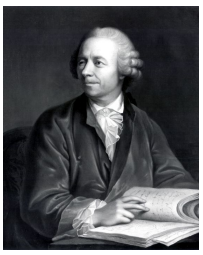


Cours Euler

Module 3

Algèbre Linéaire

C. Mermoud

2024-2025

I. Les groupes

Dans ce module d'algèbre linéaire, nous étudierons donc des phénomènes linéaires : espaces et sous-espaces vectoriels, applications linéaires, systèmes d'équations linéaires, etc. L'année passée, vous avez développé des techniques d'algèbre linéaire pour résoudre des questions géométriques dans le plan ou l'espace euclidien réel, $\mathbb{R}^2$ et $\mathbb{R}^3$. Vous avez aussi vu d'autres espaces vectoriels où ces méthodes s'appliquent : les polynômes à coefficients réels, les fonctions réelles d'une variable réelle. Au début de ce module, nous commencerons par parler de cette structure de corps dont les nombres réels sont munis. Il y a d'autres corps dans la nature, certains que nous connaissons depuis longtemps comme les nombres rationnels ou les nombres complexes, et d'autres que vous n'avez peut-être encore jamais vus !

1 Lois de composition

Lorsque l'on a deux nombres réels en main, on peut les additionner ou les multiplier. Ces deux opérations, l'addition et la multiplication, sont des lois de composition.

Définition 1.1. Une *loi de composition* sur un ensemble E est une application $E \times E \to E$.
Il s'agit donc une opération *interne à* E ou *stable dans* E qui fait correspondre à un couple (x, y) d'éléments de E un troisième élément que l'on notera souvent $x * y$.

Dans des situations particulières, on remplace la notation $x * y$ par une notation plus classique, ce que nous ferons déjà dans les exemples suivants.

Exemple 1.2.

a) L'addition $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ est une loi de composition notée $n + m$. La multiplication complexe $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ est une loi de composition notée $z \cdot z'$.

b) Il y a aussi des lois de composition d'une tout autre nature.
Soit X un ensemble et posons $E = \mathcal{P}(X)$. Alors la réunion et l'intersection définissent des lois de composition sur E. La première fait correspondre à deux sous-ensembles $A, B \subset X$ leur réunion $A \cup B$ et la seconde leur fait correspondre leur intersection $A \cap B$.

c) Dans $\mathbb{N}$, la différence

Nous nous intéressons uniquement à certaines lois de composition, celles qui satisfont des propriétés de "symétrie". L'associativité permet de se passer des parenthèses :

Définition 1.3. Une loi de composition $*$ sur un ensemble E est *associative* si

Exemple 1.4.

a) L'addition $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$ est une loi de composition associative puisque $a + (b + c) = (a + b) + c$ pour tous nombres réels a, b et c.

b) La soustraction

c) L'intersection est associative sur $\mathcal{P}(X)$. En effet, un élément appartient à $A \cap (B \cap C)$ si et seulement si il appartient à la fois à A et à $B \cap C$, c'est-à-dire à A, B et C, ou encore à $A \cap B$ et à C. Ainsi $A \cap (B \cap C) = (A \cap B) \cap C$.

Proposition 1.5. *Si $*$ est une loi de composition associative sur E, alors*

$$(x * y) * (z * t) = x * ((y * z) * t)$$

pour tous $x, y, z, t \in E$.

Démonstration.

□

De manière générale, on peut se passer du parenthésage lors de la composition de n éléments pour tout $n \geq 3$. Une autre propriété essentielle qui nous permet de travailler simplement avec l'addition est l'existence du zéro, ou celle de 1 pour la multiplication.

Définition 1.6. Une loi de composition $*$ sur un ensemble E admet un *élément neutre* s'il existe $e \in E$ tel que $e * x = x = x * e$ pour tout $x \in E$.

Exemple 1.7.
Pour la multiplication complexe,

Pour la réunion dans $\mathcal{P}(X)$,

Pour l'intersection dans $\mathcal{P}(X)$,

Pour la soustraction dans $\mathbb{Z}$,

Toute loi de composition admet au plus un élément neutre. La preuve utilise un principe de comparaison bien utile.

Proposition 1.8. *Si e et e' sont des éléments neutres pour une loi de composition $*$ sur E, alors*

$$e = e'.$$

Démonstration.

□

Le rôle de l'unité dans la multiplication est plus important dans $\mathbb{Q}$ que dans $\mathbb{Z}$:
dans $\mathbb{Q}$, on peut "inverser" tous les éléments non nuls : si $r = \frac{a}{b}$ et $a \neq 0$, alors $s = \frac{b}{a}$ est l'inverse de r dans le sens où $r \cdot s = 1$.

Définition 1.9. Soit $*$ une loi de composition sur un ensemble E qui admet un élément neutre e. Un élément $x \in E$ est *inversible à gauche* (respectivement à droite) s'il existe un élément $y \in E$ tel que $y * x = e$ (respectivement $x * y = e$).

Exemple 1.10. Quel est l'inverse (à gauche et à droite) de $A \subset X$ pour la réunion dans $\mathcal{P}(X)$?

Théorème 1.11. *Soit $*$ une loi de composition associative sur un ensemble E admettant un élément neutre. Si un élément x admet un inverse à gauche y et un inverse à droite z, alors $y = z$. On appelle cet élément l'inverse de x et on le note x^{-1}. L'inverse de x, s'il existe, est unique.*

Démonstration. Si $y * x = e = x * z$, on utilise l'astuce suivante :

□

Pour terminer cette première partie concernant les lois de composition, nous nous intéressons à une dernière propriété, celle de l'importance de l'ordre.

Définition 1.12. Une loi de composition $*$ sur un ensemble E est *commutative* si $x * y = y * x$ pour tous $x, y \in E$. Dans ce cas, on dit que les éléments x et y commutent entre eux.

La vie n'est en général pas commutative. S'habiller le matin puis se rendre à l'école ne fait pas le même effet que se rendre à l'école puis s'habiller ...
Par contre, dans un ensemble E muni d'une loi de composition associative et commutative, ni l'ordre, ni le parenthésage n'importent.

Exemple 1.13.
L'addition est commutative dans $\mathbb{R}$, donc $a + b = b + a$ pour tous nombres réels a et b.

2 Les groupes

Nous continuons en établissant une hiérarchie parmi les ensembles munis d'une, puis, la semaine suivante, de deux lois de composition.

Définition 2.1. Un *groupe* est un ensemble G muni d'une loi de composition associative, qui admet un élément neutre et pour laquelle tout élément est inversible. Un groupe est dit *commutatif* ou *abélien* si la loi de composition est commutative.

Remarque 2.2. Un peu d'histoire. Le terme de groupe abélien honore le mathématicien norvégien Niels Henrik Abel (1802 - 1829), célèbre pour ses travaux sur l'impossibilité de résoudre les équations du cinquième degré par radicaux, mais aussi pour être mort à l'âge de 26 ans de la tuberculose.

Exemple 2.3.

a) Les nombres réels munis de l'addition forment un groupe abélien. Nous avons déjà vu un peu plus tôt que l'addition est associative et commutative et que zéro est l'élément neutre.
Pour l'addition, l'inverse de $x \in \mathbb{R}$ est en fait *l'opposé* $-x$ puisque $x + (-x) = 0$.

b) Les nombres rationnels non-nuls $\mathbb{Q}^*$

Exemple 2.4. Considérons l'ensemble $E = \{0, 1, 2\}$ et définissons une loi de composition, appelée addition et notée $+$, en précisant sa table (on lit $a + b$ dans la ligne de a et la colonne de b) :

$+$	0	1	2
0			
1			
2			

On voit que cette loi de composition est commutative car

L'élément neutre est

Tous les éléments sont inversibles car

Associativité :

On appelle ce groupe abélien $\mathbb{Z}/3\mathbb{Z}$.

Définition 2.5. Soit $(G, *)$ un groupe. Un sous-ensemble $H \subset G$ est un *sous-groupe* si la loi de composition de G définit une loi de composition sur H qui en fait un groupe.

Théorème 2.6. *Soit $(G, *)$ un groupe. Alors un sous-ensemble non-vide $H \subset G$ est un sous-groupe si et seulement si $x * y$ et y^{-1} appartiennent à H pour tous $x, y \in H$.*

Démonstration. Si H est un sous-groupe de G, la condition est vraie car $*$ est une loi de composition sur H pour laquelle tout élément de H admet un inverse (dans H).
Supposons maintenant que les deux conditions sont vérifiées. Alors $*$ est une loi de composition sur H puisque

Elle est associative car

Comme H est non-vide, on peut choisir un élément $x \in H$. Alors,

□

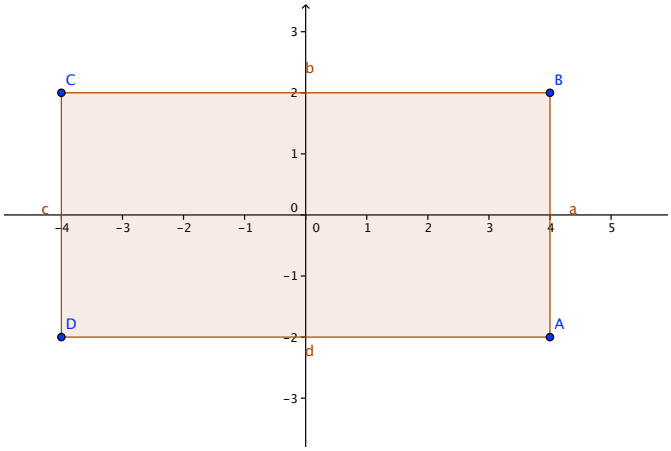
La possibilité de parler de sous-groupe simplifie parfois considérablement la vérification des axiomes de groupe.

Exemple 2.7.

a) L'ensemble des isométries du plan muni de la composition forme un groupe non abélien. En effet, la composition de deux isométries est une isométrie, l'identité est l'élément neutre, la composition est associative, et enfin chaque isométrie admet une isométrie inverse.

b) L'ensemble des isométries du plan qui fixent l'origine forment un groupe. En effet,

c) L'ensemble des isométries qui fixent globalement un rectangle centré en l'origine forment un groupe, car il s'agit d'un sous-groupe du groupe des isométries qui fixent l'origine. On l'appelle le groupe des isométries du rectangle ou le *groupe du matelas*. Mais quels sont ses éléments ?



Il y a quatre façons de replacer son matelas dans le lit :

Proposition 2.8.
Soit $n \in \mathbb{N}$. L'ensemble $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ muni de l'addition usuelle forme un groupe abélien.

Démonstration. Il suffit de se rendre compte qu'il s'agit d'un sous-groupe de $(\mathbb{Z}, +)$. En effet la somme de nk et nk' est encore un multiple de n et l'opposé de nk est $-nk = n(-k) \in n\mathbb{Z}$. □

Il s'agit en fait des *seuls* sous-groupes de $\mathbb{Z}$.

II. Les corps

Nous avons passé une semaine à étudier les lois de composition et la notion de groupe, un ensemble muni d'une loi de composition particulièrement chouette. Aujourd'hui, pour abstraire l'essence des nombres réels, rationnels ou complexes, nous allons ajouter une deuxième loi de composition, compatible avec la première. Nous serons ainsi amenés à considérer des objets appelés *anneaux* dont les plus aboutis sont les *corps*.

1 Les anneaux

Lorsque l'on a deux nombres réels dans la main, on peut les additionner ou les multiplier. Ces deux opérations, l'addition et la multiplication, sont des lois de composition.

Définition 1.1. Un *anneau* est un ensemble A muni de deux lois de compositions, notées $+$ et $\cdot$, telles que :

a) $(A, +)$ est un groupe abélien ;

b) la multiplication est associative et possède un élément neutre, noté 1_A ou 1 ;

c) la multiplication est distributive par rapport à l'addition :

$$x(y+z) = xy + xz \text{ et } (x+y)z = xz + yz,$$

pour tous $x, y, z \in A$.

On dit que l'anneau $(A, +, \cdot)$ est *commutatif* si la multiplication est commutative.

Voici quelques propriétés élémentaires, valides dans tous les anneaux, qui permettent aussi de simplifier les notations. Les preuves sont basées principalement sur la distributivité.

Lemme 1.2. *Soient $x, y \in A$. Alors :*

a) $0 \cdot x = 0 = x \cdot 0$ *;*

b) $(-1) \cdot x = -x = x \cdot (-1)$ *;*

c) $(-x)y = -xy = x(-y)$.

