application dans  $\mathcal{L}(W^*, V^*)$  définie par

$$\begin{aligned} T^t : W^* &\rightarrow V^* \\ \varphi &\mapsto \varphi \circ T : \underset{\in V}{v} \mapsto \underset{\in K}{\varphi(T(v))} \end{aligned}$$

Supposons  $\dim(V) = n$  et  $\dim(W) = m$  et fixons deux bases ordonnées  $\mathcal{B} = (v_1, \dots, v_n)$  et  $\mathcal{C} = (w_1, \dots, w_m)$  de  $V$  et  $W$ , respectivement. Considérons aussi les bases duales  $\mathcal{B}^* = (\varphi_1, \dots, \varphi_n)$  et  $\mathcal{C}^* = (\psi_1, \dots, \psi_m)$  correspondantes. On peut prouver ce qui suit.

**Théorème 10.1.7.**

- (i) Soient  $T \in \mathcal{L}(V, W)$  et  $A = (a_{ij}) \in \mathbb{M}_{m \times n}(K)$  la matrice  $[T]_{\mathcal{B}, \mathcal{C}}$ . Alors,  $a_{ij} = \psi_j(T(v_i))$ .
- (ii) En plus, la transpose de  $A$  est la matrice de l'application transposée  $T^t$  par rapport aux bases duales.

**10.1.3 Hyperplans**

**Définition 10.1.8.** Soit  $H \leq V$  un sous-espace. On appelle  $H$  un hyperplan de  $V$  si  $H$  est égal au noyau d'une forme linéaire sur  $V$  non identiquement nulle.

**Exemple 10.1.9.** L'ensemble  $\{(x, y, z) \in \mathbb{R}^3 \mid x - 2y + 3z = 0\}$  est un hyperplan en tant que noyau de la forme linéaire  $\varphi : (x, y, z) \mapsto x - 2y + 3z$ .

Notons que dans un espace vectoriel de dimension  $n$ , un hyperplan est un sous-espace de dimension  $n - 1$ . En effet, un hyperplan est le noyau d'une forme linéaire non nulle donc de rang 1, d'après le théorème du rang, un hyperplan est donc de dimension  $n - 1$ . La réciproque est aussi vraie. Si  $\{v_1, \dots, v_{n-1}\}$  est une base d'un sous-espace  $H \leq V$ , alors on complète en une base  $\{v_1, \dots, v_{n-1}, v_n\}$  de  $V$  et la forme linéaire  $\varphi$  définie par  $\varphi(v_i) = 0$  pour  $i = 1, \dots, n - 1$  et  $\varphi(v_n) = 1$  est une forme linéaire non nulle dont le noyau est précisément  $H$ .

En d'autres termes, nous avons prouvé ce qui suit.

**Proposition 10.1.10.** Soient  $V$  un espace vectoriel de dimension finie  $n$  et  $H$  un sous-espace vectoriel de  $V$ . Alors  $H$  est un hyperplan de  $V$  si et seulement si  $\dim(H) = n - 1$ .

Plus généralement, on peut montrer aussi que tout sous-espace de  $V$  de dimension  $k$  quelconque peut être décrit comme l'intersection de  $n - k$  hyperplans.

**Définition 10.1.11.** Soit  $U \leq V$  un sous-espace, on appelle **orthogonal** de  $U$  noté  $U^\perp$  (ou, parfois,  $U^\circ$ ) l'ensemble

$$U^\perp := \{\varphi \in V^* \mid \forall u \in U, \varphi(u) = 0\}$$

On peut montrer que  $U^\perp \leq V^*$  et que dans le cas où  $\dim(V) = n$  on a que  $\dim(U^\perp) = n - \dim(U)$ . En fait, si  $U \leq V$  et  $\{\varphi_1, \dots, \varphi_{n-k}\}$  est une base de  $U^\perp$ , on a que

$$u \in U \iff \begin{cases} \varphi_1(u) = 0 \\ \vdots \\ \varphi_{n-k}(u) = 0 \end{cases}.$$

Ainsi, trouver une base pour  $U^\perp$  implique, en pratique, de trouver un système linéaire à  $n$  inconnues et  $n - k$  équations dont l'espace de solutions est exactement le sous-espace  $U$ . Il découle de ce même argument que trouver une base pour  $U^\perp$  implique, en pratique, de trouver des formes linéaires  $\varphi_1, \dots, \varphi_{n-k} \in V^*$  qui sont libres et telles que  $U = \ker(\varphi_1) \cap \dots \cap \ker(\varphi_{n-k})$ . En bref, si  $U \leq V$  est un sous-espace de dimension  $k$  et  $\dim(V) = n$  alors il existe des hyperplans  $H_1, \dots, H_{n-k}$  tels que  $U = H_1 \cap \dots \cap H_{n-k}$ .

## 10.2 Pour réfléchir chez vous

**Exercice 10.2.1.** Soient  $V$  et  $W$  des espaces vectoriels de dimension finie sur un corps  $K$ . Soit encore  $T \in \mathcal{L}(V, W)$ . Montrer que

- (i)  $\ker(T^t) = \text{im}(T)^\perp$  et
- (ii)  $\text{im}(T^t) = \ker(T)^\perp$ .

**Exercice 10.2.2.** Si  $H \subset \mathbb{R}^n$  est un hyperplan, quelle est la description géométrique des sous-espaces complémentaires ? C'est-à-dire, si  $\mathbb{R}^n = H \oplus L$ , quelle est la description géométrique de  $L$  ?

## Cours 13

---

On fixe un corps  $K$ .

### Notation.

(N1) Soit  $X$  un ensemble non vide quelconque. Pour  $a, b \in X$ , le symbole de Kronecker  $\delta_{a,b}$  désigne le nombre réel tel que

$$\delta_{a,b} = \begin{cases} 0, & \text{si } a \neq b \\ 1, & \text{si } a = b \end{cases}$$

(N2) Pour chaque  $1 \leq i \leq m, 1 \leq j \leq n$ , on définit une matrice  $E_{ij} \in \mathbb{M}_{m \times n}(K)$  telle que le seul coefficient non nul soit celui trouvé dans la  $i$ -ième ligne et la  $j$ -ième colonne ; et, de plus, ce coefficient est égal à 1.

(N3) On note que  $\{E_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq n\}$  est une base de  $\mathbb{M}_{m \times n}(K)$ . Je ferai référence à cette base comme la base « standard ».

(N4) Pour

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \in \mathbb{M}_{m \times n}(K),$$

on note  $A = (a_{ij})$  ou  $A = (A_{ij})$  selon les besoins, et on note  $A_i$  la  $i$ -ième ligne de  $A$ .

## 11.1 Opérations élémentaires et forme échelonnée réduite

On définit trois types d'opérations sur les lignes d'une matrice  $A \in \mathbb{M}_{m \times n}(K)$ , appelées **opérations élémentaires**.

- **Type I** Échanger deux lignes de la matrice.
- **Type II** Multiplier une ligne de la matrice par un scalaire non nul  $\lambda \in K$ .
- **Type III** Additionner à une ligne de la matrice un multiple scalaire d'une autre ligne de la matrice.

Une opération élémentaire sur les lignes d'une matrice est donc un type particulier de fonction (règle)  $e$  qui associe à chaque matrice  $A \in \mathbb{M}_{m \times n}(K)$  une matrice  $e(A) \in \mathbb{M}_{m \times n}(K)$ . On peut décrire précisément  $e$  dans les trois cas comme suit :

Type I Si on échange  $A_r$  et  $A_s$ , alors on a que  $e(A)_{ij} = A_{ij}$  si  $i$  est différent de  $r$  et de  $s$ , que  $e(A)_{rj} = A_{sj}$  et que  $e(A)_{sj} = A_{rj}$ .

Type II Si on multiplie  $A_r$  par  $\lambda \in K^\times$ , alors on a que  $e(A)_{ij} = A_{ij}$  si  $i \neq r$ , et que  $e(A)_{rj} = \lambda A_{rj}$ .

Type III Si on additionne  $\lambda \cdot A_s$  à la ligne  $A_r$ , alors on a que  $e(A)_{ij} = A_{ij}$  si  $i \neq r$ , et que  $e(A)_{rj} = A_{rj} + \lambda A_{sj}$ .

Ici,  $K^\times = K \setminus \{0\}$  est le groupe multiplicatif du corps  $K$ .

**Remarque 7.** On note que ces trois opérations sont réversibles dans le sens qu'il existe une opération élémentaire qui renvoie à la matrice de départ.

- Le type I est son propre inverse.
- Pour le type II, on multiplie la même ligne par  $\lambda^{-1}$ .
- Pour le type III, si on additionne  $\lambda \cdot A_s$  à la ligne  $A_r$ , alors l'opération inverse est d'additionner  $-\lambda \cdot A_s$  à  $A_r$ .

**▲** Pour définir  $e(A)$ , le nombre de colonnes de  $A$  n'est pas vraiment important, mais le nombre de lignes de  $A$  est crucial. Pour simplifier la discussion, nous admettrons qu'une opération élémentaire  $e$  est définie sur la classe de toutes les matrices  $m \times n$ , pour un  $m$  fixé mais  $n$  quelconque. Autrement dit, une opération  $e$  particulière est définie sur la classe de toutes les matrices à coefficients dans  $K$  avec  $m$  lignes.

**Définition 11.1.1.** Une matrice carrée  $L \in \mathbb{M}_{m \times m}(K)$  est dite **élémentaire** si elle peut être obtenue en effectuant une seule opération élémentaire sur une seule ligne de la matrice identité  $I_m$ .

Avec tout ce qui précède à l'esprit, on peut maintenant prouver le résultat suivant.

**Proposition 11.1.2.** Soit  $e$  une opération élémentaire. Alors, il existe une matrice élémentaire inversible  $L \in \text{GL}(m, K)$  telle que  $e(A) = L \cdot A$  pour toutes  $A \in \mathbb{M}_{m \times n}(K)$ . En particulier, pour chaque  $n$ ,  $e$  définit une application  $\mathbb{M}_{m \times n}(K) \rightarrow \mathbb{M}_{m \times n}(K)$  qui est linéaire et bijective. De plus, on a que

Type I l'opération  $e : A_r \leftrightarrow A_s$  est représentée par la matrice  $L = (L_{ij}) \in \mathbb{M}_{m \times m}(K)$  telle que  $L_{ii} = 1$  si  $i \notin \{r, s\}$ ,  $L_{rs} = L_{sr} = 1$ , et tous les autres coefficients sont nuls.

Type II L'opération  $e : A_r \rightarrow \lambda \cdot A_r$  (avec  $\lambda \in \mathbb{K}^\times$ ) est représentée par la matrice  $L = (L_{ij}) \in \mathbb{M}_{m \times m}(K)$  telle que

$$L_{ij} = \begin{cases} 1, & \text{si } i = j \neq r \\ 0, & \text{si } i \neq j \\ \lambda, & \text{si } i = j = r \end{cases}$$

Type III L'opération  $e : A_r \rightarrow \lambda \cdot A_s + A_r$  est représentée par la matrice  $L = I_m + \lambda E_{rs} \in \mathbb{M}_{m \times m}(K)$ .

*Démonstration.* Étant donné une opération élémentaire  $e$ , comment trouver la matrice  $L$  correspondante? Eh bien, la matrice est simplement la matrice  $e(I_m)$ !

Pour démontrer la Proposition 11.1.2, le point crucial est que l'élément  $(LA)_{ij}$  de la  $i$ -ième ligne et de la  $j$ -ième colonne de la matrice produit  $LA$  est obtenu à partir de la  $i$ -ième ligne de  $L$  et de la  $j$ -ième colonne de  $A$ . Les trois types d'opérations élémentaires sur les lignes doivent être traités séparément. Nous allons donner une démonstration détaillée pour une opération de type III. Les deux autres cas sont encore plus faciles à traiter et seront laissés comme exercices. Supposons que  $r \neq s$  et que  $e$  soit l'opération  $A_r \rightarrow \lambda \cdot A_s + A_r$ , c.-à-d. « remplacement de  $A_r$  par  $\lambda \cdot A_s + A_r$  ». Alors, en posant  $L = e(I_m)$ , on a que

$$L_{ik} = \begin{cases} \delta_{ik}, & \text{si } i \neq r \\ \delta_{rk} + \lambda \delta_{sk}, & \text{si } i = r \end{cases}$$

Donc,  $L = I_m + \lambda E_{rs}$  et

$$(LA)_{ij} = \sum_{k=1}^m L_{ik} A_{kj} = \begin{cases} A_{ij}, & \text{si } i \neq r \\ A_{rj} + \lambda A_{sj}, & \text{si } i = r \end{cases}$$

Autrement dit,  $L \cdot A = e(A)$ . □

**Définition 11.1.3.** On dit que deux matrices  $A, B \in \mathbb{M}_{m \times n}(K)$  sont lignes équivalentes (ou équivalentes par lignes) si  $B$  peut être obtenue à partir de  $A$  en faisant une suite (finie) d'opérations élémentaires. Autrement dit, si et seulement si  $B = P \cdot A$ , où  $P \in \text{GL}(m, K)$  est un produit de matrices élémentaires  $m \times m$ .

**Remarque 8.** Soient  $A, B \in \mathbb{M}_{m \times n}(K)$  des matrices lignes équivalentes. Alors, chaque ligne de  $B$  est une combinaison linéaire des lignes de  $A$  et chaque ligne de  $A$  est une combinaison linéaire des lignes de  $B$ . En particulier,  $\text{Vect}(A_1, \dots, A_m) = \text{Vect}(B_1, \dots, B_m)$ .

**Remarque 9.** Comme toutes les opérations élémentaires sont réversibles, « être lignes équivalentes » définit une relation d'équivalence sur l'ensemble  $\mathbb{M}_{m \times n}(K)$ . En particulier, la

Si  $r = s$   
l'opération  
est de  
type II

relation est symétrique, c'est-à-dire que si on peut obtenir la matrice  $B$  à partir de la matrice  $A$  par une suite d'opérations élémentaires, on peut également obtenir  $A$  à partir de  $B$ .

**Définition 11.1.4.** On dit qu'une matrice  $A = (a_{ij}) \in \mathbb{M}_{m \times n}(K)$  est **échelonnée réduite** si soit  $A = 0$  soit les quatre propriétés suivantes sont vérifiées.

- (i) La première entrée non nulle dans chaque ligne non nulle de  $A$  est égale à 1 – ces coefficients s'appellent les pivots ;
- (ii) chaque colonne de  $A$  contenant un pivot a toutes ses autres entrées égales à 0 ;
- (iii) chaque ligne de  $A$  dont toutes les entrées sont égales à 0 apparaît sous chaque ligne ayant une entrée différente de zéro ; et
- (iv) si les lignes  $1, \dots, r$  sont les lignes non nulles de  $A$ , et si le pivot de la ligne  $i$  se trouve dans la colonne  $j_i$ , pour  $i = 1, \dots, r$ , alors  $j_1 < j_2 < \dots < j_r$  – ces entiers  $j_1, \dots, j_r$  s'appellent les échelons de la matrice  $A$ .

Notez qu'on peut également décrire une matrice  $A = (a_{ij}) \in \mathbb{M}_{m \times n}(K)$  échelonnée réduite comme suit. Soit chaque entrée dans  $A$  est nulle, soit il existe un entier positif  $r$ , avec  $1 \leq r \leq m$ , et  $r$  entiers positifs  $j_1, \dots, j_r$ , avec  $1 \leq j_i \leq n$ , tels que :

- (e1)  $a_{ij} = 0$  si  $i > r$  ou  $j < j_i$  ;
- (e2)  $a_{kj_i} = \delta_{ki}$  pour  $1 \leq i \leq r$  et  $1 \leq k \leq r$  ;
- (e3)  $j_1 < \dots < j_r$ .

**Exemple 11.1.5.** La matrice  $A = \begin{pmatrix} 0 & \textcircled{1} & -3 & 0 & 2 \\ 0 & 0 & 0 & \textcircled{1} & 4 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$  est échelonnée réduite. Par contre,

la matrice  $B = \begin{pmatrix} 1 & 2 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$  n'est pas échelonnée réduite.

**Théorème 11.1.6.** *Toute matrice est équivalente à une matrice échelonnée réduite. Autrement dit, toute matrice peut être transformée en une matrice échelonnée réduite par une suite finie d'opérations élémentaires sur les lignes de la matrice.*

*Démonstration.* La preuve sera donnée lors du prochain cours. □

## 11.2 Pour réfléchir chez vous

**Exercice 11.2.1.** Pouvez-vous décrire toutes les matrices élémentaires  $2 \times 2$  ?

**Exercice 11.2.2.** Soit  $C = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \in \mathbb{M}_{2 \times 2}(K)$ . Prouvez qu'il existe des matrices  $A, B \in \mathbb{M}_{2 \times 2}(K)$  telles que  $C = AB - BA$  si et seulement si  $c_{11} + c_{22} = 0$ .

**Exercice 11.2.3.** Soit  $A \in \mathbb{M}_{2 \times 2}(K)$ , et supposons que les lignes de la matrice  $A$  forment un ensemble de vecteurs linéairement indépendants dans  $K^2$ . Prouvez que la matrice  $A$  est inversible. Et si  $A \in \mathbb{M}_{n \times n}(K)$  ?

## 12.1 La méthode de Gauss

On fixe un corps  $K$ .

**Théorème 12.1.1.** *Toute matrice  $A \in \mathbb{M}_{m \times n}(K)$  est ligne équivalente à une matrice  $R \in \mathbb{M}_{m \times n}(K)$  échelonnée réduite. De plus, la matrice  $R$  est déterminée de manière unique.*

AZ: Rappelez-vous qu'une matrice  $R = (R_{ij}) \in \mathbb{M}_{m \times n}(K)$  échelonnée réduite si, soit chaque entrée dans  $R$  est nulle, soit il existe un entier positif  $r$ , avec  $1 \leq r \leq m$ , et  $r$  entiers positifs  $j_1, \dots, j_r$ , avec  $1 \leq j_i \leq n$ , tels que :

- (e1)  $R_{ij} = 0$  si  $i > r$  ou  $j < j_i$ ;
- (e2)  $R_{kj_i} = \delta_{ki}$  pour  $1 \leq i \leq r$  et  $1 \leq k \leq r$ ;
- (e3)  $j_1 < \dots < j_r$ .

*Démonstration.* Soit  $A \in \mathbb{M}_{m \times n}(K)$ . On suppose  $A \neq 0$  car sinon  $A$  est déjà échelonnée réduite.

Nous pouvons procéder de manière algorithmique :

Étape 1 Soit  $j_1$  le plus petit indice d'une colonne pour lequel un coefficient de  $A$  est non nul, disons  $a_{ij_1} \neq 0$ . Par une opération de type I (échanger les lignes 1 et  $i$ ), on est ramenée au cas où  $a_{1j_1} \neq 0$  (le pivot associé au plus petit échelon  $j_1$  est en première ligne).

Étape 2 Par une opération de type II, en multipliant la première ligne par  $a_{1j_1}^{-1}$ , on est ramené au cas où  $a_{1j_1} = 1$  (le pivot de la première ligne est égal à 1).

Étape 3 Par une suite d'opérations de type III, on annule tous les autres coefficients de la  $j_1$ -ème colonne ( $A_k \rightarrow -a_{kj_1}A_1 + A_k$ ). On se retrouve ainsi avec une matrice de la forme

$$A^{(1)} := \begin{pmatrix} 0 & \dots & 0 & \overset{j_1}{\textcircled{1}} & * & \dots & * \\ 0 & \dots & 0 & 0 & * & \dots & * \\ \vdots & \dots & \vdots & 0 & * & \dots & * \\ 0 & \dots & 0 & 0 & * & \dots & * \end{pmatrix}.$$

Étape 4 Posons  $B_{2 \rightarrow m}$  la matrice constituée des lignes 2 à  $m$  de  $A^{(1)}$ . Si  $B_{2 \rightarrow m} = 0$ , alors  $A^{(1)}$  est échelonnée réduite. Sinon, soit  $j_2$  le plus petit indice d'une colonne pour laquelle  $B_{2 \rightarrow m}$  possède un coefficient non nul. Alors  $j_1 < j_2$ . On applique à la matrice  $B_{2 \rightarrow m}$  la méthode utilisée ci-dessus (étapes 1, 2 et 3), ce qui crée (en reportant les opérations sur la matrice  $A^{(1)}$ ) une matrice où nous avons un pivot  $a_{1j_1} = 1$  et  $a_{2j_2} = 1$ .

Étape 5 Avec une opération de type III (notamment  $A_1 \rightarrow -a_{1j_2}A_2 + A_1$ ), on annule le coefficient  $a_{1j_2}$  à la ligne 1, ce qui crée une matrice de la forme

$$A^{(2)} := \begin{pmatrix} 0 & \dots & 0 & \textcircled{1} & * & \dots & * & 0 & * & \dots & * \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & \textcircled{1} & * & \dots & * \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & * & \dots & * \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & * & \dots & * \end{pmatrix},$$

Notez que cette dernière opération ne modifie pas les éléments sur la première ligne précédant la colonne  $j_2$ , car tous les coefficients correspondants sur la ligne 2 sont nuls.

Étape 6 On répète ce procédé jusqu'à ce qu'on obtienne une matrice échelonnée réduite, disons  $A^{(k)}$ , telle que soit  $k = m$ , soit la matrice  $B_{k \rightarrow m}$  constituée des lignes  $k$  à  $m$  de  $A^{(k)}$  est la matrice nulle.