Démonstration.

a) On écrit $0 = 0 + 0$ et on multiplie à droite par $x \in A$. Il vient

b) En utilisant a), on peut écrire

c) En utilisant b), on peut écrire

□

Exemple 1.3. Les nombres entiers $\mathbb{Z}$ forment un anneau avec l'addition et la multiplication usuelle. Nous savons que $(\mathbb{Z}, +)$ est un groupe abélien, que la multiplication est une loi de composition associative pour laquelle 1 est l'élément neutre. Enfin, la multiplication est définie de telle sorte que la distributivité soit vérifiée puisqu'on pose par récurrence $(n + 1)k = nk + k$.
De même, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ forment des anneaux qui contiennent chaque fois le précédent.

Exemple 1.4. L'*anneau nul* n'a qu'un élément, à savoir 0. On définit $0 + 0 = 0$ et $0 \cdot 0 = 0$.

Exemple 1.5. L'ensemble des parties $\mathcal{P}(E)$ d'un ensemble E est un anneau.

Il nous reste à vérifier la distributivité, ce que nous ferons sur la base d'un diagramme de Venn :

On appelle cet anneau *booléen* car $A \cap A = A$ pour tout $A \subset E$.
En notation muliplicative, cette propriété s'écrit $x \cdot x = x$, c'est-à-dire, $x^2 = x$.

Définition 1.6. Soit A un anneau. Un sous-ensemble $B \subset A$ est un *sous-anneau* de A si les lois de composition $+$ et $\cdot$ de A définissent des lois de composition sur B qui en font un anneau.

Exemple 1.7. Puisque l'addition et la multiplication des nombres réels coïncident avec ces opérations définies sur les nombres entiers, nous en déduisons que $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.

Comme dans le cas des sous-groupes, il existe un critère pratique et écologique du point de vue du gain d'énergie qui permet de reconnaître les sous-anneaux.

Proposition 1.8. *Soit A un anneau.*
Un sous-ensemble $B \subset A$ est un sous-anneau de A si et seulement si
$\forall x, y \in B$, les éléments appartiennent à B.

Démonstration. $\Rightarrow$: vrai puisque B est un sous-anneau donc un anneau.
$\Leftarrow$:
Pour que $(B, +)$ soit un groupe, on doit avoir
De plus, l'addition est commutative car
Pour que $(B, +, \cdot)$ soit un anneau,

□

Nous avons vu la semaine dernière que les conditions sur l'addition forcent l'élément 0 à faire partie de B. Pourquoi faut-il alors demander explicitement la présence de 1 dans B ?
C'est le manque d'inverse qui nous force à le faire. Par exemple, le sous-groupe des nombres pairs ne forme pas un sous-anneau de $\mathbb{Z}$, même si le produit de deux nombres pairs est bel et bien pair.

Exemple 1.9. Considérons l'ensemble $M_2(\mathbb{R})$ des matrices carrées 2×2 à coefficients réels.
L'addition est définie "terme à terme" et la multiplication est définie "ligne par colonne" :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix} =$$

Il n'est pas difficile de vérifier que $M_2(\mathbb{R})$ forme un anneau.
Le sous-ensemble B des matrices de la forme $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ forme un sous-anneau de $M_2(\mathbb{R})$.
En effet, on voit que la somme et l'opposé de matrices de cette forme sont encore dans B et que la matrice unité est aussi dans B. Il reste donc à vérifier que le produit de deux matrices de B est dans B, ce que nous faisons sans attendre :

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} x & y \\ -y & x \end{pmatrix} =$$

Tiens, tiens, on retrouve les formules définies pour la multiplication complexe...

2 Les corps

Voici enfin la définition d'un corps, traduit de l'allemand "Körper", mot qui explique aussi l'utilisation de la lettre K pour désigner un tel objet.

Définition 2.1. Un *corps* K est un anneau commutatif dans lequel $0 \neq 1$ et tout élément non-nul est inversible.

Exemple 2.2.

Proposition 2.3. *Soit K un corps et $x, y \in K$. Si $xy = 0$, alors soit $x = 0$, soit $y = 0$.*

Démonstration.

□

Remarque 2.4. En pratique, on utilise surtout la contraposée de cette proposition :

Voyons maintenant le plus petit corps du monde.

Exemple 2.5. Le corps à deux éléments. L'ensemble $\{0, 1\}$ muni de l'addition pour laquelle $1 + 1 = 0$ est un groupe abélien. Nous définissons la multiplication en posant

On utilise souvent la notation $\mathbb{F}_2$ pour le corps à deux éléments.

3 Le corps à p éléments

Nous aimerions maintenant généraliser l'exemple du corps à deux éléments et construire des corps à trois, cinq, sept, ou onze éléments ! Il nous faut à tout prix trouver une méthode qui nous évitera de devoir démontrer à la main l'associativité et la distributivité...

Définition 3.1. Soit n un nombre entier naturel.
Les entiers a et b sont *congruents* modulo n si leur différence $a - b$ est un multiple de n.
On note alors $a \equiv b (\mathrm{mod}\, n)$, ou $a \equiv b(n)$ ou même $a \equiv b$ si le contexte est clair.
La classe de congruence d'un nombre entier a est notée $[a]$.
L'ensemble des classes d'équivalence (de congruence modulo n) est noté $\mathbb{Z}/n\mathbb{Z}$.

Ainsi 7 et 11 sont congruents modulo 4. La classe de congruence de 7 modulo 4 (ou de manière équivalente celle de 11) est formée de tous les nombres entiers de la forme

Le fait que la classe d'équivalence est bien définie découle de la proposition suivante.

Proposition 3.2. *La relation de congruence est une relation d'équivalence.*

Démonstration.
Réflexivité :

Symétrie :

Transitivité :

□

Nous pouvons maintenant définir une addition et une multiplication sur les classes de congruence grâce aux opérations homonymes sur les entiers. Il y a n classes de congruence dans $\mathbb{Z}$ modulo n : $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ puisque tout entier k est congru à son reste de la division par n.

Définition 3.3. Soient $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$. Alors la *somme* est définie par $[a] + [b] = [a + b]$ et le *produit* est défini par $[a] \cdot [b] = [ab]$.

Nous devons vérifier que ces définitions ne dépendent pas du choix du représentant de la classe de congruence. Pour la somme par exemple, si $a \equiv a' (\mathrm{mod}\, n)$ et $b \equiv b' (\mathrm{mod}\, n)$, alors $(a + b) - (a' + b') = (a - a') + (b - b')$ est un multiple de n. Ainsi, $(a + b) = (a' + b') (\mathrm{mod}\, n)$.

Les autres vérifications sont similaires.

Théorème 3.4.
L'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes de congruence modulo n forme un anneau commutatif.

Démonstration. Tous les axiomes sont vérifiés parce qu'ils le sont dans $\mathbb{Z}$.
Prenons par exemple l'associativité de la multiplication. Soient $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$. Alors
$([a] \cdot [b]) \cdot [c] = [a \cdot b] \cdot [c] = [(a \cdot b) \cdot c] = [a \cdot (b \cdot c)] = [a] \cdot [b \cdot c] = [a] \cdot ([b] \cdot [c])$.
Les autres vérifications sont similaires.

□

Exemple 3.5. Il existe un anneau ayant 6 éléments $[0], [1], [2], [3], [4], [5]$. Dans cet anneau on calcule par exemple $[2] + [5] = [\quad]$ ou encore $[2]\,[3] = [\quad]$. En particulier, cet anneau

Théorème 3.6. *L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier.*

Démonstration.
$\Rightarrow$ par contraposée : Si p n'est pas premier, on peut l'écrire comme produit rs avec $r, s > 1$. Alors,

$\Leftarrow$ directement : Supposons que p est un nombre premier. Nous devons montrer que tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible. Soit $1 \leq a \leq p-1$ et $[a]$ sa classe de congruence modulo p. Considérons l'ensemble $\{a, 2a, \ldots, (p-1)a\}$. Nous affirmons que ces éléments appartiennent à $p-1$ classes de congruence modulo p distinctes. En effet,

□

Exemple 3.7. L'anneau $\mathbb{Z}/6\mathbb{Z}$, rencontré il y a un instant et qui n'est pas un corps, a la table de multiplication suivante où on note k au lieu de $[k]$ pour alléger la notation :

$\cdot$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

III. Espaces vectoriels

Nous savons donc ce qu'est un corps, et nous en avons une bonne brochette à disposition en cas de besoin : non seulement $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, mais aussi les corps $\mathbb{F}_p$ de p éléments, pour tout p premier. Nous allons maintenant développer la théorie des espaces vectoriels sur un corps K, c'est-à-dire des droites, plans, espaces, hyper-espaces construits sur K, où l'on peut additionner les "vecteurs" entre eux et les multiplier par des scalaires de K, tout comme vous l'avez fait pour les classes d'équivalence de flèches dans le plan réel et l'espace réel.

1 Définition et propriétés élémentaires

Soit K un corps. On note 0_K le zéro, l'élément neutre additif, et 1_K l'unité, l'élément neutre multiplicatif, de K. Ce corps est souvent appelé le *corps de base* des K-espaces vectoriels que nous sommes sur le point de définir.

Définition 1.1. Un *espace vectoriel* sur K ou K*-espace vectoriel* est un groupe abélien $(V, +)$, noté additivement, muni d'une *action* de K, c'est-à-dire une application $K \times V \to V$ notée multiplicativement $(\lambda, v) \mapsto \lambda v$, de sorte que :

a)

b)

c)

On appelle *vecteurs* les éléments de V et *scalaires* les éléments de K.

Voici quelques propriétés élémentaires, valides dans tous les espaces vectoriels.

Lemme 1.2. *Soient $\lambda, \lambda_1, \ldots, \lambda_n \in K$ et $v, v_1, \ldots, v_m \in V$. Alors :*

a) $0_K \cdot v = 0_V = \lambda \cdot 0_V$;

b) $(-\lambda)v = -\lambda v = \lambda(-v)$;

c) $\left(\sum_{i=1}^{n} \lambda_i\right) \cdot \left(\sum_{j=1}^{m} v_j\right) = \left(\sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_i v_j\right)$.

Démonstration.

a) On écrit $0_K = 0_K + 0_K$ et on conclut comme la semaine passée.

b) On calcule par exemple $(-\lambda)v + \lambda v = (-\lambda + \lambda)v = 0_K \cdot v = 0_V$, si bien que $(-\lambda)v = -\lambda v$.

c) Découle de la distributivité et se montre par récurrence sur m et sur n.

□

Commençons par les exemples évidents.

Exemple 1.3. Tout ensemble contenant uniquement l'élément nul d'un corps K est un espace vectoriel sur K. On parle de l'espace vectoriel nul.

Exemple 1.4. Le corps K lui-même est toujours un espace vectoriel sur K. L'action est alors simplement la multiplication de K.

Exemple 1.5. Si V et W sont deux K-espaces vectoriels, on munit $V \times W$ de la structure d'espace vectoriel *produit*. La somme est $(v, w) + (v', w') = (v + v', w + w')$ et l'action est définie par $\lambda(v, w) = (\lambda v, \lambda w)$. Ainsi le plan réel $\mathbb{R} \times \mathbb{R}$ est un espace vectoriel. Les éléments sont

Exemple 1.6. Soit X un ensemble et $\mathcal{F}(X, K)$ l'ensemble de toutes les applications $f : X \to K$.

On définit l'addition "point par point" en posant

et l'action en posant

On vérifie facilement qu'il s'agit d'un espace vectoriel sur K.

Lorsque $X = \{x, y\}$ est un ensemble de deux éléments, alors $\mathcal{F}(X, K)$ s'identifie à $K \times K$ puisqu'une application f est complètement déterminée par la donnée de deux images $f(x)$ et $f(y)$.
En revanche, lorsque X est un ensemble infini, cet espace vectoriel devient très grand !
Par exemple, lorsque $X = \mathbb{N}$, les applications $f : \mathbb{N} \to K$ sont toutes les suites dans K.
Lorsque X est encore plus grand, comme $\mathbb{R}$, on obtient en particulier l'espace vectoriel $\mathcal{F}(\mathbb{R}, \mathbb{R})$ de toutes les fonctions réelles, continues ou non !

2 Les sous-espaces vectoriels

Tout comme les groupes contiennent des sous-groupes et les anneaux contiennent des sous-anneaux, les espaces vectoriels contiennent des sous-espaces vectoriels. Tout juste après la définition, nous verrons un critère qui permet de les reconnaître.