AZ: **▲** Dans la preuve, on abuse légèrement de la notation et après chaque opération élémentaire, on appelle encore les coefficients de la matrice résultante  $a_{ij}$ .

AZ: L'unicité de  $R$  découle de sa construction et sera admise sans preuve.

□

**Exemple 12.1.2.** Considérons la matrice  $A = \begin{pmatrix} 0 & 1 & 0 & 2 \\ 3 & 4 & 1 & 2 \\ 1 & 1 & -1 & 0 \end{pmatrix} \in \mathbb{M}_{3 \times 4}(\mathbb{R})$ . On effectue les

opérations suivantes :

$$\begin{pmatrix} 0 & 1 & 0 & 2 \\ 3 & 4 & 1 & 2 \\ 1 & 1 & -1 & 0 \end{pmatrix} \xrightarrow{L_3 \leftrightarrow L_1} \begin{pmatrix} 1 & 1 & -1 & 0 \\ 3 & 4 & 1 & 2 \\ 0 & 1 & 0 & 2 \end{pmatrix} \xrightarrow{L_2 \leftrightarrow L_1} \begin{pmatrix} 1 & 1 & -1 & 0 \\ 0 & 1 & 0 & 2 \\ 3 & 4 & 1 & 2 \end{pmatrix} \xrightarrow{L_3 \rightarrow -3L_1 + L_3} \begin{pmatrix} 1 & 1 & -1 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 1 & 4 & 2 \end{pmatrix} \xrightarrow{L_1 \rightarrow -L_2 + L_1} \\ \begin{pmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 0 & 2 \\ 0 & 1 & 4 & 2 \end{pmatrix} \xrightarrow{L_3 \rightarrow -L_2 + L_3} \begin{pmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 4 & 0 \end{pmatrix} \xrightarrow{L_3 \rightarrow 1/4 \times L_3} \begin{pmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix} \xrightarrow{L_1 \rightarrow L_3 + L_1} \begin{pmatrix} 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

**Corollaire 12.1.3.** Soit  $A \in \mathbb{M}_{m \times n}(K)$ . Alors il existe une matrice inversible  $P \in \text{GL}(m, K)$  telle que  $PA$  est échelonnée réduite.

**Exemple 12.1.4.** Dans l'Exemple 12.1.2 on a que  $P$  est la matrice :

$$\begin{aligned}
 P &= \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1/4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
 &\cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \\
 &= \begin{pmatrix} 5 & 1 & 1 \\ -\frac{4}{4} & \frac{1}{4} & \frac{1}{4} \\ 1 & 0 & 0 \\ -\frac{1}{4} & \frac{1}{4} & -\frac{3}{4} \end{pmatrix}
 \end{aligned}$$

Notez qu'on peut aussi trouver  $P = \begin{pmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{pmatrix}$  en résolvant le système linéaire suivant avec 12 équations à 9 inconnues :

$$\begin{aligned}
 0 \cdot p_{11} + 3 \cdot p_{12} + 1 \cdot p_{13} &= 1 \\
 1 \cdot p_{11} + 4 \cdot p_{12} + 1 \cdot p_{13} &= 0 \\
 0 \cdot p_{11} + 1 \cdot p_{12} - 1 \cdot p_{13} &= 0 \\
 2 \cdot p_{11} + 2 \cdot p_{12} + 0 \cdot p_{13} &= -2 \\
 \hline
 0 \cdot p_{21} + 3 \cdot p_{22} + 1 \cdot p_{23} &= 0 \\
 1 \cdot p_{21} + 4 \cdot p_{22} + 1 \cdot p_{23} &= 1 \\
 0 \cdot p_{21} + 1 \cdot p_{22} - 1 \cdot p_{23} &= 0 \\
 2 \cdot p_{21} + 2 \cdot p_{22} + 0 \cdot p_{23} &= 2 \\
 \hline
 0 \cdot p_{31} + 3 \cdot p_{32} + 1 \cdot p_{33} &= 0 \\
 1 \cdot p_{31} + 4 \cdot p_{32} + 1 \cdot p_{33} &= 0 \\
 0 \cdot p_{31} + 1 \cdot p_{32} - 1 \cdot p_{33} &= 1 \\
 2 \cdot p_{31} + 2 \cdot p_{32} + 0 \cdot p_{33} &= 0
 \end{aligned}$$

Puisque, parmi ces équations, il y a exactement 9 qui ne sont pas redondantes, ce système a une solution unique.

**Remarque 10. ▲** En général, la matrice  $P$  n'est pas unique. Par exemple, la matrice

$$A = \begin{pmatrix} 0 & 0 & 3 & 2 & 1 \\ 0 & 2 & 2 & -1 & 0 \\ 0 & 2 & 5 & 1 & 1 \\ 0 & 4 & 4 & -2 & 0 \end{pmatrix} \text{ est ligne équivalente à } R = \begin{pmatrix} 0 & 1 & 0 & -7/6 & -1/3 \\ 0 & 0 & 1 & 2/3 & 1/3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Si je considère les matrices  $P_1 = \begin{pmatrix} -1/3 & 1/2 & 0 & 0 \\ 1/3 & 0 & 0 & 0 \\ -1 & -1 & 1 & 0 \\ 0 & -2 & 0 & 1 \end{pmatrix}$  et  $P_2 = \begin{pmatrix} 0 & 0 & -1/3 & 5/12 \\ 0 & 0 & 1/3 & -1/6 \\ 0 & 1 & 0 & -1/2 \\ 1 & 0 & -1 & 1/2 \end{pmatrix}$ ,

alors  $P_1A = P_2A = R$ .

En tout cas, une matrice  $P$  telle que  $PA = R$  est entièrement déterminée par la séquence d'opérations élémentaires donnée dans la preuve du Théorème 12.1.1 que nous avons choisi de suivre (dans le cas où il y a place pour des choix).

## 12.2 Pour réfléchir chez vous

**Exercice 12.2.1.** Considérez la matrice

$$A = \begin{pmatrix} 1 & 4 & -8 & -5 & 10 \\ 1 & 1 & -4 & -3 & 5 \\ -1 & 2 & 0 & 1 & 0 \end{pmatrix}.$$

Déterminer si les lignes  $A_1, A_2, A_3$  de  $A$ , considérées comme des vecteurs dans  $\mathbb{M}_{1 \times 5}(\mathbb{R})$ , sont libres ou non, et trouver la dimension du sous-espace  $\text{Vect}(A_1, A_2, A_3) \leq \mathbb{M}_{1 \times 5}(\mathbb{R}) \simeq \mathbb{R}^5$ .

**Exercice 12.2.2.** Considérez la matrice

$$B = \begin{pmatrix} 0 & 2 & 0 \\ 1 & 1 & -1 \\ -1 & 1 & 1 \end{pmatrix}.$$

(i) Montrez que  $B$  est ligne équivalente à matrice échelonnée réduite  $R = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ .

(ii) Montrez que  $\left\{ \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} \right\}$  est une base du sous-espace de  $\mathbb{M}_{3 \times 1}(\mathbb{R}) \simeq \mathbb{R}^3$  engendré par les colonnes de  $B$ .

(iii) Décrire le sous-espace de  $\mathbb{M}_{3 \times 1}(\mathbb{R}) \simeq \mathbb{R}^3$  engendré par les colonnes de  $R$ .

(iv) Déduisez que les opérations élémentaires sur les lignes peuvent modifier l'espace engendré par les colonnes d'une matrice.

## Cours 15

---

### 13.1 Applications de la méthode de Gauss

On fixe un corps  $K$ .

### 13.1.1 Systèmes d'équations linéaires

Étant donné un système linéaire avec  $m$  équations à  $n$  inconnues :

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + \dots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n &= b_m, \end{aligned}$$

où  $a_{ij}, b_i \in K$ , on souhaite résoudre l'équation matricielle correspondante  $AX = B$ , c.-à-

d., on pose  $A = (a_{ij}) \in \mathbb{M}_{m \times n}(K)$  la matrice des coefficients,  $X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$  le vecteur des

inconnues, et  $B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$  le vecteur des termes constants.

Tout d'abord, on observe que la matrice  $A$  représente une (unique) application linéaire  $\varphi : K^n \rightarrow K^m$  (par rapport aux bases canoniques des deux espaces). Donc, l'existence d'une solution signifie qu'il existe  $x = (x_1, \dots, x_n) \in K^n$  tel que  $\varphi(x) = \underbrace{(b_1, \dots, b_m)}_{:=b} \in K^m$ . C'est-à-

dire que  $b$  appartient à l'image de  $\varphi$ . Donc, si  $b \notin \text{im}(\varphi)$ , alors l'équation n'a aucune solution et si  $b \in \text{im}(\varphi)$ , alors il existe au moins une solution. Dans le cas particulier où  $b = (0, \dots, 0)$ , il existe au moins une solution car  $\varphi(0) = 0$ . Même l'ensemble des solutions est égal au noyau de  $\varphi$ .

**Corollaire 13.1.1.** *Si  $A$  est une matrice  $m \times n$  non nulle et  $m < n$ , alors le système homogène d'équations linéaires associé,  $AX = 0$ , a une solution non triviale.*

AZ: Notez : comme on peut considérer la multiplication (à gauche) par  $A$  comme une application linéaire  $\mathbb{M}_{n \times 1}(K) \simeq K^n \rightarrow \mathbb{M}_{m \times 1}(K) \simeq K^m$ , si  $m < n$ , alors cette application n'est pas injective, donc son noyau n'est pas trivial (voir Corollaire 8.1.5, cours 10). Mais la méthode reste nécessaire et est très utile pour trouver concrètement une telle solution.

*Démonstration.* Soit  $R = (R_{ij})$  une matrice échelonnée réduite, qui est ligne équivalente à  $A$ . Alors, les systèmes  $AX = 0$  et  $RX = 0$  ont les mêmes solutions. Si  $r$  est le nombre de lignes de  $R$ , alors  $r \leq m$ , et puisque  $m < n$ , on a  $r < n$ . Maintenant, on observe que le système  $RX = 0$  a exactement  $r$  équations non triviales. Si nous supposons que l'entrée non nulle de la ligne  $i$  apparaît dans la colonne  $j_i$ , alors ces équations sont :

$$\begin{aligned} x_{j_1} + \sum_{j=j_1+1}^n R_{1j}x_j &= 0 \\ &\vdots \\ x_{j_r} + \sum_{j=j_r+1}^n R_{rj}x_j &= 0 \end{aligned}$$

Pourquoi ?

En plus, on observe que pour  $1 \leq i \leq r$  et pour  $j_i < j \leq n$  on a que  $R_{ij} = 0$  si  $j \in \{j_{i+1}, \dots, j_r\}$ , donc si  $y_1, \dots, y_{n-r}$  désignent les  $n - r$  inconnues différentes de  $x_{j_1}, \dots, x_{j_r}$ , ces équations peuvent être réécrites comme suit :

$$\begin{aligned} x_{j_1} + \sum_{j=1}^{n-r} \lambda_{1j} y_j &= 0 \\ &\vdots \\ x_{j_r} + \sum_{j=1}^{n-r} \lambda_{rj} y_j &= 0, \end{aligned}$$

Mais alors, comme toutes les solutions du système d'équations  $RX = 0$  sont obtenues en attribuant n'importe quelle valeur à  $y_1, \dots, y_{n-r}$  et puis en calculant les valeurs correspondantes de  $x_{j_1}, \dots, x_{j_r}$ , il s'ensuit qu'il y aura toujours une solution non triviale : puisque  $r < n$ , on peut choisir  $x_j = y_j$  qui ne fait pas partie des  $r$  inconnues  $x_{j_1}, \dots, x_{j_r}$ , et on peut alors construire une solution avec  $x_j = 1$ .  $\square$

**Définition 13.1.2.** Dans la preuve du Corollaire 13.1.1, les inconnues  $x_{j_1}, \dots, x_{j_r}$  qui apparaissent aux échelons du système échelonné réduit  $RX = 0$ , s'appellent les inconnues principales et les autres  $y_1, \dots, y_{n-r}$  (s'il y en a) s'appellent les inconnues libres.

**Exemple 13.1.3.** Considérons la matrice  $A = \begin{pmatrix} 1 & 2 & 3 & 2 \\ 0 & 2 & 3 & 1 \\ 2 & 5 & 6 & 0 \end{pmatrix} \in \mathbb{M}_{3 \times 4}(\mathbb{R})$ . Alors, cette matrice est ligne équivalente à la matrice échelonnée réduite suivante :

$$R = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -4 \\ 0 & 0 & 1 & 3 \end{pmatrix} \in \mathbb{M}_{3 \times 4}(\mathbb{R}).$$

Donc toutes les solutions du système  $AX = 0$  ont la forme  $X = \begin{pmatrix} -x_4 \\ 4x_4 \\ -3x_4 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_4 \begin{pmatrix} -1 \\ 4 \\ -3 \\ 1 \end{pmatrix}$ ,

où  $x_4 \in \mathbb{R}$ .

En posant  $x_4 = 1$ , on obtient la solution non triviale  $(x_1, x_2, x_3, x_4) = (-1, 4, -3, 1)$ . Nous pouvons facilement vérifier que

$$\begin{pmatrix} 1 & 2 & 3 & 2 \\ 0 & 2 & 3 & 1 \\ 2 & 5 & 6 & 0 \end{pmatrix} \cdot \begin{pmatrix} -1 \\ 4 \\ -3 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

**Exemple 13.1.4.** Considérons la matrice  $A = \begin{pmatrix} 0 & 0 & 3 & 2 & 1 \\ 0 & 2 & 2 & -1 & 0 \\ 0 & 2 & 5 & 1 & 1 \\ 0 & 4 & 4 & -2 & 0 \end{pmatrix} \in \mathbb{M}_{4 \times 5}(\mathbb{R})$ . Alors, cette

matrice est ligne équivalente à la matrice échelonnée réduite suivante :

$$R = \begin{pmatrix} 0 & 1 & 0 & -7/6 & -1/3 \\ 0 & 0 & 1 & 2/3 & 1/3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in \mathbb{M}_{4 \times 5}(\mathbb{R}).$$

Donc toutes les solutions du système  $AX = 0$  ont la forme

$$X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_4 \begin{pmatrix} 0 \\ 7/6 \\ -2/3 \\ 1 \\ 0 \end{pmatrix} + x_5 \begin{pmatrix} 0 \\ 1/3 \\ -1/3 \\ 0 \\ 1 \end{pmatrix}$$

où  $x_1, x_4, x_5 \in \mathbb{R}$ , car les deux équations non triviales sont :

$$0 \cdot x_1 + 1 \cdot x_2 + 0 \cdot x_3 + (-7/6) \cdot x_4 + (-1/3) \cdot x_5 = 0$$

et

$$0 \cdot x_1 + 0 \cdot x_2 + 1 \cdot x_3 + (2/3) \cdot x_4 + (1/3) \cdot x_5 = 0.$$

Quelle est la méthode, en général, pour trouver les solutions du système  $AX = B$  ?

**Méthode :** Pour résoudre  $AX = B$  par la méthode de Gauss, on forme la matrice augmentée du système  $(A|B)$ , où  $B$  est ajoutée en tant que dernière colonne. Ensuite, on réduit cette nouvelle matrice à sa forme échelonnée réduite  $(R|\tilde{B})$ .

**Définition 13.1.5.** Soit  $r$  le rang-ligne de la matrice  $R$ , et soient  $j_1, \dots, j_r$  les échelons de  $R$ . Les inconnues  $x_{j_1}, \dots, x_{j_r}$  s'appellent les inconnues principales et les autres (s'il y en a) s'appellent les inconnues libres (qui sont  $n - r$  en nombre).

**Description des solutions :**

Cas A Si l'un des nouveaux termes constants  $\tilde{b}_{r+1}, \dots, \tilde{b}_m$  n'est pas nul, disons  $\tilde{b}_i$ , alors l'équation  $0 \cdot x_1 + \dots + 0 \cdot x_m = 0 = \tilde{b}_i$  implique que le système n'a aucune solution.

Cas B Si  $\tilde{b}_{r+1} = \dots = \tilde{b}_m = 0$ , ou si  $r = m$ , le système possède au moins une solution. Pour décrire les solutions, on donne des valeurs arbitraires aux inconnues libres et on détermine la valeur de chaque inconnue principale en fonction d'inconnues libres. Donc s'il existe des inconnues libres, il y a plus d'une solution et s'il n'existe aucune inconnue libre ( $\iff r = n$ ), le système possède une solution unique.

**Exemple 13.1.6.** Considérons la matrice de coefficients  $A = \begin{pmatrix} -1 & -2 & 1 \\ 2 & 3 & 0 \\ 0 & 1 & -2 \end{pmatrix} \in \mathbb{M}_{3 \times 3}(\mathbb{R})$  et

le vecteur de termes constants  $B = \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix}$ . Alors, la matrice augmentée associée au système

$A \cdot X = B$  est la matrice  $\left( \begin{array}{ccc|c} -1 & -2 & 1 & -1 \\ 2 & 3 & 0 & 2 \\ 0 & 1 & -2 & 0 \end{array} \right)$ . De plus, cette matrice est ligne équivalente à matrice échelonnée réduite

$$\left( \begin{array}{ccc|c} 1 & 0 & 3 & 1 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right).$$

Cela implique que les solutions du système  $AX = B$  sont données par

$$\mathbb{M}_{3 \times 1}(\mathbb{R}) \ni X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + x_3 \begin{pmatrix} -3 \\ 2 \\ 1 \end{pmatrix} \quad \text{où } x_3 \in \mathbb{R} \text{ est quelconque.}$$

En revanche, notez que si nous considérons plutôt  $C = \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}$  comme le vecteur de termes constants, alors la matrice augmentée associée au système  $A \cdot X = C$  est ligne équivalente à matrice échelonnée réduite  $\left( \begin{array}{ccc|c} 1 & 0 & 3 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right)$ , et donc le système  $AX = C$  n'a aucune solution.

### 13.1.2 Base d'un sous-espace défini par un système de générateurs

#### Définition 13.1.7.

- (D1) Un système de vecteurs dans un  $K$ -espace vectoriel  $V$  est une liste (uplet) ordonnée de vecteurs  $(v_1, \dots, v_m)$  de  $V$ .
- (D2) On dit qu'un système de vecteurs  $(v_1, \dots, v_m)$ , avec  $v_i \in K^n$ , est échelonné (réduit) si la matrice  $m \times n$  dont la  $i$ -ème ligne contient les coordonnées de  $v_i$  est échelonnée (réduite).
- (D3) Pour un système de vecteurs  $(v_1, \dots, v_m)$  dans  $V$ ,  $\dim(\text{Vect}(v_1, \dots, v_m))$  s'appelle le rang du système. Notez que le rang du système  $(v_1, \dots, v_m)$  est le nombre maximal de vecteurs linéairement indépendants (libres) dans l'ensemble  $\{v_1, \dots, v_m\}$ .
- (D4) Soit  $A \in \mathbb{M}_{m \times n}(K)$ . On regarde les lignes  $A_1, \dots, A_m$  de  $A$  comme des vecteurs de  $K^n$  ou de  $\mathbb{M}_{1 \times n}(K)$ . On dit que le rang-ligne de  $A$  est le rang du système  $(A_1, \dots, A_m)$ . Notez que le rang-ligne de  $A$  est égal au rang-ligne de  $R$ , où  $R$  est la forme échelonnée réduite de  $A$ , et que le rang-ligne de  $R$  est le nombre d'échelons de  $R$ .

Soit  $(v_1, \dots, v_m)$  un système de vecteurs dans  $K^n$ . On souhaite :

- Trouver une base aussi simple que possible de  $U := \text{Vect}(v_1, \dots, v_m)$ .
- Trouver  $\dim(U)$ .
- Compléter cette base en une base de  $K^n$ .

---

### Méthode :

Étape 1 On écrit les coordonnées des vecteurs  $v_1, \dots, v_m$  dans les lignes d'une matrice  $A \in \mathbb{M}_{m \times n}$ , c'est-à-dire que si  $v_i = (a_{i1}, \dots, a_{in})$ , on pose  $A = (a_{ij}) \in \mathbb{M}_{m \times n}(K)$ , où  $A_i = (a_{i1} \ \dots \ a_{in})$ .

Étape 2 On effectue les opérations élémentaires sur les lignes de  $A$  pour la transformer en une matrice échelonnée réduite  $R$ .

Étape 3 On observe que si  $w_i \in K^n$  est le vecteur dont les coordonnées sont données par la  $i$ -ème ligne  $R_i$  de  $R$ , alors  $\text{Vect}(w_1, \dots, w_m) = U$ . Donc les vecteurs non nuls  $w_i$  forment une base de  $U$ .

Étape 4 Pour compléter cette base en une base de  $K^n$ , on ajoute tous les vecteurs canoniques  $e_\ell$  tels que  $\ell$  n'est pas un échelon de la matrice  $R$ .

---

Plus généralement, soit  $V$  un  $K$ -espace vectoriel de dimension  $n$  avec base ordonnée  $B = (v_1, \dots, v_n)$ . On a un isomorphisme  $\varphi_B : V \rightarrow K^n$  donné par

$$v = \alpha_1 \cdot v_1 + \dots + \alpha_n \cdot v_n \mapsto (\alpha_1, \dots, \alpha_n)$$

Autrement dit, cette fonction associe à chaque  $v \in V$  son « vecteur de coordonnées » (par rapport à la base  $B$ ) dans  $K^n$  et a été beaucoup utilisée pendant le cours.

Soit maintenant  $(u_1, \dots, u_m)$  un système de vecteurs de  $V$ . Alors, comme  $\varphi$  est bijective, on a que  $\dim(\text{Vect}(u_1, \dots, u_m)) = \dim(\text{Vect}(\varphi(u_1), \dots, \varphi(u_m)))$ . De plus, nous savons que cette dimension est égale au rang-ligne de la matrice avec lignes données par  $\varphi(u_1), \dots, \varphi(u_m)$ . Ainsi, on peut utiliser la méthode développée ci-dessus pour déterminer une base de  $\text{Vect}(u_1, \dots, u_m)$  ainsi que pour compléter cette base en une base de  $V$ .

**Exemple 13.1.8.** Considérons le système  $(v_1, v_2, v_3)$  dans  $K^4$  où  $v_1 = (1, 0, -1, 0)$ ,  $v_2 = (1, 3, 1, -2)$  et  $v_3 = ()$ . On souhaite :

- Trouver une base aussi simple que possible de  $U := \text{Vect}(v_1, v_2)$ .
- Trouver  $\dim(U)$ .
- Compléter cette base en une base de  $K^4$ .

Étape 1 On considère la matrice

$$A = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 1 & 3 & 1 & -2 \\ 3 & 6 & 1 & -4 \end{pmatrix}$$

Étape 2 Cette matrice est ligne équivalente à la matrice échelonnée réduite

$$R = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & \frac{2}{3} & -\frac{2}{3} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Étape 3 Les vecteurs  $w_1 = (1, 0, -1, 0)$  et  $w_2 = (0, 1, 2/3, -2/3)$  forment une base de  $U$

Étape 4 Pour compléter cette base en une base de  $K^4$ , on ajoute les vecteurs de la base canonique  $e_3 = (0, 0, 1, 0)$  et  $e_4 = (0, 0, 0, 1)$ .

**Exemple 13.1.9.** Considérons maintenant l'espace vectoriel  $V = \mathbb{M}_{2 \times 2}(\mathbb{F}_3)$  sur le corps  $\mathbb{F}_3$  avec base ordonnée la base canonique

$B = \{E_{11}, E_{12}, E_{21}, E_{22}\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ . Considérons les vecteurs

$u_1 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$  et  $u_2 = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$ . L'isomorphisme  $\varphi_B : V \rightarrow (\mathbb{F}_3)^4$  déterminé par  $B$  est tel que  $u_1 \mapsto v_1 = (1, 1, 0, 0)$  et  $u_2 \mapsto v_2 = (1, 2, 0, 0)$ . Donc, comme

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

si nous posons  $w_1 = e_1 = (1, 0, 0, 0)$  et  $w_2 = e_2 = (0, 1, 0, 0)$ , on a que  $\{\varphi_B^{-1}(w_1), \varphi_B^{-1}(w_2)\} = \{E_{11}, E_{12}\}$  est une base de  $\text{Vect}(u_1, u_2)$ .

## Cours 16

---

On fixe un corps  $K$  et on continue avec les applications de la méthode de Gauss.

### 14.1 Le noyau et l'image d'une application linéaire

Soient  $V$  et  $W$  des espaces vectoriels de dimension finie sur  $K$ ,  $\varphi : V \rightarrow W$  une application  $K$ -linéaire, et  $B_V = (v_1, \dots, v_n)$  et  $B_W = (w_1, \dots, w_m)$  des bases ordonnées de  $V$  et  $W$  respectivement. On souhaite :

- Trouver une base aussi simple que possible de  $\ker(\varphi) \leq V$ , compléter cette base en une base de  $V$  et trouver  $\dim(\ker(\varphi))$ .
- Trouver une base aussi simple que possible de  $\text{im}(\varphi) \leq W$ , compléter cette base en une base de  $W$  et trouver  $\dim(\text{im}(\varphi))$ .

---

#### Méthode :

Étape 1 Nous considérons la matrice  $A := [\varphi]_{B_V, B_W} \in \mathbb{M}_{m \times n}(K)$  de l'application  $\varphi$  par rapport aux bases choisies.

Étape 2 Puisque  $\varphi(v) = 0_W \iff A \cdot [v]_{B_V} = 0$ , on résout l'équation  $AX = 0$ , et on observe que si le rang-ligne de  $A$  est égal à  $r$ , alors l'ensemble des solutions est un sous-espace vectoriel de  $\mathbb{M}_{n \times 1}(K)$  de dimension  $n - r$  (= nombre d'inconnues libres).

Étape 3 On trouve une base  $(u_1, \dots, u_{n-r})$  de ce sous-espace des solutions.

Étape 4 On utilise l'isomorphisme  $f_{B_V} : V \rightarrow \mathbb{M}_{n \times 1}(K)$  donné par  $v \mapsto [v]_{B_V}$  pour trouver une base  $\{\tilde{v}_1, \dots, \tilde{v}_{n-r}\}$  de  $\ker(\varphi)$  – nous considérons simplement les images inverses des vecteurs  $u_1, \dots, u_{n-r} \in \mathbb{M}_{n \times 1}(K)$  dans  $V$  sous l'isomorphisme. Autrement dit, on pose  $\tilde{v}_\ell = f_{B_V}^{-1}(\tilde{u}_\ell)$  pour  $\ell = 1, \dots, n - r$ .

Étape 5 On peut compléter cette base en une base de  $V$  en utilisant la méthode discutée pendant le cours 15.

Étape 6 Si  $\tilde{v}_{n-r+1}, \dots, \tilde{v}_{n-1}, \tilde{v}_n$  sont les vecteurs ajoutés dans Étape 5, alors en posant  $\tilde{w}_j := \varphi(\tilde{v}_{n-r+j})$ , on a que les vecteurs  $\tilde{w}_1, \dots, \tilde{w}_r$  forment une base de  $\text{im}(\varphi)$ .

Étape 7 On peut utiliser la méthode discutée pendant le cours 15 pour compléter cette base en une base de  $W$ .

Alternativement, l'étape 6 ci-dessus peut être remplacée par la suivante.

Étape 6' Si on note par  $c_j = (a_{1j}, \dots, a_{mj}) \in K^m$  le vecteur dont les coordonnées se trouvent dans la  $j$ -ième colonne de la matrice  $A = (a_{ij})$ , alors on peut considérer le système de vecteurs  $(c_1, \dots, c_n)$ . En utilisant la méthode du cours 15, on peut donc trouver une base  $\{\tilde{c}_1, \dots, \tilde{c}_r\}$  du sous-espace  $\text{Vect}(c_1, \dots, c_n) \leq K^m$ . On utilise l'isomorphisme  $f_{B_W} : W \rightarrow \mathbb{M}_{m \times 1}(K)$  donné par  $w \mapsto [w]_{B_W}$  pour trouver une base  $\tilde{w}_1, \dots, \tilde{w}_r$  de  $\text{im}(\varphi)$  – nous considérons simplement les images inverses des vecteurs  $\tilde{c}_1, \dots, \tilde{c}_r \in \mathbb{M}_{m \times 1}(K)$  dans  $W$  sous l'isomorphisme. C'est-à-dire qu'on pose  $\tilde{w}_k = f_{B_W}^{-1}(\tilde{c}_k)$  pour  $k = 1, \dots, r$ .

AZ: Les bases obtenues en utilisant Étape 6 ou Étape 6' ne sont pas nécessairement les mêmes.

AZ: En général, combien de bases possède un espace vectoriel ?

### 14.1.1 Quelques exemples

**Exemple 14.1.1.** Considérons une application linéaire  $\varphi : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  qui, par rapport aux bases canoniques, est représentée par la matrice

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 1 & 2 & -1 \\ 2 & 4 & -2 \end{pmatrix}.$$

Comme cette matrice  $A$  est ligne équivalente à la matrice échelonnée réduite

$$R = \begin{pmatrix} 1 & 2 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

on déduit que les vecteurs  $u_1 = (-2, 1, 0)$  et  $u_2 = (1, 0, 1)$  forment une base du noyau de  $\varphi$ . Pour trouver une base de  $\text{im}(\varphi)$ , on peut considérer la matrice  $B = A^t$  qui est ligne équivalente à la matrice

$$\tilde{R} = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

pour conclure que le vecteur  $\tilde{w}_1 = (1, 1, 2) = \varphi(e_1) = \varphi(1, 0, 0)$  forme une base de  $\text{im}(\varphi)$ . Notez que  $\{u_1, u_2, e_1\}$  est bien une base de  $\mathbb{R}^3$ .

**Exemple 14.1.2.** Considérons une application linéaire  $\psi : \mathbb{R}^2 \rightarrow \mathbb{R}^3$  qui, par rapport aux bases canoniques, est représentée par la matrice

$$A = \begin{pmatrix} 1 & 2 \\ 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Comme cette matrice  $A$  est ligne équivalente à la matrice échelonnée réduite

$$R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix},$$

on déduit que  $\psi$  est injective. Pour trouver une base de  $\text{im}(\psi)$ , on peut considérer la matrice  $B = A^t$  qui est ligne équivalente à la matrice

$$\tilde{R} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

pour conclure que les vecteurs  $\tilde{w}_1 = (1, 0, 1)$  et  $\tilde{w}_2 = (0, 1, 2)$  forment une base de  $\text{im}(\psi)$ . Alternativement, on pourrait également considérer les vecteurs  $(1, 0, 1)$  et  $(2, -1, 0) = 2\tilde{w}_1 - \tilde{w}_2$ .

AZ: Pour réfléchir : Quelles sont les opérations élémentaires que l'on effectue sur les lignes de la matrice  $B$  pour obtenir la matrice  $\tilde{R}$ ?

**Exemple 14.1.3.** Supposons que  $K$  est un corps de caractéristique zéro<sup>2</sup>, par exemple  $K = \mathbb{R}, \mathbb{Q}$  ou  $\mathbb{C}$ . Considérons les espaces  $V = K[x]_{\leq 3}$  et  $W = K[x]_{\leq 2}$  et l'application linéaire  $D : V \rightarrow W$  définie par

$$a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0 \mapsto 3a_3 \cdot x^2 + 2a_2 \cdot x + a_1.$$

Soient  $B_V = (1, x, x^2, x^3)$  et  $B_W = (1, x, x^2)$  des bases canoniques (ordonnées) de  $V$  et  $W$  respectivement. Alors,

$$A = [D]_{B_V, B_W} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

et en posant  $u_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$  on a que l'espace de solutions de l'équation  $AX = 0$  est égal à  $\text{Vect}(u_1)$ .

Comme l'isomorphisme  $f_{B_V} : V = K[x]_{\leq 3} \rightarrow \mathbb{M}_{4 \times 1}(K)$  défini par  $v \mapsto [v]_{B_V}$  associe à chaque polynôme  $a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0$  le vecteur colonne  $\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}$ , on déduit que le

---

2. C'est-à-dire qu'aucun entier positif  $n$  ne vérifie l'égalité  $n \cdot 1_K = 0_K$

vecteur  $1 = f_{B_V}^{-1}(u_1)$  forme une base de  $\ker(D) \leq V = K[x]_{\leq 3}$ . On peut compléter cette base en une base de  $V$  en ajoutant les vecteurs  $x, x^2$  et  $x^3$  et on sait donc que les vecteurs  $1 = D(x), 2x = D(x^2)$  et  $3x^2 = D(x^3)$  forment une base de  $\text{im}(D) = W$ .

Que se passe-t-il si, au contraire, nous considérons  $K = \mathbb{F}_2$  ou  $K = \mathbb{F}_3$  ?

## 14.2 Le rang d'une application linéaire

### Définition 14.2.1.

- Soit  $A = (a_{ij}) \in \mathbb{M}_{m \times n}(K)$ . On note par  $c_j = (a_{1j}, \dots, a_{mj}) \in K^m$  le vecteur dont les coordonnées se trouvent dans la  $j$ -ième colonne de  $A$ . Le **rang-colonne** de  $A$  est la dimension de l'espace  $\text{Vect}(c_1, \dots, c_n)$  comme sous-espace de  $K^m$ .
- Rappelez-vous que si  $B \in \mathbb{M}_{m \times n}(K)$ , alors la transposée de  $B$ , notée  $B^t$ , est la matrice  $n \times m$  telle que  $(B^t)_{ij} = B_{ji}$ . Donc, le rang-colonne de  $B$  est égal au rang-ligne de  $B^t$  et le rang-ligne de  $B$  est égal au rang-colonne de  $B^t$ .

AZ: Notez que le rang-colonne d'une matrice  $A = (a_{ij}) \in \mathbb{M}_{m \times n}(K)$  est égal à la dimension de l'image de l'application linéaire  $\varphi_A : \mathbb{M}_{n \times 1}(K) \rightarrow \mathbb{M}_{m \times 1}(K)$  définie par

$$\varphi_A : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

AZ: De plus, si  $B_{\text{can}}$  et  $C_{\text{can}}$  notent les bases canoniques de  $K^n$  et de  $K^m$  respectivement, alors le rang-colonne d'une matrice  $A = (a_{ij}) \in \mathbb{M}_{m \times n}(K)$  est aussi égal à la dimension de l'image de l'application linéaire  $\psi : K^n \rightarrow K^m$  telle que  $[\psi]_{B_{\text{can}}, C_{\text{can}}} = A$

En particulier, si  $V$  et  $W$  sont des espaces vectoriels de dimension finie sur  $K$ ,  $\varphi : V \rightarrow W$  est une application  $K$ -linéaire,  $B_V$  et  $B_W$  sont des bases ordonnées de  $V$  et  $W$  respectivement, et on pose  $A = [\varphi]_{B_V, B_W}$ , alors  $\dim(\text{im}(\varphi))$  est précisément le rang-colonne de  $A$ .

**Théorème 14.2.2.** Soit  $A = (a_{ij}) \in \mathbb{M}_{m \times n}(K)$ . Le rang-ligne de  $A$  est égal au rang-colonne de  $A$ .

*Démonstration.* Posons  $r =$  le rang-ligne de  $A$  et considérons  $\varphi_A : \mathbb{M}_{n \times 1}(K) \rightarrow \mathbb{M}_{m \times 1}(K)$  l'application linéaire définie par la multiplication (à gauche) par  $A$ . Alors, comme  $\ker(\varphi_A)$  est de dimension  $n - r$ , le théorème du rang implique que le rang-ligne de  $A$  est égal au rang-colonne de  $A$ . □

Pourquoi ?

**Corollaire 14.2.3.** Soient  $V$  et  $W$  des espaces vectoriels de dimension finie sur  $K$ ,  $\varphi \in \mathcal{L}(V, W)$ , et  $B_V$  et  $B_W$  des bases ordonnées de  $V$  et  $W$  respectivement. Posons  $A = [\varphi]_{B_V, B_W}$ . Alors,

$$\begin{aligned} \dim(\text{im}(\varphi)) &= \text{rang-ligne}(A) = \text{rang-colonne}(A) = \\ &= \text{rang-ligne}(A^t) = \text{rang-colonne}(A^t) = \\ &= \dim(\text{im}(\varphi^t)) \end{aligned}$$

### 14.2.1 Lien avec l'application transposée

Soient  $V$  et  $W$  des espaces vectoriels de dimension finie sur  $K$ ,  $T \in \mathcal{L}(V, W)$ , et  $B_V$  et  $B_W$  des bases ordonnées de  $V$  et  $W$  respectivement. Considérons aussi les bases duales correspondantes  $B_V^*$  et  $B_W^*$ , ainsi que l'application transposée  $T^t \in \mathcal{L}(W^*, V^*)$ . Nous pouvons prouver ce qui suit.

- (a)  $\ker(T^t) = \text{im}(T)^\perp$
- (b)  $\dim(\ker(T^t)) = \dim(\ker(T)) + \dim(W) - \dim(V)$
- (c)  $\text{im}(T^t) = (\ker(T))^\perp$

En particulier, si on combine le point (b) ci-dessus avec le théorème du rang appliqué à la fois à  $T$  et à  $T^t$ , on déduit que  $\dim(\text{im}(T)) = \dim(\text{im}(T^t))$  et donc on obtient une autre preuve du Théorème 14.2.2. Comment prouver (a), (b) et (c) ?

(a)

$$\begin{aligned} \varphi \in \ker(T^t) &\iff T^t(\varphi) = \varphi \circ T = 0_{V^*} \quad (\text{la forme linéaire nulle}) \\ &\iff \varphi(T(v)) = 0_K \quad \forall v \in V \\ &\iff \varphi \in (\text{im}(T))^\perp = \{ \psi \in W^* = \mathcal{L}(W, K) \mid \forall w \in \text{im}(T), \psi(w) = 0_K \} \end{aligned}$$

(b)

$$\begin{aligned} \dim(\ker(T^t)) &= \dim((\text{im}(T))^\perp) \\ &= \dim(W) - \dim(\text{im}(T)) \\ &= \dim(W) - (\dim(V) - \dim(\ker(T))) \\ &= \dim(\ker(T)) + \dim(W) - \dim(V) \end{aligned}$$

(c)

$$\begin{aligned} \psi \in \text{im}(T^t) \leq V^* &\Rightarrow \exists \varphi \in W^* \text{ tel que } T^t(\varphi) = \psi \\ &\Rightarrow \forall v \in V, \psi(v) = \varphi(T(v)) \\ &\Rightarrow \forall v \in \ker(T), \psi(v) = \varphi(0_W) = 0_K \\ &\Rightarrow \psi \in (\ker(T))^\perp \end{aligned}$$

Donc,  $\text{im}(T^t) \subset (\ker(T))^\perp$ . Mais comme (b) implique que  $\dim(\text{im}(T)) = \dim(\text{im}(T^t))$  on a que

$$\dim(\text{im}(T^t)) = \dim(\text{im}(T)) = \dim(V) - \dim(\ker(T)) = \dim(\ker(T)^\perp).$$

Ainsi,  $\text{im}(T^t) = (\ker(T))^\perp$ .

### 14.3 Pour réfléchir chez vous

**Exercice 14.3.1.** Soit  $V$  un  $K$ -espace vectoriel de dimension finie et  $U \leq V$  un sous-espace. Prouvez que

$$\dim(U^\perp) = \dim(V) - \dim(U).$$

**Exercice 14.3.2.** Pour chaque vecteur non nul  $v = (v_1, \dots, v_n) \in K^n$ , considérez la forme linéaire  $\eta_v : K^n \rightarrow K$  définie par  $u = (u_1, \dots, u_n) \mapsto v_1 \cdot u_1 + \dots + v_n \cdot u_n$ . Soient  $T \in \mathcal{L}(K^n, K^m)$  et  $A = (a_{ij}) \in \mathbb{M}_{m \times n}(K)$  la matrice de  $T$  par rapport aux bases canoniques de  $K^n$  et de  $K^m$ . Pour chaque  $i = 1, \dots, m$ , posons  $a_i = (a_{i1}, \dots, a_{in}) \in K^n$  le vecteur dont les coordonnées se trouvent dans la  $i$ -ème ligne de  $A$ . Montrez que  $\ker(T) = \ker(\eta_{a_1}) \cap \dots \cap \ker(\eta_{a_m})$ .

**Exercice 14.3.3.** Utilisez l'exercice précédent pour donner une description géométrique du noyau de la transformation linéaire  $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ , dont la matrice par rapport aux bases canoniques est  $A = \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix}$ ,

## Cours 17

---

On continue avec les applications de la méthode de Gauss.

Comme d'habitude, nous fixons un corps  $K$ .

### 15.1 Inversion de matrices carrées

**Théorème 15.1.1** (Critère d'inversibilité). *Soit  $A = (a_{ij}) \in \mathbb{M}_{n \times n}(K)$  une matrice carrée. Les conditions suivantes concernant  $A$  sont équivalentes.*

- (i)  $A$  est inversible.
- (ii) La matrice échelonnée réduite qui est ligne équivalente à  $A$  est la matrice identité  $I_n$ .
- (iii) Il existe  $C \in \mathbb{M}_{n \times n}(K)$  telle que  $AC = I_n$ .
- (iv) Il existe  $B \in \mathbb{M}_{n \times n}(K)$  telle que  $BA = I_n$ .
- (v) Le système  $AX = 0$  possède une solution unique, la solution triviale.
- (vi) Le rang (= rang-ligne = rang-colonne) de  $A$  est égal à  $n$ .

*Démonstration.*

(i)  $\Rightarrow$  (iii) Par définition.

(i)  $\Rightarrow$  (iv) Par définition.

(iii)  $\Rightarrow$  (i) Notons  $E$  la base canonique de  $K^n$  et considérons les applications linéaires  $\varphi, \psi \in \mathcal{L}(K^n, K^n)$  telles que  $[\varphi]_{E,E} = A$  et  $[\psi]_{E,E} = C$ . Alors, l'égalité  $AC = I_n$  implique que  $\varphi \circ \psi = \text{id}$  ce qui implique en outre que  $\varphi$  est surjective, car  $K^n = \text{im}(\underbrace{\varphi \circ \psi}_{=\text{id}}) \subset \text{im}(\varphi)$ .

Mais alors,  $\varphi$  est bijective (Corollaire 8.1.7, cours 10) et donc  $A$  est inversible (Exercice 2, Série 7).