Définition 2.1. Soit V un K-espace vectoriel.
Un sous-ensemble non-vide $W \subset V$ est un *sous-espace vectoriel* de V si l'addition et l'action de V se restreignent à W et le munissent d'une structure de K-espace vectoriel.

Exemple 2.2. Considérons $\mathbb{R}^3$ le $\mathbb{R}$-espace vectoriel des triplets (a, b, c) de nombres réels.
Soit le sous-ensemble $W = \{(a, b, c) \mid a + b + c = 0\}$.
C'est un sous-espace vectoriel de $\mathbb{R}^3$ car

Cet exemple indique qu'il y a en général peu d'éléments à vérifier pour voir si un sous-ensemble est un sous-espace vectoriel.

Proposition 2.3. *Soit V un K-espace vectoriel et $W \subset V$. Alors W est un sous-espace de V si et seulement si*

a) $0 \in W$;

b) $x + y \in W$ *pour tous* $x, y \in W$;

c) $\lambda x \in W$ *pour tous* $\lambda \in K$ *et* $x \in W$.

Démonstration. Les trois conditions sont clairement nécessaires car W doit être muni d'une somme avec élément neutre et d'une action. Montrons qu'elles sont suffisantes.

□

Exemple 2.4. Considérons l'espace vectoriel $\mathcal{F}(\mathbb{R}, \mathbb{R})$ de toutes les fonctions réelles.
Alors les sous-ensembles suivants sont tous des sous-espaces vectoriels réels :

a) Les fonctions

b) Les fonctions

c) Les fonctions

d) Les fonctions

Les opérations ensemblistes d'intersection et d'union se comportent de manière distincte par rapport à la structure d'espace vectoriel.

Lemme 2.5. *Toute intersection de sous-espaces vectoriels est un sous-espace vectoriel.*

Démonstration. On veut montrer que les trois propriétés de la proposition sont vérifiées.

(i) Si $0 \in W_i$ pour une famille $W_i \subset V$ de sous-espaces, alors $0 \in \bigcap W_i$.

(ii) Si $x, y \in \bigcap W_i$, alors $x, y \in W_i$ pour tout i. Comme tous les W_i sont des sous-espaces vectoriels, on a que $x + y \in W_i$ pour tout i, donc $x + y \in \bigcap W_i$.

(iii) Si $x \in \bigcap W_i$ et $\lambda \in K \Rightarrow x \in W_i$ pour tout $i \Rightarrow \lambda x \in W_i$ pour tout $i \Rightarrow \lambda x \in \bigcap W_i$.

□

En revanche, la réunion de deux sous-espaces n'est pas un sous-espace en général.
Dans $(\mathbb{F}_2)^2$, les sous-ensembles $W_1 = \{(0,0),(0,1)\}$ et $W_2 = \{(0,0),(1,0)\}$ sont des sous-espaces, mais pas la réunion puisque

Il vaut mieux travailler avec la *somme* $W_1 + W_2 = \{x + y \,|\, x \in W_1, y \in W_2\}$.
Si $W_1 \cap W_2 = \{0\}$, on dit que la somme $W_1 + W_2$ est *directe* et on note alors $W_1 \oplus W_2$.

Lemme 2.6. *Soit V un K-espace vectoriel.*
La somme de sous-espaces vectoriels de V est un sous-espace vectoriel de V.

3 Combinaisons linéaires

Vous avez déjà aperçu l'importance des combinaisons linéaires l'année passée lorsque vous avez brièvement parlé des bases de $\mathbb{R}^2$ et $\mathbb{R}^3$. Nous travaillons ici avec un K-espace vectoriel V.

Définition 3.1. Soit $S \subset V$.
On note $< S >$ l'intersection de tous les sous-espaces vectoriels de V qui contiennent S.
On appelle S un *système de générateurs* de $< S >$ et on dit que S *engendre* $< S >$.
Lorsque $S = \{x\}$, on note aussi $Kx =< \{x\} >$.

Le sous-espace $< S >$ est le plus petit sous-espace de V qui contient S.
Explicitement, les éléments de $< S >$ sont des combinaisons linéaires d'éléments de S.

Définition 3.2. Soit $S \subset V$. On dit que $x \in V$ est une *combinaison linéaire* d'éléments de S s'il existe des scalaires $\lambda_1, \ldots, \lambda_n \in K$ et des vecteurs $x_1, \ldots, x_n \in S$ tels que $x = \lambda_1 x_1 + \cdots + \lambda_n x_n$.

Proposition 3.3. *Soit $S \subset V$.*
Alors $< S >$ est l'ensemble de toutes les combinaisons linéaires d'éléments de S.

Démonstration. Appelons W l'ensemble de toutes les combinaisons linéaires d'éléments de S.

□

Remarque 3.4. Soient W_1, W_2 des sous-espaces de V. Alors $W_1 + W_2 = < W_1 \cup W_2 >$.

Définition 3.5. Soient $x_1, \ldots, x_n \in V$. On dit que ces vecteurs sont *linéairement indépendants* ou *libres* si l'unique suite de scalaires $\lambda_1, \ldots, \lambda_n \in K$ tels que

$$\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$$

est donnée par $\lambda_1 = \cdots = \lambda_n = 0$.
Si ce n'est pas le cas, on dit qu'ils sont *linéairement dépendants* ou *liés*.

Aucun vecteur d'une suite libre ne peut être nul, car, si $x_1 = 0$,

Tout ensemble contenant un unique élément non nul est forcément libre.
Par convention, l'ensemble vide est libre.

Exemple 3.6.
Dans $\mathbb{C}^2$, les éléments $x_1 = (1; i)$ et $x_2 = (1 + i; i - 1)$ sont

Les éléments $y_1 = (1; i)$ et $y_2 = (i; 1)$

4 Bases

Les meilleurs systèmes de générateurs d'un espace vectoriel sont les plus petits.
Ceci nous conduit à définir ce qu'est une base d'un K-espace vectoriel V.

Définition 4.1. Une *base* de V est un sous-ensemble ordonné et libre $\mathcal{B} \subset V$ qui engendre V.
Si V admet une base finie, on dit que V est de *dimension finie*.
On note $(e_1, \ldots, e_n)$ la base formée des vecteurs $e_1, \ldots, e_n$ car l'ordre des éléments compte.

Exemple 4.2. Soit $V = K^n$. La *base canonique* de K^n est composée des n vecteurs
$e_1 = (1_K; 0_K; \ldots; 0_K), e_2 = (0_K; 1_K; 0_K, \ldots; 0_K), \ \ldots \ , e_n = (0_K; \ldots; 0_K; 1_K)$.
Ces vecteurs sont visiblement linéairement indépendants.
Ils engendrent K^n car $(\lambda_1; \ldots; \lambda_n) = \lambda_1 e_1 + \cdots + \lambda_n e_n$.

Le lemme suivant explique comment enlever un vecteur "en trop" d'une famille liée.

Lemme 4.3. de dépendance linéaire.
Si $x_1, \ldots, x_m$ sont linéairement dépendants et $x_1 \neq 0_V$, il existe $2 \leq j \leq m$ tel que $x_j \in < x_1, \ldots, x_{j-1} >$ et les vecteurs $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m$ engendrent $< x_1, \ldots, x_m >$.

Démonstration. Par dépendance linéaire, il existe une combinaison linéaire $\lambda_1 x_1 + \ldots \lambda_m x_m = 0_V$ où les λ_i ne sont pas tous nuls.
Puisque $x_1 \neq 0_V$, il existe $j \geq 2$ tel que $\lambda_j \neq 0_K$. Choisissons le plus grand j qui vérifie cela.
En multipliant par l'inverse de λ_j et en isolant x_j, nous obtenons

ce qui conclut la preuve de la première assertion. Pour montrer la seconde, il suffit de remarquer que toute combinaison linéaire $\mu_1 x_1 + \cdots + \mu_m x_m$ peut aussi s'écrire, en remplaçant x_j par l'expression ci-dessus,

□

Le lemme de dépendance linéaire permet d'extraire une base de chaque système de générateurs.

Théorème 4.4. *Soit $x_1, \ldots, x_m$ un système de générateurs de V.*
Alors il existe des indices $1 \leq k_1 < \cdots < k_n \leq m$ tels que $(x_{k_1}, \ldots, x_{k_n})$ forme une base de V.

Démonstration. Si les vecteurs sont linéairement indépendants, il n'y a rien à faire, ils forment déjà une base. Si $x_1 = 0_V$, nous éliminons x_1 de la liste. Sinon, nous appliquons le Lemme de dépendance linéaire et éliminons x_j pour l'indice j décrit dans le lemme.
Nous continuons ensuite ce processus et nous arrêtons lorsque les vecteurs restants sont libres. □

Exemple 4.5. Soient $(1;2), (3;6), (4;7)$ et $(5;9)$ des vecteurs de $\mathbb{Q}^2$.
Ils sont linéairement dépendants puisque par exemple

Voyons maintenant que toute partie libre de V peut être complétée en une base.

Théorème 4.6. de la base incomplète.
Soit V un K-espace vectoriel de dimension finie, $L = \{x_1, \ldots, x_k\}$ une famille de vecteurs linéairement indépendants et $S = \{y_1, \ldots, y_m\}$ un système de générateurs de V.
Alors Il existe une base $\mathcal{B}$ de V telle que $L \subset \mathcal{B} \subset L \cup S$.

Démonstration. Considérons les vecteurs $x_1, \ldots, x_k, y_1, \ldots, y_m$. C'est un système de générateurs. On peut donc appliquer le théorème précédent pour en extraire une base.
Puisque $x_1, \ldots, x_k$ est libre, la méthode d'élimination laisse intacte les k premiers vecteurs. □

Dans l'optique de définir la dimension d'un espace vectoriel, nous terminons cette section en montrant qu'une famille libre ne peut pas avoir plus de vecteurs qu'un système de générateurs.

Proposition 4.7. *Soit V un espace vectoriel de dimension finie, $L = \{x_1, \ldots, x_k\}$ une partie libre et $S = \{y_1, \ldots, y_m\}$ un système de générateurs. Alors $k \leq m$.*

Démonstration.
S est un système de générateurs $\Rightarrow$ $S_1 = \{x_1, y_1, \ldots, y_m\}$ est

Or $x_1 \neq 0$ car

On applique donc le lemme 4.3 de dépendance linéaire qui élimine

Finalement, on obtient un système de générateurs de la forme $\{x_1, \ldots, x_k, y_{a_1}, \ldots, y_{a_{m-k}}\}$ qui contient toujours éléments. En effet, la méthode du lemme laisse intact les premiers vecteurs de la famille s'ils sont linéairement indépendants. et pour chaque vecteurs x_i ajouté, on a éliminé exactement un vecteurs y_j. On a donc bien enlevé k vecteurs de S, si bien que $k \leq m$.

□

IV. Applications linéaires

Le programme pour aujourd'hui est de continuer la discussion sur les bases d'un espace vectoriel, puis d'étudier les applications entre espaces vectoriels qui préservent la structure à disposition, c'est-à-dire la somme et l'action.

1 Dimension

Soit K un corps et V un K-espace vectoriel de dimension finie, ce qui signifie que V admet une base finie. Pour pouvoir définir la notion de dimension, nous devons montrer que le nombre de vecteurs qu'il faut pour former une base ne varie pas d'une base à l'autre.

Proposition 1.1. *Soit V un K-espace vectoriel de dimension finie.*
Si $\mathcal{B}$ et $\mathcal{B}'$ sont deux bases de V, alors $|\mathcal{B}| = |\mathcal{B}'|$.

Démonstration. On a vu la semaine passée que le nombre d'éléments d'une partie libre de V est toujours inférieur ou égal au nombre d'éléments d'un système de générateurs.

□

La définition suivante a donc un sens.

Définition 1.2. Soit V un K-espace vectoriel.
La *dimension* de V sur K, notée $\dim_K(V)$ ou simplement $\dim V$, est le nombre d'éléments que contient une base de V.
Si V n'est pas de dimension finie, on dit que la dimension de V est infinie et alors, par définition, aucune de ses bases n'est finie.

Exemple 1.3.
Les espaces vectoriels $\mathcal{F}(\mathbb{R},\mathbb{R})$ ou celui des suites de nombres complexes sont de dimension infinie. Par contre, $\dim \mathbb{R}^n = n$ car la base canonique contient exactement n vecteurs et l'espace vectoriel $\mathbb{F}_{23}[x]^{\leq n}$ des polynômes de degré $\leq n$ à coefficients dans le corps à 23 éléments est de dimension

Clairement, si U est un sous-espace de V, $\dim U \leq \dim V$, puisqu'on peut compléter une base de U en une base de V. Ainsi, la dimension d'une somme de sous-espaces est plus grande ou égale à la dimension de chacun d'eux. Mais comment calcule-t-on explicitement cette dimension ?