(iv)  $\Rightarrow$  (i) L'argument est très similaire à celui du point précédent. Nous utilisons les mêmes notations et considérons maintenant l'application linéaire  $\gamma \in \mathcal{L}(K^n, K^n)$  telle que  $[\gamma]_{E,E} = B$ . Alors, l'égalité  $BA = I_n$  implique que  $\gamma \circ \varphi = \text{id}$ , ce qui implique en outre que  $\varphi$  est injective, car  $\{0\} = \ker(\underbrace{\gamma \circ \varphi}_{=\text{id}}) \supset \ker(\varphi)$ . Mais alors,  $\varphi$  est bijective (Corollaire 8.1.7, cours 10) et donc  $A$  est inversible (Exercice 2, Série 7).

- (i)  $\Rightarrow$  (v) Supposons que  $A$  est inversible avec inverse  $A^{-1}$ . On considère l'équation  $AX = 0$ ; on multiplie à gauche par  $A^{-1}$  des deux côtés et on obtient qu'il n'existe que la solution triviale  $X = 0$ .
- (v)  $\Rightarrow$  (vi) On sait que la dimension de l'espace des solutions du système est égale à  $n - r$ , où  $r$  est le rang de  $A$ . Mais l'espace des solutions est le sous-espace nul et donc de dimension 0. On déduit que  $n = r$ , c.-à-d. que la matrice  $A$  est de rang  $n$ .
- (vi)  $\Rightarrow$  (ii) Supposons maintenant que le rang de  $A$  est égal à  $n$ . On effectue les opérations élémentaires sur les lignes de  $A$  pour obtenir une matrice échelonnée réduite  $R$ . Comme le rang de  $R$  est aussi  $n$ , on déduit que  $R = I_n$ .
- (ii)  $\Rightarrow$  (iv) Si  $A$  est ligne équivalente à  $I_n$ , alors il existe des matrices élémentaires  $E_1, \dots, E_k$  telles que  $E_1 \cdot \dots \cdot E_k \cdot A = I_n$ . Autrement dit, nous pouvons prendre  $B = E_1 \cdot \dots \cdot E_k$ . Cette matrice satisfait à la condition de (iv). □

**Corollaire 15.1.2.** *Toute matrice inversible est égale à un produit de matrices élémentaires.*

Ces résultats nous permettent de déterminer si une matrice donnée est inversible et de trouver l'inverse lorsqu'elle existe.

---

**Méthode :** Pour déterminer si une matrice  $A \in \mathbb{M}_{n \times n}(K)$  est inversible, et pour trouver son inverse lorsqu'elle existe, on construit une matrice augmentée en plaçant la matrice originale  $A$  à gauche et la matrice identité  $I_n$  à droite. On applique ensuite des opérations élémentaires aux lignes de cette matrice augmentée pour transformer  $A$  en une matrice échelonnée réduite  $R$ . Si  $A$  est inversible, alors  $R = I_n$  et le membre de droite de la matrice augmentée finale sera exactement l'inverse de  $A$ . Si  $R \neq I_n$ , alors on sait que  $A$  n'est pas inversible.

---

**Exemple 15.1.3.** Considérons la matrice  $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix} \in \mathbb{M}_{3 \times 3}(\mathbb{R})$ . Alors, la matrice augmentée

$$\left( \begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array} \right)$$

est ligne équivalente à la matrice

$$\left( \begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & 1 & -1 \\ 0 & 1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array} \right).$$

Par conséquent,  $A$  est inversible et

$$A^{-1} = \begin{pmatrix} 2 & 1 & -1 \\ -1 & 0 & 1 \\ -1 & -1 & 1 \end{pmatrix}.$$

## 15.2 Matrice de changement de base

Une fois que l'on sait inverser les matrices, cela nous donne un outil pour déterminer les matrices de changement de base.

**Exemple 15.2.1.** Soit  $\mathcal{B} = (e_1, e_2, e_3)$  la base canonique (ordonnée) de  $\mathbb{R}^3$  et considérons une autre base  $\mathcal{C} = (v_1, v_2, v_3)$  de  $\mathbb{R}^3$  telle que

$$\begin{cases} v_1 = (1, 2, 3) = 1 \cdot e_1 + 2 \cdot e_2 + 3 \cdot e_3 \\ v_2 = (0, 1, 1) = 0 \cdot e_1 + 1 \cdot e_2 + 1 \cdot e_3 \\ v_3 = (1, 0, -1) = 1 \cdot e_1 + 0 \cdot e_2 + (-1) \cdot e_3 \end{cases}$$

Alors, la matrice de passage  $[\text{id}]_{\mathcal{B}, \mathcal{C}} = P_{\mathcal{B} \rightarrow \mathcal{C}}$  est la matrice

$$\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ -1 & 2 & -1 \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 0 \\ 3 & 1 & -1 \end{pmatrix}^{-1}.$$

En effet, on a que

$$\begin{cases} e_1 = (1, 0, 0) = (1/2) \cdot v_1 + (-1) \cdot v_2 + (1/2) \cdot v_3 \\ e_2 = (0, 1, 0) = (-1/2) \cdot v_1 + 2 \cdot v_2 + (1/2) \cdot v_3 \\ e_3 = (0, 0, 1) = (1/2) \cdot v_1 + (-1) \cdot v_2 + (-1/2) \cdot v_3 \end{cases}.$$

Comment peut-on trouver des scalaires  $a_{ij} \in \mathbb{R}$  tels que  $e_j = a_{1j} \cdot v_1 + a_{2j} \cdot v_2 + a_{3j} \cdot v_3$ ? On peut résoudre l'équation

$$\begin{pmatrix} v_1 & v_2 & v_3 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \\ 3 & 1 & -1 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}}_{=P_{\mathcal{B} \rightarrow \mathcal{C}}} = \begin{pmatrix} e_1 & e_2 & e_3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

**Exemple 15.2.2.** Considérons des bases ordonnées  $\mathcal{B} = (v_1, v_2, v_3, v_4) = (2, 2x, 3x^2-1, x^3+1)$  et  $\mathcal{C} = (w_1, w_2, w_3, w_4) = (1, x-1, x^2+2, 2x^3)$  de  $\mathbb{R}[x]_{\leq 3}$ . Alors, la matrice de passage  $[\text{id}]_{\mathcal{B}, \mathcal{C}} = P_{\mathcal{B} \rightarrow \mathcal{C}}$  est la matrice  $A = (a_{ij}) \in \mathbb{M}_{4 \times 4}(\mathbb{R})$  telle que

$$\begin{matrix} & w_1 & w_2 & w_3 & w_4 \\ 1 & \begin{pmatrix} 1 & -1 & 2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} \\ x & \\ x^2 & \\ x^3 & \end{matrix} \cdot \underbrace{\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}}_{=P_{\mathcal{B} \rightarrow \mathcal{C}}} = \begin{matrix} & v_1 & v_2 & v_3 & v_4 \\ 1 & \begin{pmatrix} 2 & 0 & -1 & 1 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ x & \\ x^2 & \\ x^3 & \end{matrix}$$

C'est-à-dire que si on pose  $\mathcal{E} = (1, x, x^2, x^3)$ , alors

$$\begin{aligned} [\text{id}]_{\mathcal{B}, \mathcal{C}} = P_{\mathcal{B} \rightarrow \mathcal{C}} &= \begin{pmatrix} 1 & -1 & 2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 2 & 0 & -1 & 1 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ &= [\text{id}]_{\mathcal{C}, \mathcal{E}}^{-1} \cdot [\text{id}]_{\mathcal{B}, \mathcal{E}} \\ &= [\text{id}]_{\mathcal{E}, \mathcal{C}} \cdot [\text{id}]_{\mathcal{B}, \mathcal{E}}. \end{aligned}$$

Notez qu'on peut également résoudre chacun des quatre systèmes linéaires définis par des quatre équations  $v_j = a_{1j} \cdot w_1 + a_{2j} \cdot w_2 + a_{3j} \cdot w_3 + a_{4j} \cdot w_4$  :

$$\begin{pmatrix} 1 & -1 & 2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} a_{1j} \\ a_{2j} \\ a_{3j} \\ a_{4j} \end{pmatrix} = [v_j]_{\mathcal{E}}.$$

Cette méthode prend cependant généralement plus de temps.

### 15.3 Pour réfléchir chez vous

**Exercice 15.3.1.** Supposons que  $\mathcal{B} = (u_1, \dots, u_n)$  et  $\mathcal{C} = (v_1, \dots, v_n)$  soient des bases ordonnées d'un  $K$ -espace vectoriel  $V$ . Soit  $\varphi \in \mathcal{L}(V, V)$  telle que  $\varphi(v_i) = u_i$  pour chaque  $i = 1, \dots, n$ . Démontrer que

$$[\varphi]_{\mathcal{C}, \mathcal{C}} = [\text{id}]_{\mathcal{B}, \mathcal{C}}.$$

**Exercice 15.3.2.** Démontrer que les conditions du Théorème 15.1.1 sont équivalentes à la condition suivante : Pour tout  $(b_1, \dots, b_n) \in K^n$ , il existe une solution au système d'équations

$$\begin{cases} b_1 = \sum_{j=1}^n a_{1j} x_j \\ \vdots \\ b_n = \sum_{j=1}^n a_{nj} x_j \end{cases}.$$

## Cours 18

---

L'objectif des trois prochains cours est de définir rigoureusement la notion de déterminant des opérateurs linéaires (et des matrices). Si  $K$  est un corps et  $A = (a_{ij}) \in \mathbb{M}_{n \times n}(K)$  est une matrice carrée, alors le déterminant de  $A$ , désigné par  $\det(A)$ , sera défini de telle manière que :

- si l'on permute deux lignes ou deux colonnes de  $A$ , le déterminant  $\det(A) \in K$  change de signe ;

- si deux lignes ou deux colonnes de  $A$  sont identiques, le déterminant est nul ;
- on peut ajouter à une colonne (ou une ligne) de  $A$  un multiple d'une autre colonne (ou d'une autre ligne) sans changer la valeur du déterminant ;
- si l'on multiplie tous les termes d'une même ligne de  $A$  ou d'une même colonne par un scalaire  $\alpha$ , le déterminant est multiplié par  $\alpha$  ;
- en conséquence, si une ligne ou une colonne de  $A$  est nulle, le déterminant est nul.

De plus, on va voir que le déterminant se comporte bien avec le produit des matrices :

$$\det(AB) = \det(A) \cdot \det(B)$$

et, en fait, il définit un morphisme de groupes  $\det : \text{GL}(n, K) \rightarrow K^\times$ . En particulier, si  $A, B \in \mathbb{M}_{n \times n}(K)$  sont des matrices semblables, alors  $\det(A) = \det(B)$ .

En général, le déterminant d'une matrice carrée

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

peut être calculé en utilisant la formule de Leibniz :

$$\begin{aligned} \det(A) &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{j=1}^n a_{\sigma(j)j} \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n a_{i\sigma(i)} \end{aligned} \tag{2}$$

où  $S_n$  désigne le groupe de toutes les bijections (permutations) de  $\{1, 2, \dots, n\}$  et  $\varepsilon(\sigma)$  la signature de la permutation  $\sigma$ . Nous commençons donc par un exposé plus détaillé sur la structure du groupe  $S_n$ . En particulier, nous rappelons la définition de la signature d'une permutation.

AZ:  Notez que (2) nous dit que  $\det(A) = \det(A^t)$ .

## 16.1 Le groupe $S_n$

Rappelez-vous que si  $X = \{1, 2, \dots, n\}$ ,  $n$  étant un entier naturel positif, on appelle  $\text{Bij}(X)$  le **groupe symétrique de degré  $n$** , noté  $\mathfrak{S}_n$ ,  $\text{Sym}_n$ , ou simplement  $S_n$ . Pour chaque permutation  $\sigma \in S_n$  on écrit souvent

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}.$$

Pour éviter toute confusion avec les « matrices honnêtes », nous représenterons plutôt les permutations comme des produits de cycles et comme des produits de transpositions.

**Définition 16.1.1.**

(i) Une permutation  $\sigma \in S_n$  est appelée un **cycle** si  $\sigma$  est de la forme

$$\left( \begin{array}{ccccccc} a_1 & & & & & & \\ & \curvearrowright & & & & & \\ & & a_2 & & & & \\ & & & \curvearrowright & & & \\ & & & & a_3 & & \\ & & & & & \dots & \\ & & & & & & a_{\ell-1} & & \\ & & & & & & & \curvearrowright & \\ & & & & & & & & a_{\ell} \end{array} \right)$$

avec  $a_1, a_2, \dots, a_{\ell-1}, a_{\ell} \in \{1, 2, \dots, n\}$  distincts, ce qu'on note souvent de manière abrégée sans aucune flèche :

$$(a_1 \ a_2 \ \dots \ a_{\ell-1} \ a_{\ell}).$$

Implicitement, nous entendons également que les autres éléments sont tous fixes. Nous appelons  $\ell$  la longueur du cycle et le sous-ensemble  $\{a_1, \dots, a_{\ell}\} \subset \{1, \dots, n\}$  est appelé le support de la permutation.

(ii) Une permutation  $\sigma \in S_n$  est appelée une **transposition** si  $\sigma$  est un cycle de longueur deux.

Nous pouvons prouver ce qui suit.

**Théorème 16.1.2.**

(i) Toute permutation  $\sigma \in S_n$  peut être écrite de manière unique comme un produit commutatif :

$$\sigma = \sigma_1 \circ \dots \circ \sigma_k$$

de cycles de longueur au moins 2 à supports disjoints.

(ii) Le groupe  $S_n$  est engendré par les transpositions, car

$$(a_1 \ a_2 \ \dots \ a_{\ell-1} \ a_{\ell}) = (a_1 \ a_2) \circ (a_2 \ a_3) \circ \dots \circ (a_{\ell-1} \ a_{\ell}).$$

À partir de ce résultat, nous pouvons définir la signature  $\varepsilon : S_n \rightarrow \{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z}$ , qui est un morphisme des groupes. Si on écrit une permutation  $\sigma \in S_n$  comme un produit des transpositions  $\tau_1 \circ \dots \circ \tau_r$ , alors on a que sa signature est définie par  $\varepsilon(\sigma) := (-1)^r$ . On peut vérifier que cela est bien défini. C'est-à-dire que si  $\sigma = \tau_1 \circ \dots \circ \tau_r = \tilde{\tau}_1 \circ \dots \circ \tilde{\tau}_s$ , alors  $r \equiv s \pmod{2}$ .

**Exemple 16.1.3.** Considerons la permutation  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}$  dans le groupe symétrique  $S_5$ . Son écriture en cycles disjoints de longueur au moins 2 est  $(234) = (342) = (423)$ .

**Exemple 16.1.4.** L'écriture de  $\sigma = (1357)(2371)(23) \in S_8$  en produit de cycles disjoints de longueur au moins 2 est  $(12)(357) = (12)(573) = (12)(735)$ .

## 16.2 Le déterminant d'une matrice $2 \times 2$

Soit  $K$  un corps et  $A = (a_{ij}) \in \mathbb{M}_{2 \times 2}(K)$ . Comme  $S_2 = \{\text{id}, (12)\}$ , en utilisant (2), on déduit que

$$\det(A) = a_{11}a_{22} - a_{21}a_{12}$$

car  $\varepsilon(\text{id}) = 1$  et  $\varepsilon((12)) = -1$ .

AZ: Réfléchissez au lien avec exercice 5, série 4.

## 16.3 Le déterminant d'une matrice $3 \times 3$

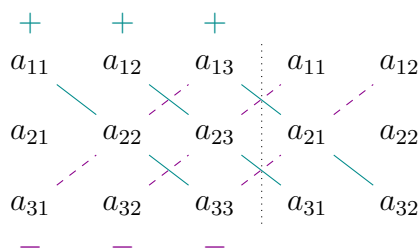
Soit  $K$  un corps et considérons

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in \mathbb{M}_{3 \times 3}(K).$$

Comme  $S_3 = \{\text{id}, (12), (13), (23), (123), (132)\}$ , en utilisant (2), on déduit que

$$\begin{aligned} \det(A) &= a_{11}a_{22}a_{33} - a_{21}a_{12}a_{33} - a_{31}a_{22}a_{13} - a_{11}a_{32}a_{23} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} \\ &= a_{11}(a_{22}a_{33} - a_{32}a_{23}) - a_{12}(a_{21}a_{33} - a_{31}a_{23}) + a_{13}(a_{21}a_{32} - a_{31}a_{22}) \\ &= a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} \end{aligned}$$

Alternativement, on peut calculer  $\det(A)$  en utilisant la règle de Sarrus :



## (★) Cours 19

---

### 17.1 Formes multilinéaires alternées

On fixe un corps  $K$  et un  $K$ -espace vectoriel  $V$  de dimension finie.

**Définition 17.1.1.** Pour  $m$  un entier positif, on pose  $V^m := \underbrace{V \times \dots \times V}_{m \text{ fois}}$ .

- (i) Une forme  $m$ -linéaire sur  $V$  est une fonction  $\alpha : V^m \rightarrow K$  qui est linéaire par rapport à chaque entrée lorsque les autres entrées sont fixées. Cela signifie que pour chaque  $k \in \{1, \dots, m\}$  et tous  $(u_1, \dots, u_m) \in V^m$ , la fonction

$$v \mapsto \alpha(u_1, \dots, u_{k-1}, v, u_{k+1}, \dots, u_m)$$

est  $K$ -linéaire (un élément de l'espace dual  $V^*$ ).

- (ii) L'ensemble des formes  $m$ -linéaires sur  $V$  sera noté  $\mathcal{L}^m(V, K)$ .

AZ: Dans la définition ci-dessus, l'expression  $\alpha(u_1, \dots, u_{k-1}, v, u_{k+1}, \dots, u_m)$  signifie  $\alpha(v, u_2, \dots, u_m)$  si  $k = 1$  et signifie  $\alpha(u_1, \dots, u_{m-1}, v)$  si  $k = m$ .

AZ: Une forme 1-linéaire sur  $V$  est une forme linéaire sur  $V$ . Une forme 2-linéaire sur  $V$  est une forme bilinéaire sur  $V$ .

AZ: De manière plus générale, étant donnés des  $K$ -espaces vectoriels  $V_1, \dots, V_m$  et  $W$ , et une application  $\alpha : V_1 \times \dots \times V_m \rightarrow W$ , on dit que  $\alpha$  est  $m$ -linéaire si  $\alpha$  est linéaire par rapport à chaque entrée.

AZ: **▲**  $\mathcal{L}^m(V, K) \neq \mathcal{L}(V^m, K)$  !!!

**Exemple 17.1.2.** Soit  $A = (a_{ij}) \in \mathbb{M}_{n \times n}(K)$ . On peut définir une forme 2-linéaire  $\beta_A$  sur  $K^n$  par

$$\begin{aligned} \beta_A(x, y) &= \beta_A((x_1, \dots, x_n), (y_1, \dots, y_n)) = \sum_{j=1}^n \sum_{i=1}^n a_{ij} x_i y_j \\ &= (x_1 \quad \dots \quad x_n) \cdot \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = x^t A y. \end{aligned}$$

Notez que  $\beta_A(e_i, e_j) = a_{ij}$  pour chaque  $1 \leq i, j \leq n$ . On peut prendre comme exemple concret,  $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{M}_{2 \times 2}(\mathbb{R})$ . Alors, la forme bilinéaire  $\beta_A$  sur  $\mathbb{R}^2$  est tout simplement le produit scalaire usuel.

AZ: Notez que si  $n = 1$  et  $A = I_1 \in \mathbb{M}_{1 \times 1}(K) \simeq K$ , alors on retrouve le produit dans  $K$ . C'était l'exemple donné par l'un.e d'entre vous.

**Remarque 11.** Si  $V = K^n$ , on peut identifier le produit cartésien  $K^n \times \dots \times K^n$  de  $n$  copies de  $K^n$  avec l'espace de matrices  $\mathbb{M}_{n \times n}(K)$ . Un élément  $(u_1, \dots, u_n) \in K^n \times \dots \times K^n$  est associé à la matrice dont la  $i$ -ème ligne est donnée par le vecteur  $u_i$ . Ou, de manière équivalente, il peut être associé à la matrice dont la  $j$ -ème colonne est donnée par le vecteur  $u_j$ . On peut donc parler des applications  $m$ -linéaires  $\alpha : \mathbb{M}_{n \times n}(K) \rightarrow K$  par rapport aux lignes ou aux colonnes.

**Définition 17.1.3.** Soit  $m$  un entier positif. Une application  $\alpha \in \mathcal{L}^m(V, K)$  est dite **alternée** si  $\alpha(u_1, \dots, u_m) = 0$  chaque fois que  $u_1, \dots, u_m$  est une liste de vecteurs de  $V$  avec  $u_i = u_j$  pour deux indices différents  $i, j \in \{1, \dots, m\}$ . L'ensemble des formes  $m$ -linéaires sur  $V$  qui sont alternées sera noté  $\mathcal{A}^m(V, K)$ .

Les affirmations suivantes découlent directement de cette définition :

- $\mathcal{A}^m(V, K)$  est un sous-espace vectoriel de  $\mathcal{F}(V^m, K)$ .
- Soit  $\alpha \in \mathcal{A}^m(V, K)$ . Si  $u_1, \dots, u_m \in V$  sont linéairement dépendants, alors  $\alpha(u_1, \dots, u_m) = 0$ .