Proposition 1.4. *Soient V un K-espace vectoriel et $U, W \subset V$ deux sous-espaces de V. Alors*

$$\dim(U+W) = \dim U + \dim W - \dim(U \cap W)$$

Démonstration. Nous devons comparer les tailles des bases des sous-espaces en jeu.
Pour faire cela, commençons par choisir une base $(v_1, \ldots, v_k)$ de l'intersection $U \cap W$.
C'est une famille libre de U que nous pouvons compléter en une base $(v_1, \ldots, v_k, u_1, \ldots, u_m)$ de U.
De même on construit une base $(v_1, \ldots, v_k, w_1, \ldots, w_n)$ de W.

Il s'agit d'un système de générateurs car tout élément de $U+W$ s'écrit $u+w$ avec $u \in U$ et $w \in W$. Puisque u est combinaison linéaire des éléments v_i et des u_j et que w est combinaison linéaire des v_i et des w_l, on voit que $u+w \in < \mathcal{B} >$. Il reste à voir qu'il s'agit de vecteurs linéairement indépendants. Considérons donc une combinaison linéaire nulle

$$\alpha_1 v_1 + \ldots + \alpha_k v_k + \beta_1 u_1 + \ldots + \beta_m u_m + \gamma_1 w_1 + \ldots + \gamma_n w_n = 0_V$$

où les $\alpha_i, \beta_j, \gamma_l \in K$. On récrit cette équation comme suit :

□

Exemple 1.5. Considérons dans $\mathbb{F}_2[x]^{\leq 3}$ les sous-espaces $U = \{p(x) \mid p(0) = 0\}$ et $W = \mathbb{F}_2[x]^{\leq 2}$.

2 La linéarité

Nous avons parlé dans ce module de groupes, d'anneaux, de corps et d'espaces vectoriels, mais nous n'avons pas encore appris à comparer les objets de chacune de ces classes entre eux. Ceci nous amène à la notion d'homomorphisme, du grec $o\mu o\varsigma$, semblable, et $\mu o\rho\varphi\eta$, forme.

Définition 2.1. Soient $(G, *)$ et $(H, \circ)$ deux groupes.
Un *homomorphisme* de groupes est une application $f : G \to H$ telle que $f(g * g') = f(g) \circ f(g')$.
Soient A et B deux anneaux. Un *homomorphisme* d'anneaux est une application $f : A \to B$ telle que $f(a + a') = f(a) + f(a')$, $f(aa') = f(a)f(a')$ et $f(1_A) = 1_B$.

Ainsi, en général, un homomorphisme, ou parfois simplement "morphisme", est une application qui préserve la structure à disposition. Le premier exemple qui vient à l'esprit est l'inclusion d'un sous-anneau. Par exemple, l'inclusion $\mathbb{Q} \subset \mathbb{R}$ est un homomorphisme d'anneaux (injectif).

Exemple 2.2. Considérons l'application de réduction modulo p qui envoie un entier relatif sur sa classe de congruence modulo p. Ainsi $f : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ est définie par $f(n) = [n]$.
Il s'agit d'un homomorphisme d'anneaux (surjectif) par définition de la somme et du produit dans les entiers modulo p.

Il est naturel de définir maintenant un *homomorphisme d'espaces vectoriels* comme étant une application qui préserve la somme et l'action.

Définition 2.3. Soient K un corps, V et W deux K-espaces vectoriels.
Une *application (K-) linéaire* est une application $\alpha : V \to W$ telle que, $\forall v, v' \in V$ et $\forall \lambda \in K$,

- $\alpha(v + v') = \alpha(v) + \alpha(v')$;
- $\alpha(\lambda v) = \lambda\alpha(v)$.

On note souvent $\mathcal{L}(V, W)$ l'ensemble de toutes les applications linéaires de V vers W.
Lorsque $V = W$ on abrège en $\mathcal{L}(V)$.
On appelle *isomorphisme* une application linéaire bijective.

En particulier, on voit que $\alpha(0_V) = 0_W$, car

De nouveau, les exemples évidents qui nous viennent à l'esprit sont les inclusions de sous-espaces vectoriels, mais nous montrerons que des transformations du plan comme les rotations, symétries, homothéties et projections orthogonales sont des applications $\mathbb{R}$-linéaires de $\mathbb{R}^2$ dans lui-même.

Proposition 2.4. *Soit $\alpha : V \to W$ une application linéaire, $U \subset V$ et $Z \subset W$ des sous-espaces. Alors $\alpha(U)$ est un sous-espace de W et $\alpha^{-1}(Z)$ est un sous-espace de V.*

Démonstration. La première affirmation se fera en exercice.
Montrons simplement la deuxième affirmation à l'aide de notre critère favori.

□

Exemple 2.5. Considérons les espaces vectoriels $\mathbb{C}^3$ et $\mathbb{C}^4$.
Un exemple d'application $\mathbb{C}$-linéaire $\alpha : \mathbb{C}^3 \to \mathbb{C}^4$ est donné par

$\alpha(z_1, z_2, z_3) =$

Exemple 2.6. L'application $\beta : \mathbb{F}_7^3 \to \mathbb{F}_7$ définie par $\beta(a, b, c) = a + b - 3c + 1$ est

3 Noyau, image et rang

Etant donné une application linéaire, deux sous-espaces importants nous aident à comprendre la signification géométrique de cette application.

Définition 3.1. Soit $\alpha : V \to W$ une application linéaire.
Le *noyau* de α, noté $\mathrm{Ker}(\alpha)$, est le sous-espace $\alpha^{-1}(0) = \{v \in V \,|\, \alpha(v) = 0\}$.
L'*image* de α, notée $\mathrm{Im}(\alpha)$, est le sous-espace $\alpha(V) = \{w \in W \,|\, \exists v \in V \text{ tel que } \alpha(v) = w\}$.
Le *rang* de α est la dimension de $\mathrm{Im}(\alpha)$.

Exemple 3.2. Considérons l'application linéaire $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ définie par $\alpha(x; y) = \left(\frac{x-y}{2}; \frac{y-x}{2}\right)$.
Calculons le noyau et l'image de cette application linéaire du plan.

Proposition 3.3.
Une application linéaire est injective si et seulement son noyau est le sous-espace $\{0\}$.

Démonstration. Si $\alpha : V \to W$ est injective, alors le seul vecteur dont l'image est 0_W doit être 0_V, si bien que $\mathrm{Ker}(\alpha) = \{0\}$.
Réciproquement, si le noyau est nul, montrons que α est injective.

□

Le théorème du rang explique la relation très forte qui existe entre les dimensions des sous-espaces vectoriels en jeu, celle du noyau et celle de l'image.

Théorème 3.4. du rang.
Soit $\alpha : V \to W$ une application linéaire et supposons que V est de dimension finie. Alors

$$\dim V = \dim(\ker \alpha) + \operatorname{rang}(\alpha)$$

Démonstration. Puisque V est de dimension finie, le sous-espace $\mathrm{Ker}(\alpha)$ aussi. Choisissons une base $(v_1, \ldots, v_k)$ du noyau et complétons-la en une base de V tout entier, $\mathcal{B}_V = (v_1, \ldots, v_k, u_1, \ldots, u_n)$. Pour terminer la preuve, il suffit de montrer que l'image de α est un sous-espace de dimension n.

Considérons donc les vecteurs $\alpha(u_1), \ldots, \alpha(u_n)$ de l'espace vectoriel W. Nous allons montrer qu'ils forment une base de $\mathrm{Im}(\alpha)$.
En effet, si $w \in \mathrm{Im}(\alpha)$, il existe $v \in V$ tel que $\alpha(v) = w$. Ecrivons ce vecteur v comme combinaison linéaire des vecteurs de la base $\mathcal{B}_V$ que nous avons construite :

$$\begin{aligned} w = \alpha(v) &= \alpha(\lambda_1 v_1 + \cdots + \lambda_k v_k + \mu_1 u_1 + \cdots + \mu_n u_n) \\ &= \end{aligned}$$

où les coefficients λ_i et μ_j sont dans K. Ainsi, w est bien combinaison linéaire de vecteurs $\alpha(u_j)$. Il reste encore à montrer que ces vecteurs sont linéairement indépendants.
Considérons donc une combinaison linéaire nulle

$$0_W = \gamma_1 \alpha(u_1) + \cdots + \gamma_n \alpha(u_n) = \alpha(\gamma_1 u_1 + \cdots + \gamma_n u_n).$$

Ainsi, le vecteur $\gamma_1 u_1 + \cdots + \gamma_n u_n$ appartient

□

Corollaire 3.5. *Soit V et W des K-espaces vectoriels.*
Alors, si $\dim V < \dim W$, il n'existe aucune application linéaire surjective $\alpha : V \to W$.

Corollaire 3.6. *Soit V et W des K-espaces vectoriels et $\alpha : V \to W$ une applicatin linéaire.*
Alors, si $rang(\alpha) = \dim W$, α est surjective.

Corollaire 3.7. *Soit V et W des K-espaces vectoriels de même dimension, finie.*
Alors une applicatin linéaire $\alpha : V \to W$ est injective si et seulement si elle est surjective si et seulement si elle est bijective.

Démonstration.
Le théorème du rang nous dit que α est injective si et seulement si $\dim \mathrm{Im}(\alpha) = \dim V$.
Puisque $\dim V = \dim W$ ceci arrive exactement lorsque α est surjective. □

Exemple 3.8. Soit $\alpha : \mathbb{C}^2 \to \mathbb{C}$ une application $\mathbb{C}$-linéaire.
Elle est donc de la forme $\alpha(z, z') = az + bz'$ avec $a, b \in \mathbb{C}$.
Lesquelles de ces applications sont surjectives, injectives, bijectives ?

4 La matrice d'une application linéaire

Nous travaillons dans cette section avec deux K-espaces vectoriels V et W de dimensions finies, disons m et n respectivement. Nous aimerions mieux comprendre l'espace vectoriel de toutes les applications linéaires $\alpha : V \to W$. Combien y en a-t-il ? Comment les représenter et travailler avec ? A quoi correspondent-elles dans la pratique ?

Définition 4.1. Une *matrice $n \times m$ à coefficients dans K* est un tableau, entouré de parenthèses, de n lignes et m colonnes dans lequel toutes les entrées sont des scalaires (de K) :

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

On note $M_{n\times m}(K)$ l'ensemble de toutes ces matrices.

On additionne les matrices de même taille coefficient par coefficient, si bien que $M_{n\times m}(K)$ est un groupe abélien. On le munit d'une action de K, coefficient par coefficient, qui en fait K-espace vectoriel.

Proposition 4.2. *L'espace vectoriel $M_{n\times m}(K)$ est de dimension $n \cdot m$.*

Démonstration. La base canonique de $M_{n\times m}(K)$ est formée des matrices e_{ij} avec $1 \leq i \leq n$ et $1 \leq j \leq m$ dont tous les coefficients sont nuls, à l'exception de celui de la $i^{\text{ème}}$ ligne, $j^{\text{ème}}$ colonne qui vaut 1_K. □

Définition 4.3. Soit $\alpha : V \to W$ une application linéaire.
On fixe une base $\mathcal{B} = (e_1, \ldots, e_m)$ de V et $\mathcal{C} = (f_1, \ldots, f_n)$ de W.
Soient a_{ij} les coefficients dans K des combinaisons linéaires, uniques, $\alpha(e_j) = \sum a_{ij} f_i$.

Alors la matrice $A = (a_{ij}) = \begin{pmatrix} a_{11} & \ldots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nm} \end{pmatrix}$ est la matrice de α dans les bases $\mathcal{B}$ et $\mathcal{C}$.

Cette définition permet de construire une application $T : \mathcal{L}(V, W) \to M_{n\times m}(K)$.

Théorème 4.4. *L'application $T : \mathcal{L}(V, W) \to M_{n\times m}(K)$ est un isomorphisme d'espaces vectoriels. En particulier,* $\dim \mathcal{L}(V, W) = n \cdot m$.