AZ: Si  $u_1, \dots, u_m \in V$  sont linéairement dépendants, alors il existe  $i \in \{1, \dots, m\}$  tel que

$$u_i \in \text{Vect}(u_1, \dots, u_i) \Rightarrow u_i = \sum_{j=1}^{i-1} \lambda_j \cdot u_j \text{ (Cours 8, Lemme 6.1.4). Donc, on a}$$

$$\begin{aligned} \alpha(u_1, \dots, u_m) &= \alpha \left( u_1, \dots, u_{i-1}, \sum_{j=1}^{i-1} \lambda_j \cdot u_j, u_{i+1}, \dots, u_m \right) \\ &= \sum_{j=1}^{i-1} \lambda_j \alpha(u_1, \dots, u_{i-1}, u_j, u_{i+1}, \dots, u_m) \\ &= 0 \end{aligned}$$

- Si  $m > \dim(V)$ , alors la seule forme  $m$ -linéaire alternée sur  $V$  est l'application nulle  $(u_1, \dots, u_m) \mapsto 0_K$ .

AZ: Si  $m > \dim(V)$ , alors  $m$  vecteurs dans  $V$  sont toujours linéairement dépendants.

- Si  $\tau \in S_m$  est une transposition, alors  $\alpha(u_{\tau(1)}, \dots, u_{\tau(m)}) = -\alpha(u_1, \dots, u_m)$ . Autrement dit, l'échange des vecteurs dans deux entrées quelconques de  $\alpha(u_1, \dots, u_m)$  modifie le signe de la valeur de  $\alpha$ .

AZ: Supposons que  $\tau = (ij)$ , avec  $i < j$ . Alors,

$$\begin{aligned} 0 &= \alpha(u_1, \dots, \underbrace{u_i + u_j}_{i\text{-ème place}}, \dots, \underbrace{u_i + u_j}_{j\text{-ème place}}, \dots, u_m) = \alpha(u_1, \dots, u_i, \dots, u_i + u_j, \dots, u_m) + \\ &\quad + \alpha(u_1, \dots, u_j, \dots, u_i + u_j, \dots, u_m) \\ &= \alpha(u_1, \dots, u_i, \dots, u_i, \dots, u_m) + \alpha(u_1, \dots, u_i, \dots, u_j, \dots, u_m) + \\ &\quad + \alpha(u_1, \dots, u_j, \dots, u_i, \dots, u_m) + \alpha(u_1, \dots, u_j, \dots, u_j, \dots, u_m) \\ &= \alpha(u_1, \dots, u_i, \dots, u_j, \dots, u_m) + \alpha(u_1, \dots, u_j, \dots, u_i, \dots, u_m) \\ &= \alpha(u_1, \dots, u_m) + \alpha(u_{\tau(1)}, \dots, u_{\tau(m)}) \\ &\Rightarrow \alpha(u_{\tau(1)}, \dots, u_{\tau(m)}) = -\alpha(u_1, \dots, u_m) \end{aligned}$$

Nous en déduisons notamment le résultat suivant.

**Proposition 17.1.4.** Soient  $m$  un entier positif et  $\alpha \in \mathcal{A}^m(V, K)$ . Alors, pour chaque  $(u_1, \dots, u_m) \in V^m$  et pour chaque permutation  $\sigma \in S_m$  on a que

$$\alpha(u_{\sigma(1)}, \dots, u_{\sigma(m)}) = \varepsilon(\sigma) \cdot \alpha(u_1, \dots, u_m)$$

Ceci conduit naturellement à une formule pour les formes  $n$ -linéaires alternées sur un espace vectoriel  $V$  de dimension  $n$ .

**Théorème 17.1.5.** Soit  $\mathcal{B} = \{v_1, \dots, v_n\}$  une base de  $V$  et soient  $u_1, \dots, u_n \in V$  des vecteurs quelconques. Pour chaque  $j \in \{1, \dots, n\}$  soient  $a_{1j}, \dots, a_{nj} \in K$  des scalaires tels que  $u_j = \sum_{i=1}^n a_{ij}v_i$ . Alors, pour chaque  $\alpha \in \mathcal{A}^n(V, K)$  on a que  $\alpha(u_1, \dots, u_n) = \eta \cdot \alpha(v_1, \dots, v_n)$ , où

$$\eta = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{j=1}^n a_{\sigma(j)j}.$$

*Démonstration.* Prenons  $\alpha \in \mathcal{A}^n(V, K)$ . Alors,

$$\begin{aligned} \alpha(u_1, \dots, u_n) &= \alpha \left( \sum_{i=1}^n a_{i1}v_i, \dots, \sum_{i=1}^n a_{in}v_i \right) \\ &= \alpha \left( \sum_{i_1=1}^n a_{i_1 1}v_{i_1}, \dots, \sum_{i_n=1}^n a_{i_n n}v_{i_n} \right) \\ &= \sum_{i_1=1}^n a_{i_1 1} \cdot \alpha \left( v_{i_1}, \sum_{i_2=1}^n a_{i_2 2}v_{i_2}, \dots, \sum_{i_n=1}^n a_{i_n n}v_{i_n} \right) \\ &= \sum_{i_2=1}^n a_{i_2 2} \left( \sum_{i_1=1}^n a_{i_1 1} \cdot \alpha \left( v_{i_1}, v_{i_2}, \sum_{i_3=1}^n a_{i_3 3}v_{i_3}, \dots, \sum_{i_n=1}^n a_{i_n n}v_{i_n} \right) \right) \\ &\vdots \\ &= \sum_{i_n=1}^n \dots \sum_{i_1=1}^n a_{i_n n} \cdot \dots \cdot a_{i_1 1} \alpha(v_{i_1}, \dots, v_{i_n}) \\ &= \sum_{\sigma \in S_n} a_{\sigma(1)1} \cdot \dots \cdot a_{\sigma(n)n} \alpha(v_{\sigma(1)}, \dots, v_{\sigma(n)}) \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{j=1}^n a_{\sigma(j)j} \alpha(v_1, \dots, v_n) \end{aligned}$$

□

**Corollaire 17.1.6.** Si  $\dim(V) = n$ , alors  $\dim(\mathcal{A}^n(V, K)) = 1$ .

*Démonstration.* Prenons  $\alpha, \beta \in \mathcal{A}^n(V, K)$  avec  $\alpha$  non nulle (voir commentaire ci-dessous). Soient  $v_1, \dots, v_n \in V$  tels que  $\alpha(v_1, \dots, v_n) \neq 0$ . Alors, il existe  $\lambda \in K$  tel que

$$\beta(v_1, \dots, v_n) = \lambda \cdot \alpha(v_1, \dots, v_n)$$

Comme  $\{v_1, \dots, v_n\}$  doit être une base, alors en utilisant Théorème 17.1.5 deux fois (et les mêmes notations là) on peut écrire Pourquoi?

$$\begin{aligned} \beta(u_1, \dots, u_n) &= \eta \cdot \beta(v_1, \dots, v_n) \\ &= \eta \cdot (\lambda \cdot \alpha(v_1, \dots, v_n)) \\ &= \lambda \cdot (\eta \cdot \alpha(v_1, \dots, v_n)) \\ &= \lambda \cdot \alpha(u_1, \dots, u_n) \end{aligned}$$

pour chaque liste de  $n$  vecteurs  $u_1, \dots, u_n \in V$ . Ce qui implique que  $\beta = \lambda \cdot \alpha$ . Ainsi,  $\{\alpha, \beta\}$  n'est pas libre et donc  $\dim(\mathcal{A}^n(V, K)) \leq 1$ . La démonstration est complète dès lors que l'on peut effectivement montrer qu'il existe une telle forme  $\alpha$  alternée non nulle sur  $V$ .

En fait, si  $\mathcal{B} = \{v_1, \dots, v_n\}$  est une base de  $V$  et  $\mathcal{B}^* = \{\varphi_1, \dots, \varphi_n\}$  est la base duale, alors l'application  $\alpha : V^n \rightarrow K$  définie par

$$\alpha(u_1, \dots, u_m) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{j=1}^n \varphi_{\sigma(j)}(v_j)$$

est non nulle; elle appartient à  $\mathcal{A}^n(V, K)$  et elle engendre donc l'espace.  $\square$

**Corollaire 17.1.7.** *Si  $\dim(V) = n$ ,  $\alpha \in \mathcal{A}^n(V, K)$  est non-nulle, et  $v_1, \dots, v_n$  sont des vecteurs dans  $V$ , alors  $\alpha(v_1, \dots, v_n) \neq 0$  si et seulement si  $\{v_1, \dots, v_n\}$  est une base de  $V$ .*

*Démonstration.* Supposons d'abord que  $\alpha(v_1, \dots, v_n) \neq 0$ . Alors,  $\{v_1, \dots, v_n\}$  doit être libre et donc une base de  $V$  (voir le deuxième point à la page 6). Maintenant, si  $\{v_1, \dots, v_n\}$  est une base de  $V$ , comme  $\alpha$  est non-nulle, il existe des vecteurs  $u_1, \dots, u_n \in V$  tels que  $\alpha(u_1, \dots, u_n) \neq 0$ . Mais alors, en utilisant le Théorème 17.1.5 on déduit que  $\alpha(v_1, \dots, v_n) \neq 0$ , car on peut écrire

$$0 \neq \alpha(u_1, \dots, u_n) = \eta \cdot \alpha(v_1, \dots, v_n)$$

pour un certain scalaire  $\eta \in K$  comme dans le Théorème 17.1.5.  $\square$

AZ: Notez que l'argument ci-dessus nous indique également que le scalaire  $\eta$  n'est pas nul.

### 17.1.1 Pour réfléchir chez vous

**Exercice 17.1.8.** Soient  $W$  un  $K$ -espace vectoriel et  $\iota : V^m \rightarrow W$  une application  $m$ -linéaire tels que la paire  $(W, \iota)$  satisfasse la propriété universelle suivante :

- Si  $U$  est un  $K$ -espace vectoriel quelconque et  $\alpha : V^m \rightarrow U$  est une application  $m$ -linéaire, alors il existe une unique application linéaire  $\tilde{\alpha} : W \rightarrow U$  telle que  $\tilde{\alpha} \circ \iota = \alpha$ .

Démontrer que si  $(\tilde{W}, \tilde{\iota})$  est une autre paire satisfaisant la propriété ci-dessus, alors les espaces vectoriels  $W$  et  $\tilde{W}$  sont isomorphes (sur  $K$ ).

AZ: On peut démontrer que de telles paires existent toujours. Les espaces  $W$  sont notés  $V^{\otimes m} = \underbrace{V \otimes \dots \otimes V}_m$ .

## Cours 20

---

### 18.1 Déterminants

On fixe un corps  $K$  et un  $K$ -espace vectoriel  $V$  de dimension finie  $n$ . Pour  $T \in \mathcal{L}(V, V)$  et pour  $\alpha \in \mathcal{A}^n(V, K)$ , définissons une autre forme  $n$ -linéaire alternée sur  $V$ , notée  $\alpha_T$ , par

$$\alpha_T(u_1, \dots, u_n) := \alpha(T(u_1), \dots, T(u_n))$$

pour chaque liste  $u_1, \dots, u_n$  de vecteurs dans  $V$ . Ceci définit un opérateur linéaire  $\alpha \mapsto \alpha_T$  de  $\mathcal{A}^n(V, K)$ .

Or, nous savons que  $\dim(\mathcal{A}^n(V, K)) = 1$ , et puisque toute transformation linéaire d'un espace vectoriel unidimensionnel vers lui-même est une multiplication par un unique scalaire, pour la transformation linéaire  $\alpha \mapsto \alpha_T$ , nous pouvons maintenant définir  $\det(T)$  comme étant ce scalaire.

**Définition 18.1.1.**

- (i) Soit  $T \in \mathcal{L}(V, V)$ . Le **déterminant** de  $T$  est l'unique scalaire dans  $K$ , noté  $\det(T)$ , tel que pour chaque  $\alpha \in \mathcal{A}^n(V, K)$  on a  $\alpha_T = \det(T) \cdot \alpha$ .
- (ii) Soit  $A \in \mathbb{M}_{n \times n}(K)$  et  $T \in \mathcal{L}(K^n, K^n)$  telle que la matrice de  $T$  par rapport à la base canonique de  $K^n$  est égale à  $A$ . Le déterminant de  $A$ , noté  $\det(A)$ , est défini par  $\det(A) = \det(T)$ .

AZ: Ce commentaire vise à aborder des concepts plus avancés, qui dépassent le cadre de ce cours mais que vous rencontrerez probablement plus tard. Étant donné l'application linéaire  $T : V \rightarrow V$ , je peux considérer l'application linéaire induite  $V \otimes \dots \otimes V \rightarrow V \otimes \dots \otimes V$  définie par  $v_1 \otimes \dots \otimes v_n \mapsto T(v_1) \otimes \dots \otimes T(v_n)$ . L'application transposée de cette application est précisément l'opérateur linéaire  $\alpha \mapsto \alpha_T$  de  $\mathcal{L}^n(V, K) \simeq (V \otimes \dots \otimes V)^*$  défini par

$$\alpha \mapsto ((u_1, \dots, u_n) \mapsto \alpha(T(u_1), \dots, T(u_n))).$$

Ci-dessus, on considère simplement la restriction au sous-espace  $\mathcal{A}^m(V, K) \simeq (\Lambda^n V)^* \simeq \Lambda^n V^*$ .

Notez que les propriétés suivantes découlent directement de la définition du déterminant :

- Comme  $\alpha_{\text{id}} = \alpha$  pour chaque  $\alpha \in \mathcal{A}^n(V, K)$ ,  $\det(\text{id}) = 1$ .
- Comme pour chaque  $\lambda \in K$  on a que  $\alpha_{\lambda \cdot \text{id}} = \lambda^n \cdot \alpha$  pour toute  $\alpha \in \mathcal{A}^n(V, K)$ , alors  $\det(\lambda \cdot \text{id}) = \lambda^n$ .
- Plus généralement, pour  $T \in \mathcal{L}(V, V)$  et  $\lambda \in K$ , on a que  $\alpha_{\lambda \cdot T} = \lambda^n \alpha_T = \lambda^n \cdot (\det(T)) \cdot \alpha$  pour chaque  $\alpha \in \mathcal{A}^n(V, K)$ . Donc  $\det(\lambda \cdot T) = \lambda^n \cdot (\det(T))$
- Pour  $\alpha \in \mathcal{A}^n(V, K)$ ,  $u_1, \dots, u_n \in V$  et  $S, T \in \mathcal{L}(V, V)$  on a que

$$\begin{aligned} \alpha_{S \circ T}(u_1, \dots, u_n) &= \alpha(S(T(u_1)), \dots, S(T(u_n))) \\ &= (\det(S)) \cdot \alpha(T(u_1), \dots, T(u_n)) \\ &= (\det(S)) \cdot (\det(T)) \cdot \alpha(u_1, \dots, u_n). \end{aligned}$$

Donc  $\det(S \circ T) = (\det(S)) \cdot (\det(T))$ .

- En particulier, si  $A$  et  $B$  sont des matrices carrées de même taille (à coefficients dans  $K$ ). Alors,  $\det(AB) = \det(A) \cdot \det(B)$ .

Maintenant, pour le résultat suivant, considérez chaque liste  $u_1, \dots, u_n$  de  $n$  vecteurs dans  $K^n$  comme une liste de matrices colonnes. La notation  $(u_1 \ \dots \ u_n)$  désigne alors la matrice carrée  $n \times n$  dont la  $j$ -ième colonne est  $u_j$  pour chaque  $j = 1, \dots, n$ .

**Proposition 18.1.2.** *L'application qui associe une liste  $u_1, \dots, u_n$  de vecteurs dans  $K^n$  au scalaire  $\det((u_1 \ \dots \ u_n))$  est une forme  $n$ -linéaire alternée sur  $K^n$ .*

*Démonstration.* Soit  $\mathcal{E} = \{e_1, \dots, e_n\}$  la base canonique de  $K^n$  et prenons  $u_1, \dots, u_n \in K^n$ . Soit  $T \in \mathcal{L}(K^n, K^n)$  l'unique opérateur linéaire tel que  $T(e_j) = u_j$  pour chaque  $j = 1, \dots, n$ . Ainsi,

$$[T]_{\mathcal{E}, \mathcal{E}} = (u_1 \ \dots \ u_n)$$

Par conséquent,  $\det((u_1 \ \dots \ u_n)) = \det(T)$ , par définition du déterminant d'une matrice.

Soit maintenant  $\alpha \in \mathcal{A}^n(K^n, K)$  telle que  $\alpha(e_1, \dots, e_n) = 1_K$ . Alors,

$$\begin{aligned} \det((u_1 \ \dots \ u_n)) &= \det(T) \\ &= (\det(T)) \cdot \alpha(e_1, \dots, e_n) \\ &= \alpha(T(e_1), \dots, T(e_n)) \\ &= \alpha(u_1, \dots, u_n). \end{aligned}$$

En d'autres termes, l'application qui prend une liste de vecteurs  $u_1, \dots, u_n \in K^n$  à  $\det((u_1 \ \dots \ u_n))$  est précisément la forme  $n$ -linéaire alternée  $\alpha$ .  $\square$

AZ: Pourquoi la forme  $\alpha$  existe-t-elle ?

AZ: Notez que le même résultat sera valable si l'on considère les lignes au lieu des colonnes.

**Remarque 12.** Si l'on applique le Théorème 17.1.5 à forme linéaire alternée  $u_1, \dots, u_n \mapsto \det((u_1 \ \dots \ u_n))$  sur  $K^n$ , alors, en prenant pour base de  $K^n$  la base canonique, on peut déduire la formule de Leibniz (2) du cours 18.

**Remarque 13.** Soit  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{M}_{2 \times 2}(\mathbb{R})$  et considérons l'application linéaire

$$\begin{aligned} \varphi_A : \mathbb{R}^2 \simeq \mathbb{M}_{2 \times 1}(\mathbb{R}) &\rightarrow \mathbb{R}^2 \simeq \mathbb{M}_{2 \times 1}(\mathbb{R}) \\ \begin{pmatrix} x \\ y \end{pmatrix} &\mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}. \end{aligned}$$

Soit encore  $P \subset \mathbb{R}^2$  un parallélogramme. Alors,  $\text{Aire}(\varphi_A(P)) = |\det(A)| \cdot \text{Aire}(P)$ . En particulier, si  $C$  est le carré déterminé par les deux vecteurs de base canoniques  $e_1$  et  $e_2$ , alors on déduit que  $\det(A) = \text{Aire}(\varphi_A(C))$ . Ce résultat peut être généralisé aux dimensions supérieures en considérant les «  $n$ -cubes ».

AZ: Je vous propose de regarder la vidéo « The determinant » sur la chaîne 3Blue1Brown pour acquérir une intuition de la signification géométrique du déterminant.

### 18.1.1 Pour réfléchir chez vous

**Exemple 18.1.3.** Soit  $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{M}_{2 \times 2}(\mathbb{R})$  et considérez la forme bilinéaire  $\beta_A$  sur  $\mathbb{R}^2$  définie dans l'Exemple 17.1.2 (du produit scalaire usuel). Alors, le produit vectoriel  $\mathbb{R}^3 \times \mathbb{R}^3 \ni (v, w) \mapsto v \times w \in \mathbb{R}^3$  est une opération bilinéaire alternée qui satisfait la propriété suivante :

- Étant donné deux vecteurs  $v$  et  $w$  quelconques dans  $\mathbb{R}^3$  le vecteur  $v \times w$  est l'unique vecteur dans  $\mathbb{R}^3$  tel que

$$\beta_A(u, v \times w) = \det((u \ v \ w))$$

pour chaque  $u \in \mathbb{R}^3$ .

## 18.2 Quelques propriétés des déterminants en plus

Le déterminant d'un opérateur indique si cet opérateur est inversible.

**Proposition 18.2.1.** *Un opérateur  $T \in \mathcal{L}(V, V)$  est inversible si et seulement si  $\det(T) \neq 0$ . De plus, si  $T$  est inversible, alors  $\det(T^{-1}) = (\det(T))^{-1}$ .*

*Démonstration.* Si  $T$  est inversible, alors il existe  $T^{-1} \in \mathcal{L}(V, V)$  telle que  $T \circ T^{-1} = \text{id}_V$ . Donc,

$$1_K = \det(\text{id}) = \det(T \circ T^{-1}) = \det(T) \cdot (\det(T^{-1}))$$

et, par conséquent,  $\det(T) \neq 0_K$  et  $(\det(T^{-1}))$  est l'inverse de  $\det(T)$  dans le groupe multiplicatif  $K^\times = K \setminus \{0\}$ .

Pour prouver l'autre implication, supposons que  $\det(T) \neq 0$  et prenons  $v \in V$  non nul. Complétons  $\{v\}$  en une base  $\{v, v_2, \dots, v_n\}$  de  $V$ . Alors, si  $\alpha \in \mathcal{A}^n(V, K)$  est non nulle on a que

$$\alpha(v, v_2, \dots, v_n) \neq 0 \Rightarrow \alpha(T(v), T(v_2), \dots, T(v_n)) = \det(T) \cdot \alpha(v, v_2, \dots, v_n) \neq 0.$$

En particulier,  $T(v) \neq 0$  et puisque  $v$  a été choisi arbitrairement,  $T$  est inversible ( $\ker(T) = \{0\}$  implique  $T$  injective, donc bijective).  $\square$

Le déterminant est un invariant de similarité.