Démonstration. Voyons d'abord pourquoi l'application T est linéaire.
Si α et β sont deux applications linéaires, alors $(\alpha+\beta)(e_i) = \alpha(e_i)+\beta(e_i)$, si bien que les coefficients de la matrice de $\alpha + \beta$ sont la somme de ceux des matrices de α et de β.
De même, $T(\lambda\alpha) = \lambda T(\alpha)$ pour tout $\lambda \in K$.
De plus, l'application linéaire T est injective, car

Enfin, T est aussi surjective car à toute matrice $(a_{ij})_{n\times m}$, on peut faire correspondre une application $\alpha \in \mathcal{L}(V, W)$ définie comme suit :

□

Ainsi, une fois qu'on s'est fixé une base $\mathcal{B}_V$ de l'espace vectoriel de départ V et une base $\mathcal{B}_W$ de l'espace vectoriel d'arrivée W, la matrice d'une application se construit en plaçant dans les colonnes les composantes des images des vecteurs de la base $\mathcal{B}_V$ relativement à la base $\mathcal{B}_W$.

Réciproquement, pour calculer l'image d'un vecteur $v \in V$ par une application linéaire dont on nous donne seulement la matrice, il faut exprimer le vecteur v comme combinaison linéaire des vecteurs de la base $\mathcal{B}_V = (e_1, \ldots, e_m)$, écrire ses composantes dans un vecteur colonne et multiplier ce vecteur à droite par A pour obtenir les composantes de $\alpha(v)$ relativement à $\mathcal{B}_W = (f_1, \ldots, f_n)$:

$$v = \sum \lambda_j e_j \qquad \Rightarrow \quad A \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix} = \begin{pmatrix} \sum a_{1j}\lambda_j \\ \vdots \\ \sum a_{nj}\lambda_j \end{pmatrix} = \begin{pmatrix} \mu \\ \vdots \\ \mu_n \end{pmatrix} \qquad \Rightarrow \quad \alpha(v) = \sum \mu f_i$$

Exemple 4.5. Soit $\rho : \mathbb{R}^2 \to \mathbb{R}^2$ l'application linéaire donnée par la matrice $A = \frac{1}{2}\begin{pmatrix} \sqrt{2} & -\sqrt{2} \\ \sqrt{2} & \sqrt{2} \end{pmatrix}$ relativement à la base canonique de $\mathbb{R}^2$.

Alors l'image du point $(1;1)$ est donné par

l'image de $e_1 = (1;0)$ est

l'image de $e_2 = (0;1)$ est

Géométriquement, A est la matrice de

V. Opérations élémentaires

Nous avons terminé la semaine passée en identifiant l'espace vectoriel de toutes les applications linéaires entre deux espaces de dimension finie avec un espace vectoriel de matrices. Nous allons voir aujourd'hui que cette identification est aussi compatible avec le produit. Nous verrons ensuite quelques matrices élémentaires que nous utiliseront dans les cours suivants.

1 Espaces vectoriels de dimension finie

Pour commencer, nous voulons réfléchir à la signification du choix d'une base $\mathcal{B} = (e_1, \dots, e_n)$ d'un K-espace vectoriel V de dimension finie n. Nous nous en servons pour écrire la matrice d'une application linéaire $\alpha : V \to V$, mais aussi pour se représenter les éléments $v \in V$ comme des vecteurs écrits en colonne $\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$ où les λ_i sont les coefficients des vecteurs de base e_i dans l'expression de v comme combinaison linéaire des e_i. Explicitement, $v = \sum_{i=1}^{n} \lambda_i e_i = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}_{\mathcal{B}}$

Exemple 1.1.
Dans $\mathbb{R}[x]^{\leq 2}$ muni de la base canonique $\mathcal{B} = (x^2, x, 1)$, $3x^2 + 5x - 7 =$

Toujours dans $\mathbb{R}[x]^{\leq 2}$ mais muni de la base $\mathcal{B}^* = (3x^2, x - 1, 2)$, $3x^2 + 5x - 7 =$

Théorème 1.2. *Soit V un K-espace vectoriel de dimension finie n.*
Alors il existe un isomorphisme d'espaces vectoriels $\alpha : V \to K^n$.

Démonstration. On choisit une base $\mathcal{B} = (e_1, \ldots, e_n)$ de V et on définit $\alpha : V \to K^n$ de la façon suivante :

□

Exemple 1.3.
Soit $\mathbb{Q}[x]^{\leq 5}$ l'espace vectoriel rationnel des polynômes à coefficients dans $\mathbb{Q}$ de degré ≤ 5.

2 Produit et composition

Soit K un corps, V un K-espace vectoriel de dimension finie m et W un K-espace vectoriel de dimension finie n. Fixons une base $\mathcal{B} = (e_1, \ldots, e_m)$ de V et une base $\mathcal{C} = (f_1, \ldots, f_n)$ de W. Considérons l'application $T : \mathcal{L}(V, W) \to M_{n\times m}(K)$ qui envoie une application linéaire $\alpha : V \to W$ sur la matrice $(\alpha)^{\mathcal{C}}_{\mathcal{B}}$ dont les colonnes sont les composantes des images des vecteurs de la base $\mathcal{B}$ exprimés dans la base $\mathcal{C}$. Nous avons démontré que cette application est un isomorphisme de K-espaces vectoriels. Montrons à présent que cet isomorphisme respecte aussi le produit.

Définition 2.1. Soit $A = (a_{ij})_{1\leq i\leq n; 1\leq j\leq m} \in M_{n\times m}(K)$ et $B = (b_{jk})_{1\leq j\leq m; 1\leq k\leq p} \in M_{m\times p}(K)$.
Le *produit* $A \cdot B \in M_{n\times p}(K)$ est la matrice C dont le coefficient

$$c_{ik} = \sum_{j=1}^{m} a_{ij} b_{jk}.$$

On peut multiplier A avec B dans cet ordre si et seulement si le nombre de colonnes de A est égal au nombre de lignes de B. On "combine" chaque ligne de A par chaque colonne de B.

Exemple 2.2.

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

Lorsque $n = m = p$, les deux matrices sont carrées $n \times n$ et on peut les multiplier entre elles dans n'importe quel ordre. On trouve dans les deux cas une matrice carrée $n \times n$.
Mais attention, le produit matriciel n'est pas commutatif en général.

Théorème 2.3. *Les matrices carrées $M_n(K)$ forment un anneau.*

Ajoutons à notre panoplie de K-espaces vectoriels V et W un troisième K-espace vectoriel U de dimension finie p muni d'une base $\mathcal{D} = (g_1, \ldots, g_p)$.

Proposition 2.4. *Soit $\alpha : V \to W$ et $\beta : W \to U$ deux applications linéaires. Alors*

$$T(\beta \circ \alpha) = T(\beta)T(\alpha).$$

Démonstration. Puisque T est déterminée par les images des vecteurs de base, il suffit de suivre les vecteurs e_i au travers de α, puis β.
L'image $\alpha(e_i)$ s'exprime comme combinaison linéaire $\sum_{j=1}^{n} a_{ji} f_j$, si bien que la i-ème colonne de la matrice $T(\alpha)$ est constituée des coefficients a_{ji}.

De même, $\beta(f_j) = \sum_{k=1}^{p} b_{kj} g_k$ et la k-ème colonne de $T(\beta)$ est constituée des coefficients b_{kj}.
La matrice $T(\beta \circ \alpha)$ est déterminée par les images des e_i et nous calculons donc

Le k-ème coefficient de la i-ème colonne de la matrice de $\beta \circ \alpha$ est $\sum_{j=1}^{n} b_{kj} a_{ji}$, c'est-à-dire, par définition du produit matriciel, le k-ème coefficient de la i-ème colonne de la matrice $T(\beta)T(\alpha)$. □

Exemple 2.5. Soit $\mathbb{F}_p[x]^{\leq k}$ l'espace vectoriel des polynômes de degré $\leq k$ à coefficients dans le corps à p éléments $\mathbb{F}_p$.
On considère les applications linéaires $\alpha : \mathbb{F}_p[x]^{\leq 2} \to \mathbb{F}_p[x]^{\leq 1}$ définie par la dérivation, et
$\beta : \mathbb{F}_p[x]^{\leq 1} \to \mathbb{F}_p[x]^{\leq 2}$ définie par la multiplication par x.
Quelle est la matrice de $\beta \circ \alpha$?

On choisit les bases $(1, x, x^2)$ de $\mathbb{F}_p[x]^{\leq 2}$ et $(1, x)$ de $\mathbb{F}_p[x]^{\leq 1}$.

Lorsque $V = W = U$ de dimension n est muni d'une base $\mathcal{B}$, le produit de l'anneau $M_n(K)$ correspond via T à la composition des applications linéaires. En particulier, l'image de l'identité $Id : V \to V$ est la *matrice unité* I ou I_n dont tous les coefficients diagonaux sont égaux à 1 et tous les autres sont nuls. Elle a la propriété que $A \cdot I = A = I \cdot A$ puisque $\alpha \circ Id = \alpha = Id \circ \alpha$.

Proposition 2.6. *Soit V un K-espace vectoriel de dimension finie n muni d'une base $(e_1, \ldots, e_n)$. Alors $T : \mathcal{L}(V) \to M_n(K)$ est un isomorphisme d'anneaux.*

En fait, les structures de K-espace vectoriel et d'anneau de $M_n(K)$ sont compatibles dans un sens précis. On dit que $M_n(K)$ est une *K-algèbre*.

3 Matrices particulières

Voyons maintenant quelques matrices dont la forme est si spéciale qu'elles méritent un nom particulier.
Une matrice carrée A de taille $n \times n$ est dite *triangulaire supérieure* (respectivement *inférieure*) si

Si on appelle diagonaux les coefficients a_{ii} de la matrice, cela signifie que les coefficients en-dessous (respectivement au-dessus) de la diagonale sont tous nuls.

Exemple 3.1. La matrice $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$ est triangulaire supérieure. En effet,

Une matrice qui est à la fois triangulaire supérieure et inférieure est dite *diagonale*. Les seuls coefficients non-nuls d'une telle matrice A sont donc les a_{ii} et on note parfois $\text{diag}(a_{11}, \ldots, a_{nn})$ pour une telle matrice. Vue comme matrice d'une application linéaire $\alpha : V \to V$ relativement à la base $\mathcal{B} = (e_1 \ldots, e_n)$, cela signifie que $\alpha(e_i) = a_{ii}e_i$. Chaque vecteur de base est envoyé sur un multiple de lui-même.
La matrice unité I de $M_n(K)$ est diagonale. C'est $\text{diag}(1, \ldots, 1)$.

Exemple 3.2. Considérons la matrice diagonale $D = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix} \in M_3(\mathbb{R})$.
Si on interprète cette matrice comme celle d'une application linéaire de $\mathbb{R}^3$ muni de n'importe quelle base,

Définition 3.3. Soit $1 \leq i \leq m$ et $1 \leq j \leq n$. La matrice $e_{ij} \in M_{m\times n}(K)$ est celle dont tous les coefficients sont nuls, sauf celui de la i-ème ligne et j-ème colonne qui vaut 1.

Ainsi, si $m = 2$ et $n = 3$, la matrice e_{23} est $\begin{pmatrix} & & \\ & & \end{pmatrix}$.
Nous avons déjà vu que ces matrices forment une base, dite canonique, de $M_{m\times n}(K)$. C'est cette base qui nous a permis de calculer la dimension de $M_{m\times n}(K)$.
Que se passe-t-il lorsqu'on multiplie une matrice à gauche par e_{ij} ?
Puisque le produit se calcule ligne par colonne et que la seule ligne non nulle de e_{ij} est la i-ème

$$e_{ij} \cdot \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} =$$

est la matrice dont

Définition 3.4. Soit $1 \leq i \neq j \leq n$ et $\lambda \in K$. La *matrice élémentaire* $E_{ij}(\lambda) \in M_n(K)$ est

$$E_{ij}(\lambda) = I + \lambda e_{ij}.$$

Que se passe-t-il lorsqu'on multiplie une matrice à gauche par E_{ij} ?

Soit $A \in M_{m\times n}(K)$ et $E_{ij}(\lambda) = I + \lambda e_{ij} \in M_n(K)$. Alors,

Définition 3.5. Soit $1 \leq i \leq n$ et $\mu \in K^*$. La *matrice élémentaire* $D_i(\mu) \in M_n(K)$ est

$$D_i(\mu) = I + (\mu - 1)e_{ii}.$$

La matrice $D_i(\mu)$ est donc

Définition 3.6. Soit $1 \leq i < j \leq n$. La *matrice élémentaire* $P_{ij} \in M_n(K)$ est

$$P_{ij} = I - e_{ii} - e_{jj} + e_{ij} + e_{ji}.$$

Lorsque $n = 2$, la matrice P_{12} est $\begin{pmatrix} & \\ & \end{pmatrix}$.

En général, pour obtenir P_{ij} à partir de I on échange les lignes i et j.
Lorsqu'on multiplie une matrice à gauche par P_{ij}, on échange les i-ème et j-ème lignes.

Exemple 3.7. Calculons $P_{13}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix} =$

4 Matrices inversibles

Les matrices élémentaires que nous retrouverons à l'heure de résoudre des systèmes d'équations sont des cas particuliers de matrices que l'on peut "inverser". Nous avons vu que $M_n(K)$ est un anneau, mais en général pas un corps : certaines matrices admettent un inverse et d'autres pas.

Définition 4.1. Soit $A \in M_n(K)$. La matrice A est *inversible* s'il existe une matrice $B \in M_n(K)$ telle que $AB = I = BA$. On note alors $B = A^{-1}$.
L'ensemble des matrices inversibles est noté $GL_n(K)$.

Nous savons que si l'inverse de A existe, il est unique. Nous savons aussi que $GL_n(K)$ forme un groupe pour la multiplication. A priori, il n'y a pas de raison générale pour que $AB = I \Rightarrow BA = I$, mais c'est toujours le cas ! Il n'importe donc pas de trouver l'inverse à "droite" ou à "gauche".

Proposition 4.2. *Soit $A, B \in M_n(K)$ telles que $AB = I$. Alors $BA = I$.*

Démonstration. Considérons l'application linéaire $\alpha : M_n(K) \to M_n(K)$ définie par $\alpha(X) = BX$.

□

Exemple 4.3. Les matrices $E_{ij}(\lambda), D_i(\mu)$ et P_{ij} sont inversibles.

Réfléchissons un instant à la signification de l'inversibilité en termes d'applications linéaires plutôt qu'en termes de matrices.
Soit $\alpha : V \to W$ une application linéaire et A sa matrice pour un choix de bases. Il n'y a de sens de parler d'inverse que si A est une matrice carrée, si bien que l'on peut supposer que $V = W$ et que l'on choisit deux fois la même base $\mathcal{B}$ de V. Autrement dit, $A = (\alpha)^{\mathcal{B}}_{\mathcal{B}}$.

Théorème 4.4. *La matrice $A = (\alpha)_{\mathcal{B}}^{\mathcal{B}}$ est inversible si et seulement si α est un isomorphisme.*

Démonstration.
Si α est un isomorphisme, on peut considérer l'application réciproque $\alpha^{-1} : V \to V$.
Il s'agit d'une application linéaire (voir les exercices) telle que $\alpha^{-1} \circ \alpha = \mathrm{Id}_V$.
Par conséquent, si B est la matrice de α^{-1} dans la base $\mathcal{B}$, alors

ce qui montre que A est inversible.
Réciproquement, supposons que A est inversible et soit B son inverse. On définit $\beta : V \to V$ comme étant l'unique application linéaire dont la matrice est B dans la base $\mathcal{B}$.
Ceci signifie que $\beta(e_i) = \sum_{j=1}^{n} b_{ji} e_j$ et, par linéarité, si $v = \sum_i \lambda_i e_i$, on a $\beta(v) = \sum_i \sum_j \lambda_i b_{ji} e_j$.
Alors $\beta \circ \alpha$ a pour matrice $BA = I$. Autrement dit, $T(\beta \circ \alpha) = T(Id)$.
Comme T est un isomorphisme (d'espaces vectoriels et d'anneaux) on en déduit que $\beta \circ \alpha = Id$.
De même $\alpha \circ \beta = Id$. □

Exemple 4.5.
La symétrie axiale σ d'axe $x = y$ est une application linéaire du plan réel qui est bijective.

Exemple 4.6. Soit la matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$. On aimerait calculer son inverse.

Tu verras l'année prochaine que cela se généralise pour toutes les matrices carrées :

Théorème 4.7. *Une matrice $A \in M_n(\mathbb{R})$ est inversible si et seulement si* $\det(A) \neq 0$.

VI. Calcul du rang et systèmes d'équations

Nous avons fait connaissance la semaine passée avec les matrices élémentaires de trois types. Lors de multiplication à gauche avec l'une de ces matrices, on effectue des opérations élémentaires sur les lignes. Nous allons voir comment un usage systématique de ces opérations permet de calculer le rang d'une application linéaire et de résoudre des systèmes d'équations linéaires.

1 Changement de base

Soit $\alpha : V \to W$ une application linéaire entre deux espaces vectoriels de dimension finie. Pour comprendre α, nous avons vu que nous pouvons choisir une base $\mathcal{B} = (e_1, \ldots, e_m)$ de V et une base $\mathcal{C} = (f_1, \ldots, f_n)$ de W afin de construire la matrice $A = (\alpha)_{\mathcal{B}}^{\mathcal{C}}$. Il suffit alors d'étudier la matrice A. Par exemple, α est un isomorphisme si et seulement si A est une matrice inversible.
Mais que se passe-t-il si nous choisissons d'autres bases ? Un autre choix peut valoir la peine si la forme de la matrice se simplifie et rend la nature de l'application plus lisible...

Définition 1.1. Soit $\mathcal{B} = (e_1, \ldots, e_m)$ et $\mathcal{B}' = (e'_1, \ldots, e'_m)$ deux bases de V. Alors la matrice $P = (Id_V)_{\mathcal{B}}^{\mathcal{B}'}$ de l'application linéaire identité où l'on fixe la base $\mathcal{B}$ au départ et $\mathcal{B}'$ à l'arrivée s'appelle la *matrice de changement de base* de $\mathcal{B}$ à $\mathcal{B}'$.

Proposition 1.2. *Une matrice $P \in M_m(K)$ est une matrice de changement de base si et seulement si elle est inversible.*

Démonstration. Une matrice de changement de base $(Id_V)_{\mathcal{B}}^{\mathcal{B}'}$ est inversible puisque son inverse est la matrice

Réciproquement, si P est inversible, cela signifie que son rang vaut m, ou encore que son image est de dimension m.
En particulier, si $\mathcal{B} = (e_1, \ldots, e_m)$ est la base canonique de K^m, choisissons $e'_j = \sum p_{ij} e_i$.
Les e'_j forment une base $\mathcal{B}'$ de K^m. On interprète alors P comme matrice de l'application linéaire identité de K^m muni de la base $\mathcal{B}'$ dans K^m muni de la base canonique. En effet, l'image de e'_j se lit dans la j-ème colonne : ses coordonnées dans la base canonique sont $(p_{1j}, \ldots, p_{mj})$. □

Exemple 1.3. La matrice $P = \begin{pmatrix} 1 & 3 \\ -3 & 1 \end{pmatrix}$ est inversible puisque ses colonnes sont des

Une autre façon de le voir serait de constater que la seule solution au système $\begin{cases} x + 3y = 0 \\ -3x + y = 0 \end{cases}$ est

Choisissons donc $e'_1 = \begin{pmatrix} 1 \\ -3 \end{pmatrix}$ et $e'_2 = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$ pour former une nouvelle base $\mathcal{B}' = (e_1, e_2)$.

Alors la matrice de l'identité de la base $\mathcal{B}'$ à la base canonique est formée de la façon suivante :

Ses colonnes sont formées des composantes des vecteurs de la base $\mathcal{B}'$ dans la base canonique car

2 Le rang-colonne d'une matrice

Lorsqu'on souhaite calculer le rang de α, c'est-à-dire la dimension de l'image (puis en déduire la dimension du noyau par le théorème du rang), nous pouvons choisir des bases des espaces vectoriels de départ et d'arrivée, calculer la matrice de α par rapport à ces deux bases et observer les colonnes de cette matrice.

Définition 2.1. Soit A une matrice de $M_{n\times m}(K)$. Le *rang-colonne* de A est la dimension du sous-espace vectoriel de K^n engendré par les vecteurs colonnes $\begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix}$ pour $1 \leq i \leq m$.

Le *rang-ligne* de A est la dimension du sous-espace vectoriel de K^m engendré par les vecteurs lignes $(a_{j1} \ \dots \ a_{jm})$ pour $1 \leq j \leq n$.

L'un des grands résultats du jour est que ces deux rangs sont égaux ! Avant de démontrer ce théorème, nous allons nous concentrer sur la signification géométrique du rang-colonne.
Considérons la matrice A comme celle d'une application linéaire $\alpha : K^m \to K^n$ qui envoie les vecteurs de la base canonique sur les vecteurs colonnes donnés par les colonnes de la matrice A. Concrètement,

$$\alpha(e_i) = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix}.$$

Ainsi, les colonnes de la matrice A sont les images des vecteurs de la base canonique de K^m, et par conséquent, engendrent l'image de α. En effet,

Nous avons donc montré le résultat suivant :

Proposition 2.2. *Soient V et W deux K-espaces vectoriels de dimension finie, $\mathcal{B} = (e_1, \dots, e_m)$ une base de V et $\mathcal{C} = (f_1, \dots, f_n)$ une base de W. Soit $\alpha : V \to W$ une application linéaire et $A = (\alpha)^{\mathcal{C}}_{\mathcal{B}}$. Alors le rang de α est égal au rang-colonne de A.* □

Exemple 2.3. Quel est le rang de l'application linéaire $\alpha : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ donnée par la matrice

$$P = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \in M_3(\mathbb{F}_2)$$

par rapport à la base canonique ?
On constate que

3 Matrices équivalentes

Nous pouvons nous permettre une certaine souplesse à l'heure de construire la matrice de α. Choisissons en effet deux bases $\mathcal{B} = (e_1, \ldots, e_m)$ et $\mathcal{B}' = (e'_1, \ldots, e'_m)$ de V et deux autres $\mathcal{C} = (f_1, \ldots, f_n)$ et $\mathcal{C}' = (f'_1, \ldots, f'_n)$ de W. Nous pouvons alors construire deux matrices qui représentent l'application linéaire α, la matrice $A = (\alpha)_{\mathcal{B}}^{\mathcal{C}}$ et $B = (\alpha)_{\mathcal{B}'}^{\mathcal{C}'}$. On peut obtenir l'une à partir de l'autre en utilisant les matrices de changement de base $Q = (Id)_{\mathcal{B}}^{\mathcal{B}'}$ et $P = (Id)_{\mathcal{C}'}^{\mathcal{C}}$. En effet, le diagramme

Définition 3.1. Deux matrices A et B de $M_{n\times m}(K)$ sont *équivalentes* et on note $A \sim B$ s'il existe deux matrices inversibles $P \in GL_n(K)$ et $Q \in GL_m(K)$ telles que $A = PBQ$.

Théorème 3.2. *Deux matrices A et B de $M_{n\times m}(K)$ sont équivalentes si et seulement elles représentent la même application linéaire $\alpha : K^m \to K^n$.*

Démonstration. Si A et B représentent α par rapport à des bases différentes, nous avons vu ci-dessus que A et B sont équivalentes via des matrices P et Q de changement de base.

Supposons maintenant que $A \sim B$ et considérons les matrices inversibles P et Q comme des matrices de changement de base, Q de la base $\mathcal{B}$ à la base $\mathcal{B}'$ de K^m et P de la base $\mathcal{C}'$ à la base $\mathcal{C}$ de K^n. Alors, si A est la matrice d'une application linéaire α exprimée par rapport aux bases $\mathcal{B}$ et $\mathcal{C}$, B est la matrice de cette même application α par rapport aux nouvelles bases $\mathcal{B}'$ et $\mathcal{C}'$ □

Corollaire 3.3. *Si $A \sim B$, alors A et B ont le même rang-colonne.*

Démonstration.

□

Exemple 3.4. Considérons l'application linéaire $\alpha : \mathbb{C}^3 \to \mathbb{C}^3$ définie par

$$\alpha(x; y; z) = (x + iy + (1 - i)z; ix + y + (1 + i)z; (1 + i)x + (1 + i)y + 2z).$$

Quel est son rang ?