**Proposition 18.2.2.** *Soient  $T \in \mathcal{L}(V, V)$ ,  $W$  un  $K$ -espace vectoriel de dimension finie  $n$  ( $=\dim(V)$ ) et  $S \in \mathcal{L}(W, V)$  une application inversible. Alors*

$$\det(S^{-1} \circ T \circ S) = \det(T).$$

*Démonstration.* Prenons  $\beta \in \mathcal{A}^n(W, K)$  et définissons  $\alpha \in \mathcal{A}^n(V, K)$  par

$$\alpha(v_1, \dots, v_n) := \beta(S^{-1}(v_1), \dots, S^{-1}(v_n)),$$

où  $v_1, \dots, v_n \in V$ . Alors, pour chaque liste  $w_1, \dots, w_n$  de vecteurs dans  $W$  on a que

$$\begin{aligned} \beta_{S^{-1} \circ T \circ S}(w_1, \dots, w_n) &= \beta((S^{-1} \circ T \circ S)(w_1), \dots, (S^{-1} \circ T \circ S)(w_n)) \\ &= \alpha((T \circ S)(w_1), \dots, (T \circ S)(w_n)) \\ &= \alpha_T(S(w_1), \dots, S(w_n)) \\ &= \det(T) \cdot \alpha(S(w_1), \dots, S(w_n)) \\ &= \det(T) \cdot \beta(w_1, \dots, w_n). \end{aligned}$$

Donc  $\det(S^{-1} \circ T \circ S) = \det(T)$ .  $\square$

Le déterminant d'un opérateur est égal au déterminant de toute matrice qui le représente.

**Corollaire 18.2.3.** *Si  $T \in \mathcal{L}(V, V)$  et  $\mathcal{B} = (u_1, \dots, u_n)$  est une base ordonnée de  $V$ . Alors,*

$$\det(T) = \det([T]_{\mathcal{B}, \mathcal{B}}).$$

*Démonstration.* La preuve découle du diagramme commutatif ci-dessous.

$$\begin{array}{ccccccc}
 \mathbb{M}_{n \times 1}(K) \simeq K^n & \xrightarrow{I_n} & \mathbb{M}_{n \times 1}(K) \simeq K^n & \xrightarrow{[T]_{\mathcal{B}, \mathcal{B}}} & \mathbb{M}_{n \times 1}(K) \simeq K^n & \xrightarrow{I_n} & \mathbb{M}_{n \times 1}(K) \simeq K^n \\
 \simeq_{\mathcal{E}} \uparrow & & \simeq_{\mathcal{B}} \uparrow & & \simeq_{\mathcal{B}} \uparrow & & \simeq_{\mathcal{E}} \uparrow \\
 \mathbb{M}_{n \times 1}(K) \simeq K^n & \xrightarrow[e_i \mapsto u_i]{S} & V & \xrightarrow{T} & V & \xrightarrow[u_i \mapsto e_i]{S^{-1}} & \mathbb{M}_{n \times 1}(K) \simeq K^n
 \end{array}$$

où  $\mathcal{E} = \{e_1, \dots, e_n\}$  désigne la base canonique de  $\mathbb{M}_{n \times 1}(K) \simeq K^n$ . □

## Cours 21

---

On fixe un corps  $K$ . On considère un  $K$ -espace vectoriel  $V$  et l'anneau unitaire  $\mathcal{L}(V, V)$ . Notez que si  $V$  est de dimension finie  $n$ , cet anneau est isomorphe à l'anneau  $\mathbb{M}_{n \times n}(K)$ .

### 19.1 Vecteurs propres et valeurs propres

Les matrices les plus faciles à « manipuler » algébriquement sont les matrices diagonales. Ensuite, les matrices triangulaires présentent également quelques propriétés utiles. Si  $A = (a_{ij}) \in \mathbb{M}_{n \times n}(K)$  est une matrice diagonale ou triangulaire supérieure, alors, par l'isomorphisme entre  $\mathbb{M}_{n \times n}(K)$  et  $\mathcal{L}(K^n, K^n)$  associé au choix de la base canonique  $\mathcal{E} = \{e_1, \dots, e_n\}$  de  $K^n$ , il existe une unique application linéaire  $\varphi : K^n \rightarrow K^n$  telle que  $[\varphi]_{\mathcal{E}} = A$ . D'après les hypothèses sur la matrice  $A$ , on a que  $\varphi(e_1) = a_{11} \cdot e_1$  et donc  $\text{Vect}(e_1) = \text{Vect}(\varphi(e_1))$ . Cette observation motive la définition suivante.

**Définition 19.1.1.** Soit  $\varphi \in \mathcal{L}(V, V)$ .

- (i) On dit que  $v \in V$  est un **vecteur propre** de  $\varphi$  si  $v \neq 0_V$  et  $\text{Vect}(v) = \text{Vect}(\varphi(v))$ . C'est-à-dire que  $v$  est non-nul et  $\varphi(v)$  est un multiple scalaire de  $v$ . Ce qui revient à dire que  $v \neq 0$  et qu'il existe un scalaire  $\lambda \in K$  tel que  $\varphi(v) = \lambda \cdot v$ .
- (ii) Le scalaire  $\lambda$  de (i) s'appelle la **valeur propre** de  $\varphi$  associée au vecteur propre  $v$ .
- (iii) Si  $\lambda$  est une valeur propre de  $\varphi$ , alors le sous-espace  $E_\lambda := \{v \in V ; \varphi(v) = \lambda \cdot v\} \leq V$  s'appelle l'espace propre de  $\varphi$  associé à la valeur propre  $\lambda$ .

Notez qu'on a une notion analogue pour les matrices carrées  $A = (a_{ij}) \in \mathbb{M}_{n \times n}(K)$  en considérant l'application linéaire  $\varphi_A : \mathbb{M}_{n \times 1}(K) \rightarrow \mathbb{M}_{n \times 1}(K)$  canoniquement associée à  $A$  et définie par

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Plus précisément,  $0 \neq v \in \mathbb{M}_{n \times 1}(K)$  est un vecteur propre de  $A$  si et seulement s'il existe un scalaire  $\lambda \in K$  tel que  $\varphi_A(v) = \lambda \cdot v$ . Si tel est le cas,  $\lambda$  s'appelle la valeur propre de  $A$  associée au vecteur propre  $v$ .

**Exercice 19.1.2.** Montrez que  $0_K$  est une valeur propre d'une application linéaire  $\varphi \in \mathcal{L}(V, V)$  si et seulement si  $\varphi$  n'est pas injective.

Le résultat suivant découle directement des définitions ci-dessus.

**Théorème 19.1.3.** Soient  $\varphi \in \mathcal{L}(V, V)$  et  $\lambda \in K$ . Alors  $\lambda$  est une valeur propre de  $\varphi$  si et seulement si l'application linéaire  $\varphi - \lambda \cdot \text{id}_V$  n'est pas inversible. Si et seulement si  $\ker(\varphi - \lambda \cdot \text{id}_V) \neq \{0\}$ .

*Démonstration.* Par définition, on a que  $\lambda \in K$  est une valeur propre de  $\varphi$  si et seulement s'il existe  $v \in V$  non nul tel que  $\varphi(v) = \lambda \cdot v$ . Donc, si et seulement s'il existe  $v \in V$  non nul tel que  $(\varphi - \lambda \text{id}_V)(v) = 0 \iff v \in \ker(\varphi - \lambda \text{id}_V)$ . Mais cela revient à dire que  $\ker(\varphi - \lambda \text{id}_V) \neq \{0\}$ , ce qui est en outre équivalent à ce que  $\varphi - \lambda \cdot \text{id}_V$  soit non inversible.  $\square$

Dans le cas où  $\dim(V) = n$ , ce résultat nous fournit une méthode pour déterminer les valeurs propres.

**Proposition 19.1.4.** Supposons  $\dim(V) = n$ . Soit  $\varphi \in \mathcal{L}(V, V)$ , fixons une base ordonnée  $B$  de  $V$  et posons  $A = [\varphi]_B$ . Alors  $\lambda \in K$  est une valeur propre de  $\varphi$  (ou de  $A$ ) si et seulement si la matrice  $A - \lambda \cdot I_n$  est non inversible, ce qui est le cas si et seulement si  $\det(A - \lambda \cdot I_n) = 0$ .

*Démonstration.* Il suffit de noter que  $[\varphi - \lambda \cdot \text{id}_V]_B = A - \lambda \cdot I_n$  et de se rappeler qu'une transformation linéaire est inversible si et seulement si l'une, donc toutes, de ses représentations matricielles est également inversible.  $\square$

Ceci motive, à son tour, la définition suivante.

**Définition 19.1.5.** Soit  $A \in \mathbb{M}_{n \times n}(K)$ . Soit encore  $x$  une indéterminée. Alors  $c_A(x) := \det(A - x \cdot I_n) \in K[x]$  est appelé le **polynôme caractéristique** de la matrice  $A$ .

Par la caractérisation des valeurs propres donnée par Théorème 19.1.3 et par Proposition 19.1.4, nous déduisons que  $\lambda \in K$  est une valeur propre de  $A \in \mathbb{M}_{n \times n}(K)$  si et seulement si  $\lambda$  est une racine du polynôme caractéristique  $c_A(x)$ , c.-à-d.  $c_A(\lambda) = 0$ .

**Exemple 19.1.6.** Si  $A = (a_{ij}) \in \mathbb{M}_{n \times n}(K)$  est une matrice triangulaire, alors

$$c_A(x) = (a_{11} - x) \cdot (a_{22} - x) \cdot \dots \cdot (a_{nn} - x).$$

Par conséquent, ses valeurs propres sont précisément celles situées le long de sa diagonale.

AZ: Une matrice est dite triangulaire si elle est carrée et si tous les coefficients d'un côté ou de l'autre de la diagonale principale sont nuls.

**Exemple 19.1.7.** Soit  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{M}_{2 \times 2}(K)$ . Alors

$$c_A(x) = \det \left( \begin{pmatrix} a - x & b \\ c & d - x \end{pmatrix} \right) = x^2 - (a + d) \cdot x + (ad - bc) = x^2 - \text{tr}(A) \cdot x + \det(A)$$

Grâce au résultat suivant, on peut également définir le polynôme caractéristique d'un endomorphisme linéaire d'un espace vectoriel de dimension finie sur  $K$ , puis l'utiliser pour calculer des valeurs propres.

**Proposition 19.1.8.** *Deux matrices semblables (similaires) ont le même polynôme caractéristique. En particulier, deux matrices semblables ont les mêmes valeurs propres.*

*Démonstration.* Soient  $A, B \in \mathbb{M}_{n \times n}(K)$  et  $P \in \text{GL}(n, K)$  telles que  $B = P^{-1}AP$ . On a que

$$\begin{aligned} c_B(x) &= \det(B - x \cdot I_n) \\ &= \det(P^{-1}AP - x \cdot I_n) \\ &= \det(P^{-1}AP - x \cdot P^{-1}I_nP) \\ &= \det(P^{-1}(A - x \cdot I_n)P) \\ &= \det(A - x \cdot I_n) \\ &= c_A(x) \end{aligned}$$

□

**Définition 19.1.9.** Supposons  $V$  de dimension finie. Soit  $\varphi \in \mathcal{L}(V, V)$ . Le polynôme caractéristique de  $\varphi$ , noté  $c_\varphi(x)$ , est le polynôme caractéristique de n'importe quelle matrice représentant  $\varphi$  par rapport à un choix de base ordonnée quelconque.

La caractérisation donnée par le Théorème 19.1.3 et par la Proposition 19.1.4 est également utile pour prouver le résultat suivant et, en particulier, pour déterminer une borne supérieure du nombre de valeurs propres distinctes qu'un opérateur peut avoir.

**Proposition 19.1.10.** *Toute liste de vecteurs propres d'une application linéaire  $\varphi \in \mathcal{L}(V, V)$  correspondant à des valeurs propres distinctes est linéairement indépendante.*

*Démonstration.* Sinon, il existe un plus petit entier positif  $m$  tel qu'il existe une liste linéairement dépendante de  $m$  vecteurs propres de  $\varphi$ , disons  $v_1, \dots, v_m$ , correspondant à des valeurs propres distinctes  $\lambda_1, \dots, \lambda_m$ . Mais alors, en raison de la minimalité de  $m$ , il existe des scalaires  $a_1, \dots, a_m \in K$ , dont aucun n'est nul, tels que

$$a_1 \cdot v_1 + \dots + a_m \cdot v_m = 0_V.$$

Donc, en appliquant  $\varphi - \lambda_m \text{id}$  aux deux membres de l'équation ci-dessus, on obtient

$$a_1(\lambda_1 - \lambda_m) \cdot v_1 + \dots + a_{m-1}(\lambda_{m-1} - \lambda_m) \cdot v_{m-1} = 0_V.$$

Maintenant, comme  $m$  est nécessairement supérieur ou égal à deux, cette dernière égalité n'est pas vide; et puisque les valeurs propres  $\lambda_1, \dots, \lambda_m$  sont distinctes, aucun des coefficients ci-dessus n'est égal à  $0_K$ . Ainsi,  $v_1, \dots, v_{m-1}$  est une liste linéairement dépendante de  $m - 1$  vecteurs propres de  $\varphi$  correspondant à des valeurs propres distinctes. Eh bien, cela contredit la minimalité de  $m$ . □

Pourquoi ?

**Corollaire 19.1.11.** *Supposons que  $V$  soit de dimension finie. Alors chaque endomorphisme linéaire de  $V$  possède au plus  $\dim(V)$  valeurs propres distinctes.*

AZ: Notez que ce dernier corollaire peut bien sûr être déduit à partir du polynôme caractéristique. Quel est le degré du polynôme  $c_\varphi(x)$ ? Quel est le nombre maximal de racines distinctes?

AZ: Ce qui n'est peut-être pas encore clair, c'est si tout opérateur linéaire (ou toute matrice carrée) possède une valeur propre ou non. La réponse dépend fortement du corps  $K$ .

### 19.1.1 Pour réfléchir chez vous

AZ: Je vous propose de regarder la vidéo « À quoi servent les vecteurs et valeurs propres ? » par Lê Nguyễn Hoang dans la chaîne Wandida, EPFL.

## Cours 22

---

### 20.1 Multiplicité géométrique et multiplicité algébrique

**Définition 20.1.1.** Soient  $K$  un corps,  $V$  un  $K$ -espace vectoriel de dimension finie et soit encore  $\lambda \in K$  une valeur propre d'une application linéaire  $\varphi \in \mathcal{L}(V, V)$ .

- (i) La multiplicité algébrique de  $\lambda$ , notée  $\mu_a(\lambda)$ , est la multiplicité de  $\lambda$  en tant que racine du polynôme caractéristique.
- (ii) La multiplicité géométrique de  $\lambda$ , notée  $\mu_g(\lambda)$ , est la dimension de l'espace propre  $E_\lambda$ . Autrement dit, c'est la dimension du noyau de l'application  $\varphi - \lambda \cdot \text{id}$ .

**Exemple 20.1.2.** Considérons la matrice  $A = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \in \mathbb{M}_{2 \times 2}(\mathbb{R})$ .

Alors, on a que  $c_A(x) = x^2 - 7x + 10 = (x - 2)(x - 5)$  et donc les valeurs propres de  $A$  sont  $\lambda_1 = 2$  et  $\lambda_2 = 5$ . Dans ce cas, les deux valeurs propres ont la même multiplicité algébrique, égale à 1.

**Exemple 20.1.3.** Considérons maintenant,  $B = \begin{pmatrix} 3 & 0 & 0 \\ 2 & 3 & 0 \\ 1 & 0 & 3 \end{pmatrix}$ . Alors,

$$B - x \cdot I_3 = \begin{pmatrix} 3 - x & 0 & 0 \\ 2 & 3 - x & 0 \\ 1 & 0 & 3 - x \end{pmatrix}$$

et on a que  $c_B(x) = \det(B - x \cdot I_3) = (3 - x)^3$  et donc que  $\lambda = 3$  est la seule valeur propre de la matrice  $B$ , avec multiplicité algébrique égale à 3.

Calculons maintenant la multiplicité géométrique  $\mu_g(3)$ . Par définition,  $\mu_g(3) = \dim(\ker(\varphi_B - 3 \cdot \text{id}))$ , où  $\varphi_B : \mathbb{M}_{3 \times 1}(\mathbb{R}) \simeq \mathbb{R}^3 \rightarrow \mathbb{M}_{3 \times 1}(\mathbb{R}) \simeq \mathbb{R}^3$  est l'application linéaire donnée par la multiplication (à gauche) par  $B$ . Comme la matrice de  $\varphi_B - 3 \cdot \text{id}$  par rapport à la base canonique est donnée par

$$B - 3 \cdot I_3 = \begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

nous en déduisons que  $\mu_g(3) = 2$ .

En fait, dans cet exemple, d'espace propre  $E_3$  est engendré par des vecteurs propres  $e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$  et  $e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ . Vérifiez-le!

AZ: Cet exemple montre notamment que, de manière générale, les deux notions de multiplicité (algébrique et géométrique) sont différentes. On peut en tout cas démontrer le résultat suivant.

**Proposition 20.1.4.** *Soient  $K$  un corps,  $V$  un  $K$ -espace vectoriel de dimension finie et soit encore  $\lambda \in K$  une valeur propre d'une application linéaire  $\varphi \in \mathcal{L}(V, V)$ . Alors,  $\mu_g(\lambda) \leq \mu_a(\lambda)$ .*

*Démonstration.* Posons  $m = \mu_g(\lambda)$ . Considérons donc une base ordonnée  $\mathcal{B} = (v_1, \dots, v_m)$  de l'espace propre  $E_\lambda$ . Si  $m = \dim(V) = \deg(c_\varphi(x))$ , il n'y a rien à prouver, car  $c_\varphi(x) = c_A(x) = (\lambda - x)^m$ . Sinon, nous pouvons compléter  $\mathcal{B}$  en une base ordonnée de  $V$ , disons  $\mathcal{C} = (v_1, \dots, v_m, v_{m+1}, \dots, v_n)$ . Alors, la matrice  $A = [\varphi]_{\mathcal{C}, \mathcal{C}}$  a la forme

$$\begin{pmatrix} D & M \\ 0_{n-m} & N \end{pmatrix}$$

où la matrice  $D = \left[ \varphi|_{E_\lambda} \right]_{\mathcal{B}, \mathcal{B}} = \lambda \cdot I_m$  est diagonale, et on a  $M \in \mathbb{M}_{m \times (n-m)}(K)$  et  $N \in \mathbb{M}_{(n-m) \times (n-m)}(K)$ . Donc,

$$c_\varphi(x) = c_A(x) = \det(A - x \cdot I_n) = \det(D - x \cdot I_m) \cdot \det(N - x \cdot I_{n-m}) = (\lambda - x)^m \cdot c_N(x)$$

ce qui montre que la multiplicité algébrique  $\mu_a(\lambda)$  est supérieure ou égale à  $m = \mu_g(\lambda)$ .  $\square$

## 20.2 (★) Polynôme minimal d'un endomorphisme (non examinable)

Rappelons que, par définition, les valeurs propres des opérateurs sur un  $K$ -espace vectoriel  $V$  et les zéros des polynômes de  $K[x]$  doivent appartenir à  $K$ . Une question importante se pose donc : quand les valeurs propres existent-elles ?

**Théorème 20.2.1** (existence de valeurs propres). *Tout opérateur sur un  $\mathbb{C}$ -espace vectoriel non trivial de dimension finie possède une valeur propre.*

AZ: Ce théorème est valable de manière plus générale sur un corps algébriquement clos.

*Première preuve.* Soit  $V$  un  $\mathbb{C}$ -espace vectoriel de dimension finie et soit  $\varphi \in \mathcal{L}(V, V)$ . Alors,  $\lambda \in \mathbb{C}$  est une valeur propre de  $\varphi$  si et seulement si  $p_\varphi(\lambda) = 0$  ( $\lambda$  est une racine du polynôme caractéristique de  $\varphi$ ). Comme  $p_\varphi(x) \in \mathbb{C}[x]$ , on sait, par le théorème fondamental de l'algèbre (Théorème 3.3.7), que  $p_\varphi(x)$  admet toujours une racine dans  $\mathbb{C}$ , il s'ensuit que  $\varphi$  possède une valeur propre.  $\square$

AZ: Notez que ce premier argument fonctionne même si  $V = \{0\}$ . Mais ce cas est trivial.

*Deuxième preuve.* Soit  $V$  un  $\mathbb{C}$ -espace vectoriel de dimension finie  $n$  et soit  $\varphi \in \mathcal{L}(V, V)$ . Supposons  $V \neq \{0\}$  et prenons  $0 \neq v \in V$ . Alors, les vecteurs

$$v, \varphi(v), \dots, \varphi^n(v)$$

ne sont pas libres. Par conséquent, une combinaison linéaire des vecteurs ci-dessus (dont tous les coefficients ne sont pas nuls) est égale au vecteur nul  $0_V$ . Il existe donc un polynôme non constant  $f(x) \in \mathbb{C}[x]$  de plus petit degré tel que

$$f(\varphi)(v) = 0_V.$$

Or, par le théorème fondamental de l'algèbre, il existe  $\lambda \in \mathbb{C}$  tel que  $f(\lambda) = 0$  et donc il existe  $g(x) \in \mathbb{C}[x]$  tel que

$$f(x) = (x - \lambda) \cdot g(x).$$

Mais cela implique alors que

$$0_V = f(\varphi)(v) = (\varphi - \lambda \cdot \text{id}_V) \cdot (g(\varphi)(v)),$$

et par la minimalité du degré de  $f$ , on déduit que  $g(\varphi)(v) \neq 0_V$  et donc que  $\lambda$  est une valeur propre de  $\varphi$  avec vecteur propre  $g(\varphi)(v)$ .  $\square$

AZ: La dernière démonstration est plus compliquée, mais elle contient de nombreuses idées intéressantes et importantes qui peuvent être utilisées pour prouver le résultat suivant.