La matrice de α par rapport aux bases canoniques est

Théorème 3.5. *Soit A une matrice de $M_{n\times m}(K)$. Les rangs ligne et colonne de A sont égaux.*

Démonstration. Soit $Q \in GL_n(K)$. Nous venons de démontrer que le rang-colonne de A et QA est le même car ces matrices sont équivalentes. Regardons les lignes $l_j = (a_{j1} \ \dots \ a_{jm})$ de A.
Si le rang-ligne vaut k, cela signifie qu'il existe k lignes linéairement indépendantes et que toutes les autres peuvent s'exprimer comme combinaison linéaire de celles-ci. Quitte à multiplier A à gauche par des matrices P_{ij} (inversibles, donc le rang-colonne ne change pas !), nous pouvons supposer qu'il s'agit des k premières lignes. Les autres s'expriment comme $l_s = \lambda_{s1} l_1 + \cdots + \lambda_{sk} l_k$ pour $s > k$. Multiplions alors A par $E_{s1}(-\lambda_{s1}) \cdots E_{sk}(-\lambda_{sk})$ pour obtenir une matrice de la forme

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ \vdots & \vdots & & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{km} \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Soit r_1 le numéro de la première colonne de notre matrice qui possède un coefficient non-nul. Quitte à échanger des lignes comme auparavant, nous pouvons supposer que ce coefficient est dans la première ligne, c'est a_{1r_1}. On multiplie la matrice par $D_1(a_{1r_1}^{-1})$ pour que ce coefficient soit égal à 1. En multipliant la matrice par $E_{21}(-a_{2r_1}) \cdots E_{k1}(-a_{kr_1})$, on garde le même rang-colonne, mais on obtient des zéros dans toute la r_1-ème colonne ; dans la matrice suivante $r_1 = 2$:

$$\begin{pmatrix} 0 & 1 & a_{13} & \cdots & a_{1m} \\ 0 & 0 & a_{23} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots & \\ 0 & 0 & a_{k3} & \cdots & a_{km} \\ 0 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & \cdots & 0 \end{pmatrix}.$$

On procède de la même façon en ne travaillant que sur les lignes 2 à k, puis les lignes 3 à k, etc. en effectuant des opérations élémentaires à chaque pas pour obtenir des zéros sous le premier coefficient non nul de chaque ligne qui vaudra 1. On obtient ainsi une matrice de même rang que A en n'ayant effectué des opérations élémentaires que sur les lignes et qui a la forme suivante :

$$\begin{pmatrix} 0 & 1 & a_{13} & a_{14} & a_{15} & \cdots & \cdots & a_{1m} \\ 0 & 0 & 0 & 1 & a_{25} & \cdots & \cdots & a_{2m} \\ 0 & 0 & 0 & 0 & 1 & a_{36} & \cdots & a_{3m} \\ \vdots & \vdots & \vdots & & & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & & 1 & a_{km} \\ 0 & 0 & \cdots & \cdots & & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & \cdots & & \cdots & \cdots & 0 \end{pmatrix}.$$

Le rang-ligne de cette matrice vaut k et son rang-colonne, qui est le rang-colonne de la matrice équivalente A, vaut k également. En effet, les k colonnes qui contiennent l'un des coefficients égal à 1 par lequel commence une ligne de la matrice sont linéairement indépendantes et engendrent toutes les colonnes de la matrice. □

4 Echelonner et réduire

La méthode que nous avons utilisée dans la démonstration ci-dessus consiste à "échelonner" la matrice, les *échelons* étant les 1 que nous avons introduits petit à petit.

Définition 4.1. Une matrice $A = (a_{ij})_{1\leq i\leq n;1\leq j\leq m} \in M_{n\times m}(K)$ est *échelonnée* s'il existe une suite strictement croissante $r_1 < r_2 < \cdots < r_k$ telle que $a_{ij} = 0$ si $j < r_i$ ou $i > k$ et $a_{ir_i} \neq 0$. Dans ce cas elle est *réduite* si $a_{ir_i} = 1$ et $a_{jr_i} = 0$ si $j \neq i$.

Nous avons donc démontré que l'on peut échelonner et réduire une matrice en effectuant des opérations élémentaires sur les lignes de cette matrice. Ce procédé s'appelle la méthode de Gauss.

Exemple 4.2. Echelonnons et réduisons la matrice $\begin{pmatrix} 1 & 1 & 0 & -1 \\ 0 & 1 & 2 & 3 \\ 1 & 3 & 4 & 5 \\ 2 & 3 & 2 & 1 \end{pmatrix}$.

Nous indiquerons à chaque opération quelle matrice élémentaire on utilise.

Pour terminer, appliquons cette méthode à la résolution d'un système d'équations linéaires. On écrit ce système sous la forme $AX = b$, où $X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$ est le vecteur colonne des inconnues, $A \in M_{n\times m}(K)$ est la matrice des coefficients et $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$.
La méthode de Gauss consiste à effectuer des opérations élémentaires sur les lignes de la matrice A augmentée de b, que l'on écrit $(A \,|\, b)$, pour l'échelonner et la réduire. Il est très dangereux d'effectuer des opérations sur les colonnes car cela revient à mélanger les inconnues !

Exemple 4.3. Nous voulons résoudre le système d'équations

$$\begin{cases} x + y = -1 \\ y + 2z = 3 \\ x + 3y + 4z = 5 \\ 2x + 3y + 2z = 1 \end{cases}$$

La matrice augmentée de ce système est

VII. Matrices semblables

Nous étudierons aujourd'hui plus spécialement les matrices carrées : le calcul de l'inverse, puis la notion de similitude pour des matrices carrées, une notion plus restrictive que celle d'équivalence, mais qui fait plus de sens au moment de l'interprétation géométrique d'une application linéaire.

1 Bref retour sur les systèmes d'équations

Considérons un système d'équations linéaires de la forme $AX = b$, où $A \in M_{n\times m}(K)$ est la matrice des coefficients, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ et $X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$ est le vecteur colonne des inconnues.

On appelle A la *matrice du système* et $(A|b)$ la matrice *augmentée* du système.

Proposition 1.1. *Le système $Ax = b$ admet une solution si et seulement si les rangs des matrices A et $(A|b)$ sont égaux.*

Démonstration. Par double contraposition. Lorsqu'on échelonne la matrice augmentée du système, on arrive dans l'une des lignes à une équation sans solution de la forme $0 = c$ avec $c \neq 0$ si et seulement les rangs des matrices A et $(A|b)$ sont distincts. □

Exemple 1.2. Nous voulons résoudre le système d'équations

$$\begin{cases} x + y + z = 1 \\ x \quad\quad + z = 0 \\ \quad\quad y \quad\quad = a \end{cases}$$

Echelonnons la matrice augmentée de ce système

2 Inversion de matrices

Les méthodes d'échelonnement et de réduction permettent non seulement de résoudre à coup sûr tous les systèmes d'équations linéaires, mais aussi de calculer l'inverse d'une matrice carrée pour autant qu'il existe. La méthode est basée sur l'observation qu'effectuer une opération élémentaire sur les lignes de A correspond à multiplier la matrice par la matrice élémentaire correspondante à gauche. Ainsi, pour calculer l'inverse d'une matrice inversible $S \in GL_n(K)$ ou pour décider si elle est inversible, on peut écrire côte à côte les matrices S et I_n, puis effectuer des opérations élémentaires simultanément sur S et I_n jusqu'à obtenir la matrice I_n et une autre matrice à ses côtés. Cette matrice sera S^{-1} !

Exemple 2.1. On cherche l'inverse de la matrice carrée $S = \begin{pmatrix} a & 1 & 1 \\ 1 & a & 1 \\ 1 & 1 & a \end{pmatrix}$:

La matrice est échelonnée.
Posons $u = \dfrac{1}{2-a-a^2}$ pour simplifier l'écriture et réduisons la matrice :

Proposition 2.2. *Soit $A \in M_n(K)$.*
Alors le système $Ax = b$ admet une solution $\forall\ b \in M_{n\times 1}(K)$ si et seulement si $\det(A) \neq 0$.

Démonstration.

□

Remarque 2.3. Si $\det(A) = 0$, alors le système est impossible ou indéterminé. On peut alors échelonner la matrice augmentée pour trouver la solution.

Exemple 2.4. Résoudre le système $\begin{cases} 2x + y + z = 3 \\ x + 2y + z = 1 \\ x + y + 2z = 0 \end{cases}$

3 Matrices semblables

Lorsqu'on travaille avec des applications linéaires de V dans lui-même, on préfère fixer une seule base de V, au lieu de considérer une base de V comme espace vectoriel de départ et une autre comme espace d'arrivée. Nous avons le droit de le faire lorsque nous parlons de matrices ou d'applications linéaires équivalentes, mais le sens géométrique des applications devient obscur.

Exemple 3.1. Soit $\rho : \mathbb{R}^2 \to \mathbb{R}^2$ la rotation de centre $(0;0)$ et d'angle $\varphi = 17,345^o$.
Si l'on s'autorise à choisir deux bases différentes de $\mathbb{R}^2$, on arrive à obtenir I_2 comme matrice de cette rotation. En effet,

Par conséquent, nous décidons de fixer une seule base $\mathcal{B}$ de V et de représenter une application linéaire $\alpha : V \to V$ par la matrice carrée $A = (\alpha)^{\mathcal{B}}_{\mathcal{B}}$.

Définition 3.2. Deux matrices A et B de $M_n(K)$ sont *semblables* et on note $A \approx B$ s'il existe une matrice inversible $S \in GL_n(K)$ telle que $A = SBS^{-1}$.

Puisqu'une matrice de changement de base est une matrice inversible, nous obtenons le résultat suivant de la même façon que nous avons démontré le résultat correspondant sur les matrices équivalentes.

Théorème 3.3. *Deux matrices A et B de $M_n(K)$ sont semblables si et seulement si elles représentent la même application linéaire $\alpha : K^n \to K^n$, c'est-à-dire s'il existe deux bases $\mathcal{B}$ et $\mathcal{C}$ de K^n telles que $A = (\alpha)^{\mathcal{B}}_{\mathcal{B}}$ et $B = (\alpha)^{\mathcal{C}}_{\mathcal{C}}$.*

Démonstration. Soient $\mathcal{B}$ et $\mathcal{C}$ deux bases de K^n et $S = (Id)^{\mathcal{C}}_{\mathcal{B}}$ la matrice de changement de base de $\mathcal{B}$ vers $\mathcal{C}$. Alors le diagramme

$$(V,\mathcal{B}) \xrightarrow{Id_V} (V,\mathcal{C}) \xrightarrow{\alpha} (V,\mathcal{C}) \xrightarrow{Id_V} (V,\mathcal{B})$$

illustre l'égalité matricielle $A = (\alpha)^{\mathcal{B}}_{\mathcal{B}} = (Id)^{\mathcal{B}}_{\mathcal{C}}(\alpha)^{\mathcal{C}}_{\mathcal{C}}(Id)^{\mathcal{C}}_{\mathcal{B}} = S^{-1}BS$. □

Exemple 3.4. Décrire géométriquement l'application linéaire $\alpha : \mathbb{R}^3 \to \mathbb{R}^3$ définie par

$$\alpha(x; y; z) = (-0,8 \cdot y - 0,6 \cdot z; 0,8 \cdot x + 0,36 \cdot y - 0,48 \cdot z; 0,6 \cdot x + 0,64 \cdot z - 0,48 \cdot y).$$

La matrice de α dans la base canonique n'est pas très jolie :

$$A = \frac{1}{25} \begin{pmatrix} 0 & -20 & -15 \\ 20 & 9 & -12 \\ 15 & -12 & 16 \end{pmatrix}$$

et nous ne voyons pas de quoi il s'agit.
Choisissons judicieusement une autre base de $\mathbb{R}^3$, par exemple $\mathcal{B}^* = (f_1, f_2, f_3)$ avec

$$f_1 = e_1, \quad f_2 = \frac{4e_2 + 3e_3}{5} \quad \text{et} \quad f_3 = \frac{-3e_2 + 4e_3}{5}.$$

Calculons les images des f_i.

Remarquons que la base $\mathcal{B}^*$ que nous avons choisie est constituée de vecteurs de norme 1, orthogonaux deux à deux, et il s'agit d'une base directe, orientée comme la base canonique.

4 Valeurs propres et vecteurs propres

Pour construire la matrice d'une application linéaire $\alpha : V \to V$, nous sommes maintenant convaincus qu'une base vaut parfois mieux qu'une autre car l'interprétation géométrique est plus immédiate. Nous allons voir cette semaine quelques outils qui nous permettront par la suite de savoir s'il existe une base par rapport à laquelle la matrice de α est diagonale, et le cas échéant de trouver une telle base.
Pour cela, revenons dans le monde des matrices.

Définition 4.1. Un scalaire $\lambda \in K$ est *valeur propre* de la matrice $A \in M_n(K)$ s'il existe un vecteur non-nul $v \in M_{n\times 1}(K)$ tel que $Av = \lambda v$.
Un tel vecteur est appelé *vecteur propre* pour la valeur propre λ. L'*espace propre* E_λ est le sous-espace vectoriel de K^n formé de tous les vecteurs $v \in M_{n\times 1}(K)$ tels que $Av = \lambda v$.