**Théorème 20.2.2.** Soit  $K$  un corps et supposons que  $V$  soit un  $K$ -espace vectoriel de dimension finie. Soit  $\varphi \in \mathcal{L}(V, V)$ . Alors il existe un unique polynôme unitaire  $m_\varphi(x) \in K[x]$  de degré minimal tel que  $m_\varphi(\varphi) = 0$ . De plus,  $\deg(m_\varphi) \leq \dim(V)$ .

*Démonstration.* Admis sans preuve dans ce cours.  $\square$

AZ: Ce dernier résultat implique qu'un polynôme  $p(x) \in K[x]$  est tel que  $p(\varphi) = 0$  si et seulement si  $p(x)$  est un multiple de  $m_\varphi(x)$ . Le théorème de Cayley-Hamilton nous dit que le polynôme caractéristique  $c_\varphi(x)$  a cette propriété, c.-à-d.  $c_\varphi(\varphi) = 0$ . C'est un théorème que vous verrez le semestre prochain.

**Définition 20.2.3.** Soient  $K$  un corps et  $V$  un  $K$ -espace vectoriel de dimension finie. Soit encore  $\varphi \in \mathcal{L}(V, V)$ . Alors le **polynôme minimal** de  $\varphi$  est l'unique polynôme unitaire  $m_\varphi(x) \in K[x]$  de degré minimal tel que  $m_\varphi(\varphi) = 0$ .

Pour calculer le polynôme minimal d'un opérateur  $\varphi \in \mathcal{L}(V, V)$ , nous devons trouver le plus petit entier positif  $r$  tel que l'équation

$$a_0 \text{id}_V + a_1 \cdot \varphi + \dots + a_{r-1} \cdot \varphi^{r-1} = -\varphi^r$$

admet une solution  $a_0, \dots, a_{r-1} \in K$ . Si l'on choisit une base de  $V$  et remplace  $\varphi$  dans l'équation ci-dessus par la matrice correspondante à cette base, on peut alors considérer cette équation comme un système de  $(\dim(V))^2$  équations linéaires à  $r$  inconnues  $a_0, \dots, a_{r-1} \in K$ . L'élimination de Gauss permet de déterminer l'existence d'une solution en testant successivement les valeurs de  $r$  jusqu'à en trouver une. D'après le théorème ci-dessus, une telle solution existe pour un plus petit entier positif  $d \leq \dim(V)$ . Le polynôme minimal de  $\varphi$  est alors le polynôme

$$a_0 + a_1 \cdot x + \dots + a_{d-1} \cdot x^{d-1} + x^d \in K[x].$$

**Exemple 20.2.4.** Supposons  $K = \mathbb{R}, V = \mathbb{R}^5$  et  $\varphi \in \mathcal{L}(V, V)$  tel que la matrice de  $\varphi$  par rapport à la base canonique est la matrice

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 4 \\ 1 & 0 & 0 & 0 & -7 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Alors,

$$\begin{aligned} \varphi(e_1) &= e_2 \\ \varphi^2(e_1) &= \varphi(\varphi(e_1)) = \varphi(e_2) = e_3 \\ \varphi^3(e_1) &= \varphi(\varphi^2(e_1)) = \varphi(e_3) = e_4 \\ \varphi^4(e_1) &= \varphi(\varphi^3(e_1)) = \varphi(e_4) = e_5 \\ \varphi^5(e_1) &= \varphi(\varphi^4(e_1)) = \varphi(e_5) = 4e_1 - 7e_2 \end{aligned}$$

ce qui implique que

$$\{e_1, e_2, e_3, e_4, e_5\} = \{e_1, \varphi(e_1), \varphi^2(e_1), \varphi^3(e_1), \varphi^4(e_1)\}$$

et, par conséquent, que  $m_\varphi(x) = -4 + 7x + x^5$ .

**Proposition 20.2.5.** Soient  $K$  un corps,  $V$  un  $K$ -espace vectoriel de dimension finie et  $\varphi \in \mathcal{L}(V, V)$ .

- (i) Les racines du polynôme minimal de  $\varphi$  sont les valeurs propres de  $\varphi$ .
- (ii) Si  $K = \mathbb{C}$ , alors

$$m_\varphi(x) = (x - \lambda_1) \cdot \dots \cdot (x - \lambda_d),$$

où  $\lambda_1, \dots, \lambda_d$  est une liste de toutes les valeurs propres de  $\varphi$ , éventuellement avec répétition.

AZ: Notez que (i) dit que le polynôme minimal  $m_\varphi(x)$  et le polynôme caractéristique  $c_\varphi(x)$  ont les mêmes racines.

*Démonstration.*

- (i) Ce que nous voulons prouver, c'est qu'étant donné  $\lambda \in K$ , alors  $c_\varphi(\lambda) = 0 \iff m_\varphi(\lambda) = 0$ . Si,  $m_\varphi(\lambda) = 0$ , alors il existe  $q(x) \in K[x]$  tel que

$$m_\varphi(x) = (x - \lambda)q(x)$$

et donc

$$0_V = m_\varphi(\varphi)(v) = (\varphi - \lambda \cdot \text{id})(q(\varphi)(v))$$

pour chaque  $v \in V$ . Or, comme  $\deg(q(x)) < \deg(m_\varphi)$ , il découle de la définition du polynôme minimal que  $q(\varphi) \neq 0$  et donc il existe au moins un vecteur  $v \in V$  tel que  $q(\varphi)(v) \neq 0$ . Mais alors l'équation ci-dessus dit que  $\lambda$  est une valeur propre de  $\varphi$  associée au vecteur propre  $q(\varphi)(v)$ .

Inversement, si  $m_\varphi(\lambda) \neq 0$ , alors il existe (algorithme de division)  $q(x) \in K[x]$  et  $\alpha \in K^\times$  tels que

$$m_\varphi(x) = (x - \lambda)q(x) + \alpha.$$

Mais alors, comme  $\alpha = m_\varphi(\lambda) \neq 0$  on a que

$$\begin{aligned} 0 = m_\varphi(\varphi) &= (\varphi - \lambda \cdot \text{id})q(\varphi) + \alpha \cdot \text{id} \\ &\Rightarrow -\alpha^{-1}(\varphi - \lambda \cdot \text{id})q(\varphi) = \text{id} \\ &\Rightarrow \varphi - \lambda \cdot \text{id} \quad \text{est inversible} \\ &\Rightarrow \lambda \text{ n'est pas une valeur propre de } \varphi \\ &\Rightarrow c_\varphi(\lambda) \neq 0. \end{aligned}$$

(ii) Cela découle du théorème fondamental de l'algèbre (Théorème 3.3.7). □

## Cours 23

---

On fixe un corps  $K$  et un  $K$ -espace vectoriel  $V$ . De plus, étant donné une matrice carrée  $A \in \mathbb{M}_{n \times n}(K)$ , on note  $\varphi_A$  l'unique application linéaire

$$\varphi_A : \mathbb{M}_{n \times 1}(K) \simeq K^n \rightarrow \mathbb{M}_{n \times 1}(K) \simeq K^n$$

dont la matrice, par rapport à la base canonique, est égale à  $A$ . Autrement dit,  $\varphi_A$  est définie tout simplement par multiplication (à gauche) par  $A$ .

### 21.1 Matrices triangulaires et endomorphismes trigonalisables

**Définition 21.1.1.** Soit  $\varphi \in \mathcal{L}(V, V)$ . Un sous-espace  $U \leq V$  est dit **invariant** sous  $\varphi$  si  $\varphi(U) \subset U$ , c.-à-d.  $u \in U \Rightarrow \varphi(u) \in U$ .

AZ: Notez que les espaces propres fournissent des exemples de sous-espaces invariants.

**▲** À partir de maintenant, nous supposons implicitement que  $\dim(V) = n < \infty$ .

**Proposition 21.1.2.** Soient  $\varphi \in \mathcal{L}(V, V)$  et  $\mathcal{B} = (v_1, \dots, v_n)$  une base ordonnée de  $V$ . Alors les affirmations suivantes sont équivalentes.

- (i) La matrice  $[\varphi]_{\mathcal{B}}$  est triangulaire supérieure.
- (ii) Pour chaque  $k = 1, \dots, n$ , le sous-espace  $\text{Vect}(v_1, \dots, v_k) \leq V$  est invariant sous  $\varphi$ .
- (iii) Pour chaque  $k = 1, \dots, n$  on a que  $\varphi(v_k) \in \text{Vect}(v_1, \dots, v_k)$ .

De plus, chacune de ces affirmations implique l'affirmation suivante :

- (iv) Il existe des sous-espaces  $\varphi$ -invariants  $W_0, \dots, W_n$  de  $V$  avec

$$\{0\} = W_0 \subset W_1 \subset \dots \subset W_{n-1} \subset W_n = V$$

et  $\dim(W_i) = i$  pour chaque  $i = 0, \dots, n$ .

Inversement, s'il existe des sous-espaces  $\varphi$ -invariants  $W_0, \dots, W_n$  comme dans (iv) ci-dessus, en considérant une base ordonnée  $\tilde{\mathcal{B}} = (u_1, \dots, u_n)$  de  $V$ , avec  $(u_1, \dots, u_k)$  base de  $W_k$  pour tout  $1 \leq k \leq n$ , la matrice  $[\varphi]_{\tilde{\mathcal{B}}}$  sera triangulaire supérieure.

*Démonstration.* Nous prouverons  $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$ . On observe que l'implication  $(ii) \Rightarrow (iv)$  est claire, car nous pouvons tout simplement considérer les espaces  $W_0 = \{0\}$  et  $W_k = \text{Vect}(v_1, \dots, v_k)$  pour chaque  $k = 1, \dots, n$ . La dernière affirmation est également claire.

- (i)  $\Rightarrow$  (ii) Choisissez  $k \in \{1, \dots, n\}$ . Comme  $[\varphi]_{\mathcal{B}}$  est triangulaire supérieure, on a que  $\varphi(v_j) \in \text{Vect}(v_1, \dots, v_j)$  pour tout  $1 \leq j \leq k$ . Mais alors comme

$$\text{Vect}(v_1, \dots, v_j) \subset \text{Vect}(v_1, \dots, v_k),$$

nous concluons que  $\varphi(v_j) \in \text{Vect}(v_1, \dots, v_k)$  pour chaque  $1 \leq j \leq k$ , ce qui nous dit que le sous-espace  $\text{Vect}(v_1, \dots, v_k) \leq V$  est invariant sous  $\varphi$ .

- (ii)  $\Rightarrow$  (iii) Cela découle immédiatement de la définition de sous-espace invariant, puisque, pour tout  $1 \leq k \leq n$ , on a  $v_k \in \text{Vect}(v_1, \dots, v_k)$ .
- (iii)  $\Rightarrow$  (i) Si (iii) est vérifié, alors en écrivant chaque vecteur  $\varphi(v_k)$  comme une combinaison linéaire des vecteurs de la base  $\mathcal{B}$ , on n'utilise que les vecteurs  $v_1, \dots, v_k$ . Par conséquent, tous les coefficients sous la diagonale de la matrice  $[\varphi]_{\mathcal{B}}$  sont nuls. Ainsi, cette matrice est triangulaire supérieure. □

**Définition 21.1.3.**

- (i) Un endomorphisme linéaire  $\varphi$  de  $V$  est dit **trigonalisable** s'il vérifie la condition (iv) de la Proposition 21.1.2 ci-dessus.
- (ii) De même, une matrice  $A \in \mathbb{M}_{n \times n}(K)$  est dite trigonalisable si l'application linéaire  $\varphi_A$  est trigonalisable, ce qui est équivalent à dire qu'il existe une matrice inversible  $P \in \text{GL}(n, K)$  telle que  $P^{-1}AP$  est triangulaire supérieure.

**Exemple 21.1.4.** Considérez l'application linéaire  $\varphi_A : \mathbb{M}_{4 \times 1}(\mathbb{R}) \rightarrow \mathbb{M}_{4 \times 1}(\mathbb{R})$  définie par

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \mapsto \underbrace{\begin{pmatrix} 2 & 0 & 0 & 0 \\ -4 & 1 & 2 & 0 \\ -1 & 0 & 2 & -2 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_A \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

En prenant la matrice inversible  $P = \begin{pmatrix} 0 & 0 & 1 & 1 \\ -1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$  on a que  $P^{-1}AP = \begin{pmatrix} 1 & 1 & 3 & 1 \\ 0 & 2 & 1 & 3 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ .

- Comment trouver cette matrice? Notez que  $P$  est la matrice de changement de base  $[\text{id}]_{\mathcal{B}, \mathcal{E}}$ , où  $\mathcal{E}$  désigne la base canonique et  $\mathcal{B}$  la base ordonnée constituée des vecteurs

$$\text{(en ordre)} \quad v_1 = \begin{pmatrix} 0 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ -1 \\ -1 \\ 0 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{et} \quad v_4 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

- Comment trouver une base  $\mathcal{B}$  telle que  $[\varphi_A]_{\mathcal{B}}$  soit triangulaire supérieure?

Étape 1 Choisissons un vecteur propre de  $\varphi_A$ , disons  $v_1 = \begin{pmatrix} 0 \\ -1 \\ 0 \\ 0 \end{pmatrix}$ .

Étape 2 Complétons  $v_1$  en une base ordonnée  $\mathcal{B}_1 = (v_1, w_2, w_3, w_4)$  de  $\mathbb{M}_{4 \times 1}(\mathbb{R})$ . Supposons

$$w_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad w_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{et} \quad w_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Étape 3 Calculons

$$[\varphi_A]_{\mathcal{B}_1} = \begin{pmatrix} 1 & 4 & -2 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & -1 & 2 & -2 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Étape 4 Considérons l'application  $\varphi_{A_1} : \text{Vect}(w_2, w_3, w_4) \rightarrow \text{Vect}(w_2, w_3, w_4)$  définie par multiplication à gauche par la sous-matrice

$$A_1 = \begin{pmatrix} 2 & 0 & 0 \\ -1 & 2 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

et répétons les étapes précédentes.

Étape 5 Le vecteur  $v_2 = w_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$  est un vecteur propre de  $\varphi_{A_1}$ . Donc, si nous remplaçons

la base  $\mathcal{B}_1$  par une autre base  $\mathcal{B}_2 = (v_1, v_2, \tilde{w}_3, \tilde{w}_4)$  on trouvera que la matrice  $[\varphi_A]_{\mathcal{B}_2}$

Comparez l'algorithme avec la preuve du Théorème 21.1.6.

a la forme

$$\begin{pmatrix} 1 & a & b & c \\ 0 & 2 & d & e \\ 0 & 0 & f & g \\ 0 & 0 & h & i \end{pmatrix}.$$

Étape 6 L'étape suivante consiste à considérer l'application  $\varphi_{A_2} : \text{Vect}(\tilde{w}_3, \tilde{w}_4) \rightarrow \text{Vect}(\tilde{w}_3, \tilde{w}_4)$  définie par multiplication à gauche par la sous-matrice

$$A_2 = \begin{pmatrix} f & g \\ h & i \end{pmatrix}$$

et à répétez les étapes 1 à 3.

Étape 7 Nous continuons jusqu'à obtenir la base souhaitée.

AZ: **▲** Il est important de noter que cet algorithme implique de nombreux choix. Il n'existe pas de choix unique pour la base  $\mathcal{B}$ . En fait, je vous ai montré que le choix  $(v_1, v_2 = w_3, w_2, w_4)$  est également une possibilité.

- Finalement, notez que  $c_A(x) = c_\varphi(x) = (x-1)^2(x-2)^2$  est scindé dans  $\mathbb{R}[x]$ .

AZ: On peut en plus démontrer que  $\mu_g(1) = \mu_g(2) = 1 < 2 = \mu_a(1) = \mu_a(2)$ . Le Théorème 22.1.3 ci-dessus nous dit que ceci fournit donc un exemple d'opérateur trigonalisable mais non diagonalisable. Voir Définition 22.1.1

Le résultat suivant nous indique que si  $\varphi \in \mathcal{L}(V, V)$  est trigonalisable, alors le dernier point de l'exemple ci-dessus n'est pas une coïncidence car  $\varphi$  satisfait toujours une équation simple en fonction de ses valeurs propres. Voir aussi le Théorème 21.1.6 ci-dessous.

**Proposition 21.1.5.** Soit  $\varphi \in \mathcal{L}(V, V)$  et supposons qu'il existe une base ordonnée  $\mathcal{B}$  de  $V$  telle que la matrice  $[\varphi]_{\mathcal{B}}$  soit triangulaire supérieure avec les coefficients dans la diagonale  $\lambda_1, \dots, \lambda_n$ , c.-à-d.

$$[\varphi]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Alors,

- (i)  $(\varphi - \lambda_1 \cdot \text{id}) \cdot \dots \cdot (\varphi - \lambda_n \cdot \text{id}) = 0$ , et
- (ii) les valeurs propres de  $\varphi$  sont précisément les scalaires  $\lambda_1, \dots, \lambda_n$ .

*Démonstration.*

- (i) Soit  $\mathcal{B} = \{v_1, \dots, v_n\}$  une base ordonnée de  $V$  telle que la matrice  $[\varphi]_{\mathcal{B}}$  soit triangulaire supérieure comme dans l'énoncé. Il suffit alors d'observer que

$$\psi := (\varphi - \lambda_1 \cdot \text{id}) \circ \dots \circ (\varphi - \lambda_n \cdot \text{id})$$

est nul sur chaque vecteur  $v_k$  de la base  $\mathcal{B}$ . Cela s'explique par le fait que les opérateurs  $\varphi_i := \varphi - \lambda_i \cdot \text{id}$  et  $\varphi_j := \varphi - \lambda_j \cdot \text{id}$  commutent ( $\varphi_i \circ \varphi_j = \varphi_j \circ \varphi_i$ ) et, de plus, que,

pour tout  $1 \leq k \leq n$ , on a  $(\varphi - \lambda_k \cdot \text{id})(v_k) \in \text{Vect}(v_1, \dots, v_{k-1})$ . En effet, il suffit de constater que

$$\begin{aligned} \varphi(v_1) = \lambda_1 \cdot v_1 &\iff (\varphi - \lambda_1 \cdot \text{id})(v_1) = 0 \\ &\implies (\varphi - \lambda_1 \cdot \text{id}) \cdot \dots \cdot (\varphi - \lambda_k \cdot \text{id})(v_1) = 0 \quad \forall k = 1, \dots, n \\ &\implies \psi(v_1) = 0 \end{aligned}$$

et il en découlera par récurrence que pour chaque  $k = 1, \dots, n$

$$\begin{aligned} (\varphi - \lambda_k \cdot \text{id})(v_k) \in \text{Vect}(v_1, \dots, v_{k-1}) &\implies (\varphi - \lambda_1 \cdot \text{id}) \cdot \dots \cdot (\varphi - \lambda_k \cdot \text{id})(v_k) = 0 \\ &\implies (\varphi - \lambda_1 \cdot \text{id}) \cdot \dots \cdot (\varphi - \lambda_j \cdot \text{id})(v_k) = 0 \quad \forall j = k, \dots, n \\ &\implies \psi(v_k) = 0. \end{aligned}$$

(ii) Puisque  $\varphi(v_1) = \lambda_1 \cdot v_1$ , on a que  $\lambda_1$  est une valeur propre de  $\varphi$ . Choisissons  $k \in \{2, \dots, n\}$  et, pour chaque  $j \in \{1, \dots, n\}$ , posons  $W_j := \text{Vect}(v_1, \dots, v_j)$ . Comme pour tout  $j \in \{1, \dots, n\}$ , on a  $(\varphi - \lambda_j \cdot \text{id})(v_j) \in W_{j-1}$  et, si  $j \leq k$ , on a aussi que  $W_{j-1} \subset W_{k-1}$ , nous concluons que  $\varphi - \lambda_k \cdot \text{id}$  envoie  $W_k$  dans  $W_{k-1}$ . Mais  $\dim(W_k) = k$  et  $\dim(W_{k-1}) = k - 1$ , donc l'application  $\varphi - \lambda_k \cdot \text{id}$  n'est pas injective et il existe alors un vecteur non nul  $v \in \ker(\varphi - \lambda_k \cdot \text{id})$ . C'est-à-dire que  $\lambda_k$  est une valeur propre de  $\varphi$ . Ainsi, chaque élément de la diagonale de  $[\varphi]_{\mathcal{B}}$  est une valeur propre de  $\varphi$ . Pour démontrer que  $\varphi$  n'a pas d'autres valeurs propres, on considère le polynôme  $p(x) = (x - \lambda_1) \cdot \dots \cdot (x - \lambda_n) \in K[x]$ . Comme  $p(\varphi) = 0$ , ce polynôme doit être un multiple du polynôme minimal  $m_{\varphi}(x)$ . Mais alors, chaque racine de  $m_{\varphi}(x)$  est une racine de  $p(x)$ . Donc, toutes les valeurs propres de  $\varphi$  sont contenues dans la liste  $\lambda_1, \dots, \lambda_n$ . □

**AZ:** Notez que ce dernier résultat nous dit que si  $\varphi$  est trigonalisable, alors le polynôme minimal et le polynôme caractéristique de  $\varphi$  sont scindés.

Une question naturelle se pose alors : quand un opérateur linéaire est-il trigonalisable ? Pour répondre à cette question, nous concluons notre discussion par le résultat suivant.

**Théorème 21.1.6.** Soit  $V$  un  $K$ -espace vectoriel de dimension finie  $n$  et soit  $\varphi \in \mathcal{L}(V, V)$ . Alors  $\varphi$  est trigonalisable si et seulement si  $c_{\varphi}(x)$  est scindé dans l'anneau  $K[x]$ .

*Démonstration.* On a déjà montré que si  $\varphi$  est trigonalisable, alors  $c_{\varphi}(x)$  est scindé. Nous ne discuterons donc que de l'idée principale concernant l'autre implication.

Comme  $c_{\varphi}(x)$  est scindé,  $\varphi$  possède au moins une valeur propre  $\lambda_1$ . Soit  $v_1$  un vecteur propre associé à la valeur propre  $\lambda_1$ . Complétons  $\{v_1\}$  en une base ordonnée  $\mathcal{B} = (v_1, v_2, \dots, v_n)$  de  $V$  et posons  $A = [\varphi]_{\mathcal{B}}$ . Alors,

$$A = \left( \begin{array}{c|ccc} \lambda_1 & a_{12} & \dots & a_{1n} \\ \hline 0 & & & \\ \vdots & & \tilde{A} & \\ 0 & & & \end{array} \right)$$

où  $\tilde{A}$  est une matrice carrée à coefficients dans  $K$  de taille  $n - 1$ . Or, comme  $c_\varphi(x) = c_A(x) = (\lambda_1 - x)c_{\tilde{A}}(x)$ , on peut donc considérer un autre opérateur linéaire  $\tilde{\varphi}$ , cette fois dans l'espace  $\text{Vect}(v_2, \dots, v_n)$  de dimension  $n - 1$ , dont le polynôme caractéristique est également scindé, à savoir l'opérateur représenté par  $\tilde{A}$  par rapport à la base ordonnée  $(v_2, \dots, v_n)$ . Cela montre que pour prouver le théorème, nous pouvons simplement raisonner par récurrence sur la dimension de  $V$ . Autrement dit, nous pouvons répéter la première étape avec la paire  $(\text{Vect}(v_2, \dots, v_n), \tilde{\varphi})$ , remplacer les vecteurs  $v_2, \dots, v_n$  par une nouvelle base ordonnée de cet espace, où le premier sera un vecteur propre de  $\tilde{\varphi}$ , puis continuer ainsi jusqu'à obtenir une bonne base  $\mathcal{C}$  de  $V$  qui exposera  $\varphi$  comme trigonalisable.

AZ: Notez que la méthode cachée dans cette preuve a été utilisée dans Exemple 21.1.4.

□

Notez que, par le théorème fondamental de l'algèbre, chaque polynôme de  $\mathbb{C}[x]$  est scindé. Le théorème précédent implique alors que toute transformation linéaire d'un espace vectoriel de dimension finie sur  $\mathbb{C}$  est trigonalisable.

## Cours 24

---

### 22.1 Matrices diagonales et endomorphismes diagonalisables

On fixe un corps  $K$ , un  $K$ -espace vectoriel  $V$  de dimension finie  $n$  et un endomorphisme linéaire  $\varphi : V \rightarrow V$ .

**Définition 22.1.1.** L'application linéaire  $\varphi \in \mathcal{L}(V, V)$  est dite **diagonalisable** (sur  $K$ ) si elle possède une matrice diagonale par rapport à une certaine base de  $V$ . Autrement dit, il existe une base  $\mathcal{B}$  de  $V$  telle que  $[\varphi]_{\mathcal{B}}$  soit diagonale.

AZ: Notez que si  $\varphi$  est diagonalisable, alors  $\varphi$  est trigonalisable.

**Proposition 22.1.2.** Supposons que  $\lambda_1, \dots, \lambda_m$  soient des valeurs propres distinctes de  $\varphi$ . Alors la somme  $E_{\lambda_1} + \dots + E_{\lambda_m}$  est une somme directe. En particulier,

$$\dim(E_{\lambda_1}) + \dots + \dim(E_{\lambda_m}) = \mu_g(\lambda_1) + \dots + \mu_g(\lambda_m) \leq \dim(V) = n.$$

*Démonstration.* Pour montrer que la somme est une somme directe, supposons que  $v_1 + \dots + v_m = 0_V$ , où chaque  $v_i$  appartient à  $E_{\lambda_i}$ . Puisque les vecteurs propres associés à des valeurs propres distinctes sont linéairement indépendants (d'après Proposition 19.1.10, cours 21), cela implique que chaque  $v_i$  est égal à  $0_V$ . Ainsi,  $E_{\lambda_1} + \dots + E_{\lambda_m}$  est une somme directe, comme souhaité. □

AZ: Rappelez-vous que si  $V_1, \dots, V_m$  sont des sous-espaces de  $V$ . Alors  $V_1 + \dots + V_m$  est une somme directe si et seulement si la seule façon d'écrire  $0_V$  comme une somme  $v_1 + \dots + v_m$ , où chaque  $v_i \in V_i$ , est de prendre chaque  $v_i$  égal à  $0_V$ .

### 22.1.1 Conditions de diagonalisation

**Théorème 22.1.3.** Soient  $\lambda_1, \dots, \lambda_m$  les valeurs propres distinctes de  $\varphi$ . Alors les propriétés suivantes sont équivalentes :

- (i)  $\varphi$  est diagonalisable.
- (ii)  $V$  possède une base constituée des vecteurs propres de  $\varphi$ .
- (iii)  $V = E_{\lambda_1} \oplus \dots \oplus E_{\lambda_m}$
- (iv)  $\dim(V) = \dim(E_{\lambda_1}) + \dots + \dim(E_{\lambda_m}) = \mu_g(\lambda_1) + \dots + \mu_g(\lambda_m)$ .
- (v)  $c_\varphi(x)$  est scindé dans  $K[x]$  et pour chaque  $i = 1, \dots, m$  on a que  $\mu_g(\lambda_i) = \mu_a(\lambda_i)$ .

AZ:  Notez que je ne suppose pas que  $m = n$  !

*Démonstration.*

- (i)  $\iff$  (ii)  $\Rightarrow$  (v)  $\Rightarrow$  (iv)  
 $\varphi$  possède une matrice diagonale

$$\begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix}$$

par rapport à une base ordonnée  $\mathcal{B} = (v_1, \dots, v_n)$  de  $V$  si et seulement si  $\varphi(v_j) = \alpha_j \cdot v_j$  pour tout  $j = 1, \dots, n$ . Cela montre que (i) et (ii) sont équivalentes.

En plus, notez qu'en particulier les  $\alpha_j$ s doivent appartenir à la liste des valeurs propres  $\lambda_1, \dots, \lambda_m$ . Donc, si  $\varphi$  est diagonalisable, alors

$$c_\varphi(x) = (-1)^n (x - \lambda_1)^{d_1} \cdot \dots \cdot (x - \lambda_m)^{d_m}.$$

avec  $d_i = \mu_a(\lambda_i) = \mu_g(\lambda_i)$ , car

$$\mu_g(\lambda_i) = \dim(E_{\lambda_i}) \geq \#\{v_j \in \mathcal{B}; v_j \in E_{\lambda_i}\} = d_i = \mu_a(\lambda_i) \geq \mu_g(\lambda_i).$$

Finalement, l'implication (v)  $\Rightarrow$  (iv) est claire.

- (ii)  $\Rightarrow$  (iii)  $\Rightarrow$  (iv)  $\Rightarrow$  (ii)

Si (ii) est vrai, alors tout vecteur de  $V$  est une combinaison linéaire des vecteurs propres de  $\varphi$  et donc  $V = E_{\lambda_1} + \dots + E_{\lambda_m}$ . Or, d'après la Proposition 22.1.2, la somme est toujours directe. Par conséquent, (iii) est vérifiée.

Maintenant, si (iii) est vraie, c'est immédiat que (iv) est vraie aussi. Supposons donc que (iv) soit vrai. Choisissez une base de chaque espace propre  $E_{\lambda_i}$ ; rassemblez toutes ces bases pour former une liste  $v_1, \dots, v_n$  de vecteurs propres de  $V$ . Pour montrer que cette liste est libre, supposons

$$a_1 \cdot v_1 + \dots + a_n \cdot v_n = 0,$$

où  $a_1, \dots, a_n \in K$ . Pour chaque  $i = 1, \dots, m$ , soit  $u_i$  la somme de tous les termes  $a_j \cdot v_j$  tels que  $v_j \in E_{\lambda_i}$ . Ainsi, chaque  $u_i$  appartient à  $E_{\lambda_i}$ , et en plus

$$u_1 + \dots + u_m = 0.$$

Mais alors, puisque les vecteurs propres correspondant à des valeurs propres distinctes sont linéairement indépendants (voir Proposition 19.1.10, cours 21), cela implique que chaque  $u_i$  est égal à  $0_V$ . Et puisque chaque  $u_i$  est une somme de termes  $a_j \cdot v_j$ , où les  $v_j$  ont été choisis pour former une base de  $E_{\lambda_i}$ , cela implique que tous les scalaires  $a_1, \dots, a_n$  sont égaux à  $0_K$ . Par conséquent,  $(v_1, \dots, v_n)$  est une base de  $V$  et donc (iv) implique (ii). □

Notez que le Théorème 22.1.3 nous dit qu'en choisissant un ordre des valeurs propres distinctes, disons  $\lambda_1, \dots, \lambda_m$ , et en posant  $g_i = \mu_g(\lambda_i)$ , alors  $\varphi$  est diagonalisable si et seulement si il existe une base ordonnée  $\mathcal{B} = \underbrace{(v_{1_1}, \dots, v_{1_{g_1}}, v_{2_1}, \dots, v_{2_{g_2}}, \dots, v_{m_1}, \dots, v_{m_{g_m}})}_{n=g_1+\dots+g_m}$

de  $V$  avec  $\varphi(v_{i_j(i)}) = \lambda_i \cdot v_{i_j(i)}$ , pour tous  $i = 1, \dots, m$  et pour tous  $j(i) = 1, \dots, g_i$ . En plus, si tel est le cas, alors

$$[\varphi]_{\mathcal{B}} = \begin{pmatrix} D_{\lambda_1} & 0 & \dots & \dots & \dots & 0 \\ 0 & D_{\lambda_2} & \dots & \dots & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & D_{\lambda_{m-1}} & \dots & 0 \\ 0 & \dots & \dots & 0 & \dots & D_{\lambda_m} \end{pmatrix}$$

où chaque bloc  $D_{\lambda_i}$  est de taille  $g_i = \mu_g(\lambda_i)$  et a la forme

$$\begin{pmatrix} \lambda_i & 0 & \dots & \dots & \dots & 0 \\ 0 & \lambda_i & \dots & \dots & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & \dots & \lambda_i \\ 0 & \dots & \dots & 0 & \dots & 0 \end{pmatrix}.$$

**Corollaire 22.1.4.** Si le polynôme caractéristique  $c_{\varphi}(x)$  possède  $n$  racines distinctes (dans  $K$ ), alors  $\varphi$  est diagonalisable (sur  $K$ ).

Nous avons également le critère suivant :

**Proposition 22.1.5.**  $\varphi$  est diagonalisable (sur  $K$ ) si et seulement si  $m_{\varphi}(x)$ , le polynôme minimal de  $\varphi$ , est égal à

$$(x - \lambda_1) \cdot \dots \cdot (x - \lambda_m)$$

pour une certaine liste de scalaires distincts  $\lambda_1, \dots, \lambda_m \in K$ .

*Démonstration.* Ce résultat est facultatif et nous ne donnons ici que l'idée de la démonstration.

Supposons d'abord que  $\varphi$  soit diagonalisable. Il existe donc une base  $(v_1, \dots, v_n)$  de  $V$  constituée des vecteurs propres de  $\varphi$ . Soient  $\lambda_1, \dots, \lambda_m$  les valeurs propres distinctes de  $\varphi$ . Alors, pour chaque  $v_j$ , il existe une seule valeur propre  $\lambda_i$  telle que  $(\varphi - \lambda_i \cdot \text{id})(v_j) = 0_V$ . Ainsi,

$$(\varphi - \lambda_1 \cdot \text{id}) \cdot \dots \cdot (\varphi - \lambda_m \cdot \text{id})(v_j) = 0$$

pour chaque  $v_j$ . De plus, soit  $m = 1$ , soit si nous omettons l'un des opérateurs  $\varphi - \lambda_i \cdot \text{id}$  dans l'expression ci-dessus, alors nous pouvons trouver au moins un vecteur  $v_j$  qui ne sera pas annihilé par les autres. Cela implique que le polynôme minimal de  $\varphi$  est égal à

$$(x - \lambda_1) \cdot \dots \cdot (x - \lambda_m).$$

Pour démontrer l'implication dans l'autre sens, on argumente par récurrence sur  $m$  en utilisant le fait que  $(\varphi - \lambda_1 \cdot \text{id}) \cdot \dots \cdot (\varphi - \lambda_m \cdot \text{id}) = 0$  et que  $V = \text{im}(\varphi - \lambda_i \cdot \text{id}) \oplus \ker(\varphi - \lambda_i \cdot \text{id})$ .  $\square$

## Cours 25

---

On fixe un corps  $K$ , un  $K$ -espace vectoriel  $V$  de dimension finie  $n$ .

### 23.1 (\*) Opérateurs commutatifs

#### Définition 23.1.1.

- (i) Deux opérateurs linéaires  $\varphi$  et  $\psi$  définis sur un même espace vectoriel  $V$  commutent si  $\varphi \circ \psi = \psi \circ \varphi$ .
- (ii) Deux matrices carrées  $A$  et  $B$  de même taille (et à coefficients dans le même corps) commutent si  $AB = BA$ .

**Théorème 23.1.2.** *Supposons que  $\varphi, \psi \in \mathcal{L}(V, V)$  et que  $\mathcal{B} = (v_1, \dots, v_n)$  soit une base ordonnée de  $V$ . Alors,*

- (i)  $\varphi$  et  $\psi$  commutent si et seulement si les matrices  $[\varphi]_{\mathcal{B}}$  et  $[\psi]_{\mathcal{B}}$  commutent.
- (ii) Supposons que  $\varphi$  et  $\psi$  commutent et que  $\lambda \in K$  soit une valeur propre de  $\varphi$ . Alors  $E_{\lambda}$  est invariant sous  $\psi$ .
- (iii) Supposons que  $\varphi$  et  $\psi$  soient diagonalisables. Alors,  $\varphi$  et  $\psi$  peuvent être représentées par des matrices diagonales par rapport à la même base si et seulement si  $\varphi$  et  $\psi$  commutent.
- (iv) Si  $K = \mathbb{C}$  et  $\varphi$  et  $\psi$  commutent, alors  $\varphi$  et  $\psi$  ont un vecteur propre commun et il existe une base de  $V$  par rapport à laquelle  $\varphi$  et  $\psi$  sont représentées par des matrices triangulaires supérieures.

*Démonstration.*

- (i) On a que  $\varphi \circ \psi = \psi \circ \varphi \iff [\varphi \circ \psi]_{\mathcal{B}} = [\psi \circ \varphi]_{\mathcal{B}} \iff [\varphi]_{\mathcal{B}} \cdot [\psi]_{\mathcal{B}} = [\psi]_{\mathcal{B}} \cdot [\varphi]_{\mathcal{B}}$ .
- (ii) Si  $v \in E_{\lambda}$ , alors  $\varphi(\psi(v)) = \psi(\varphi(v)) = \psi(\lambda \cdot v) = \lambda \cdot \psi(v)$ , ce qui nous dit que  $\psi(v) \in E_{\lambda}$ .
- (iii) Les matrices diagonales de même taille commutent toujours, donc en utilisant (i), l'implication  $\Rightarrow$  est claire.

Pour démontrer l'implication dans l'autre sens, supposons maintenant que  $\varphi$  et  $\psi$  sont des opérateurs diagonalisables et commutatifs. Soient  $\lambda_1, \dots, \lambda_m$  les valeurs propres distinctes de  $\varphi$ . Puisque  $\varphi$  est diagonalisable, on sait d'après le Théorème 22.1.3 que

$$V = E_{\lambda_1} \oplus \dots \oplus E_{\lambda_m}$$

Or, pour chaque  $i = 1, \dots, m$ , le sous-espace  $E_{\lambda_i}$  est invariant par  $\psi$  par (ii). Puisque  $\psi$  est diagonalisable, cela implique que la restriction de  $\psi$  à chacun de ces espaces propres de  $\varphi$  est diagonalisable aussi. Par conséquent, pour chaque  $i = 1, \dots, m$ , il existe une base de  $E_{\lambda_i}$  constituée des vecteurs propres de  $\psi$ . La combinaison de ces bases donne une base  $\mathcal{C}$  de  $V$ , chaque vecteur de cette base étant un vecteur propre à la fois de  $\varphi$  et de  $\psi$ . Ainsi,  $[\varphi]_{\mathcal{C}}$  et  $[\psi]_{\mathcal{C}}$  sont des matrices diagonales, comme souhaité.

Pourquoi? Quel est le polynôme minimal de la restriction?

- (iv) Comme  $K = \mathbb{C}$ ,  $\varphi$  possède au moins un vecteur propre associé à une certaine valeur propre  $\lambda$ . Or, comme  $E_{\lambda}$  est invariant par  $\psi$  lorsque  $\varphi$  et  $\psi$  commutent, la restriction de  $\psi$  à cet espace  $E_{\lambda}$  possède également au moins un vecteur propre, à la fois pour  $\varphi$  et pour  $\psi$ .

Maintenant, pour prouver la dernière partie de l'énoncé, nous pouvons procéder par récurrence sur  $n = \dim(V)$ . Le résultat souhaité est vérifié si  $n = 1$  car toutes les matrices  $1 \times 1$  sont déjà triangulaires supérieures. Puis, si  $n > 1$  et on suppose que le résultat souhaité est vérifié pour tous les espaces vectoriels complexes de dimension  $n - 1$ , il suffit d'observer que  $\varphi$  et  $\psi$  ont un vecteur propre commun, disons  $v_1$ , de considérer une somme directe  $V = \text{Vect}(v_1) \oplus W$  et les opérateurs  $\tilde{\varphi} = \pi_W \circ \varphi$  et  $\tilde{\psi} = \pi_W \circ \psi$ , où  $\pi_W : V \rightarrow W$  est la projection sur  $W$ , c'est-à-dire l'application linéaire

$$\pi_W(\underbrace{\alpha \cdot v_1 + w}_{\in \text{Vect}(v_1) \oplus W}) = w.$$

L'hypothèse d'induction peut leur être appliquée (ou mieux, à leur restriction à  $W$ ). Il existe une base  $v_2, \dots, v_n$  de  $W$  par rapport à laquelle  $\tilde{\varphi}$  et  $\tilde{\psi}$  ont toutes deux des matrices triangulaires supérieures. En plus,  $(v_1, \dots, v_n)$  constitue une base ordonnée de  $V$ , et, par construction, les matrices de  $\varphi$  et  $\psi$  sont triangulaires supérieures dans cette base.

AZ: Notez que pour chaque  $w \in W$  il existe  $\alpha \in K$  tel que

$$\begin{aligned} (\tilde{\psi} \circ \tilde{\varphi})(w) &= \tilde{\psi}(\pi_W(\varphi(w))) = \tilde{\psi}(\varphi(w) - \alpha \cdot v_1) \\ &= \pi_W(\psi(\varphi(w) - \alpha \cdot v_1)) \\ &= \pi_W(\psi(\varphi(w))), \end{aligned}$$

où dans la dernière inégalité nous utilisons le fait que  $v_1$  est vecteur propre de  $\psi$  et que  $\pi_W(v_1) = 0_V$ . De façon similaire, on peut déduire que  $(\tilde{\varphi} \circ \tilde{\psi})(w) = \pi_W(\varphi(\psi(w)))$ . Mais comme  $\varphi$  et  $\psi$  commutent,

$$\pi_W(\psi(\varphi(w))) = \pi_W(\varphi(\psi(w)))$$

et donc les restrictions de  $\tilde{\varphi}$  et  $\tilde{\psi}$  à  $W$  commutent aussi. □

**Corollaire 23.1.3.** Si  $K = \mathbb{C}$  et  $\varphi$  et  $\psi$  commutent, alors :

- (i) toute valeur propre de  $\varphi + \psi$  est une valeur propre de  $\varphi$  plus une valeur propre de  $\psi$ , et
- (ii) toute valeur propre de  $\varphi \circ \psi (= \psi \circ \varphi)$  est une valeur propre de  $\varphi$  multipliée par une valeur propre de  $\psi$ .

### 24.1 (\*) Espaces munis d'un produit scalaire (non examinable)

AZ: To be added.