Exemple 4.2. Soit $\alpha : \mathbb{R}^3 \to \mathbb{R}^3$ l'application linéaire de matrice

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

relativement à la base canonique de $\mathbb{R}^3$.
Vérifier que $u = (2; 1; 1)$ est un vecteur propre de α et préciser la valeur propre λ associée.
Donner une base de l'espace propre E_λ.

Il est facile de montrer directement que E_λ est un sous-espace, mais nous pouvons aussi nous appuyer sur l'identification suivante :

Proposition 4.3. *Soit λ une valeur propre de la matrice $A \in M_n(K)$.*
Alors l'espace propre E_λ est le noyau de $A - \lambda I_n$.

Démonstration.

□

Ainsi, pour découvrir les valeurs propres, puis calculer les espaces propres associés, il faut étudier la matrice $A - \lambda I_n$, trouver les valeurs de λ pour lesquelles le rang de cette matrice n'est pas maximal car si le rang est n, le noyau est réduit au vecteur nul et donc λ n'est pas une valeur propre. Une autre méthode consiste à utiliser le déterminant de la matrice.

Corollaire 4.4. *Soit la matrice $A \in M_n(K)$.*
Alors λ est une valeur propre de A si et seulement si $\det(A - \lambda I_n) = 0$.

Démonstration.

□

Exemple 4.5. Soit $\alpha : \mathbb{R}^3 \to \mathbb{R}^3$ l'endomorphisme de matrice

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

relativement à la base canonique de $\mathbb{R}^3$ donnée dans l'exemple 4.2.
Déterminer l'autre valeur propre de α, ainsi qu'une base de l'espace propre associé.
Prouver qu'il existe une base $\mathcal{B}^*$ formée de vecteurs propres et déterminer la matrice de α relativement à cette base $\mathcal{B}^*$.

VIII. Matrices diagonalisables

Pour terminer ce chapitre consacré aux bases de l'algèbre linéaire, nous étudierons aujourd'hui les matrices diagonalisables, qui sont les matrices semblables à une matrice diagonale. Cela nous permettra ensuite de décrire plus facilement des applications linéaires, en trouvant une base adaptée à l'interprétation géométrique.

1 Matrices diagonalisables

Pour construire la matrice d'une application linéaire $\alpha : V \to V$, nous avons vu qu'une base vaut parfois mieux qu'une autre car l'interprétation géométrique est plus immédiate. Notre but est de savoir s'il existe une base par rapport à laquelle la matrice de α est diagonale, et le cas échéant de trouver une telle base.

Définition 1.1. Une matrice $A \in M_n(K)$ est *diagonalisable* s'il existe une matrice inversible $S \in GL_n(K)$ telle que $SAS^{-1} = D$ est diagonale.
Une application linéaire $\alpha : V \to V$ est *diagonalisable* s'il existe une base $\mathcal{B}$ de V telle que $(\alpha)^{\mathcal{B}}_{\mathcal{B}} = D$ est diagonale.

Remarque 1.2. Une matrice A est donc diagonalisable si elle est semblable à une matrice diagonale.

Proposition 1.3. *Une application linéaire $\alpha : V \to V$ est diagonalisable si et seulement si il existe une base formée de vecteurs propres.*

Démonstration.

□

Exemple 1.4. Considérons la matrice $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Exemple 1.5. Considérons la matrice $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

Exemple 1.6. Considérons l'application linéaire $\alpha(x, y, z) = (3y - z, 2x - y + z, 2z)$.

Exprimé dans la base canonique la matrice de α est $A = \begin{pmatrix} 0 & 3 & -1 \\ 2 & -1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$.

Déterminons les valeurs propres :

Déterminons ensuite les espaces propres associés à chaque valeur propre :

La base (f_1, f_2, f_3) est une base de $\mathbb{R}^3$ formée de vecteurs propres.
Dans cette base, la matrice de α a la forme

Exemple 1.7. Les rotations du plan. Soit $\rho : \mathbb{R}^2 \to \mathbb{R}^2$ la rotation d'angle φ, un angle exprimé en radian, et R_φ la matrice de rotation correspondante, exprimée dans la base canonique. Alors

$$R_\varphi = \left(\qquad \right).$$

Remarquons d'abord que si $\sin\varphi = 0$,

Cherchons les valeurs propres lorsque $\sin\varphi \neq 0$:

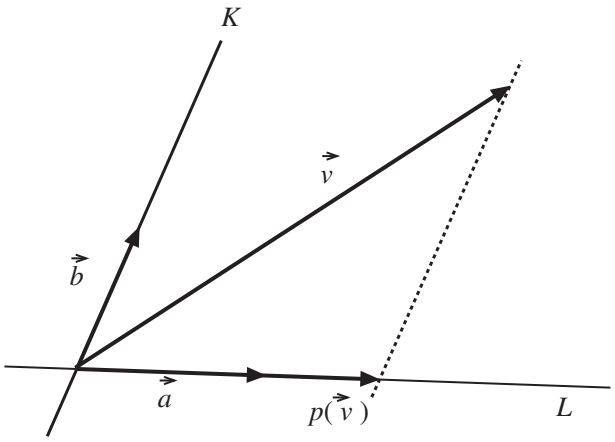
Exemple 1.8. Reprenons le même exemple, mais en considérant cette matrice dans $M_2(\mathbb{C})$.
Alors le polynôme $\lambda^2 - 2\cos(\varphi)\lambda + 1$ admet deux racines complexes distinctes.
En faisant les calculs, nous obtenons deux espaces propres de dimension 1.
On peut donc choisir une base de vecteurs propres afin de diagonaliser cette matrice !

Pour les sections suivantes, on fait la correspondance suivante entre points et vecteurs du plan ou de l'espace :

$$M(x;y) \iff \vec{v} = \begin{pmatrix} x \\ y \end{pmatrix} \qquad \text{et} \qquad M(x;y;z) \iff \vec{v} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

2 Projections vectorielles du plan

Soit $\vec{a}$ et $\vec{b}$ deux vecteurs non colinéaires de V_2.
L'application p qui associe à tout vecteur $\vec{v}$ sa projection $p(\vec{v})$ sur la droite vectorielle $L = \langle \vec{a} \rangle$ parallèlement à la droite vectorielle $K = \langle \vec{b} \rangle$ est une application linéaire.



Proposition 2.1. *Une application linéaire $\alpha : V_2 \to V_2$ est une projection si et seulement si elle possède les valeurs propres 0 et 1.*
Dans ce cas, α est une projection sur E_1 parallèlement à E_0.

Démonstration.

□

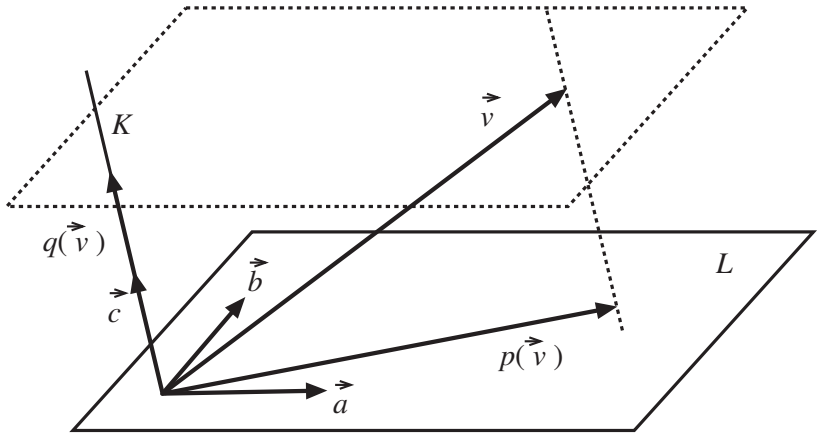
Exemple 2.2. Prouver que l'application linéaire $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ de matrice $A = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ relativement à la base canonique est une projection.

3 Projections vectorielles de l'espace

Soit $(\vec{a};\vec{b};\vec{c})$ trois vecteurs non coplanaires de l'espace.

- L'application p qui associe à tout vecteur $\vec{v}$ sa projection $p(\vec{v})$ sur le plan vectoriel $L = \langle\vec{a};\vec{b}\rangle$ parallèlement à la droite vectorielle $K = \langle\vec{c}\rangle$ est une application linéaire.
- L'application q qui associe à tout vecteur $\vec{v}$ sa projection $q(\vec{v})$ sur la droite vectorielle $K = \langle\vec{c}\rangle$ parallèlement au plan vectoriel $L = \langle\vec{a};\vec{b}\rangle$ est une application linéaire.
- Les projections p et q sont liées par la relation

$$q(\vec{v}) = \vec{v} - p(\vec{v}) = (\mathrm{id}_{V_3} - p)(\vec{v})$$



Proposition 3.1. *Une application linéaire $\alpha : V_3 \to V_3$ est une projection si et seulement si elle possède les valeurs propres 0 et 1 et si l'un des espaces propres est de dimension 2.*
Dans ce cas, α est une projection sur E_1 parallèlement à E_0.

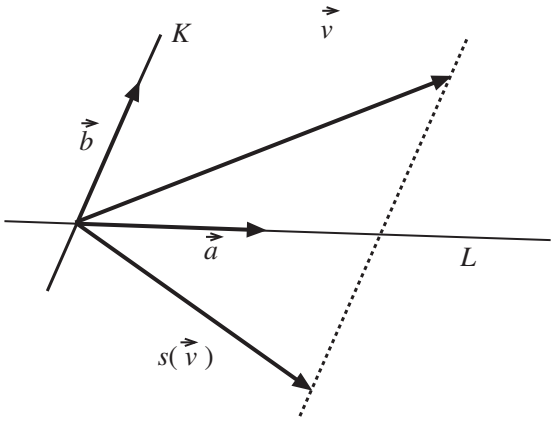
Démonstration.

□

Remarque 3.2. Une projection p vérifie forcément $p \circ p = p$. En effet, vous prouverez en exercices que si $p \circ p = p$, alors les seules valeurs propres possibles sont 0 et 1. La réciproque est évidente.

4 Symétries vectorielles du plan

Soit $\vec{a}$ et $\vec{b}$ deux vecteurs non colinéaires de V_2. L'application s qui associe à tout vecteur $\vec{v}$ son symétrique $s(\vec{v})$ relativement à la droite vectorielle $L = \langle\vec{a}\rangle$ parallèlement à la droite vectorielle $K = \langle\vec{b}\rangle$ est une application linéaire.



Proposition 4.1. *Une application linéaire $\alpha : V_2 \to V_2$ est une symétrie si et seulement si elle possède les valeurs propres -1 et 1.*
Dans ce cas, α est une symétrie relativement à E_1 parallèlement à E_{-1}.

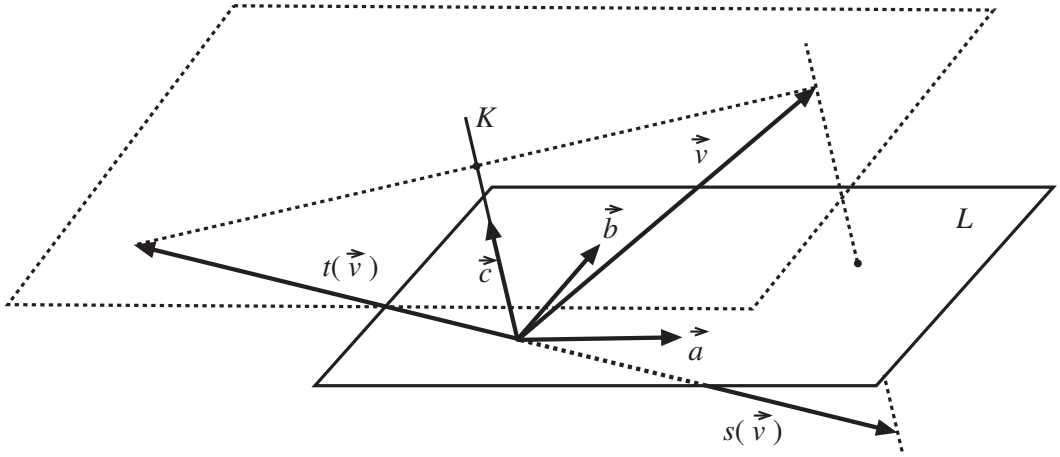
Exemple 4.2. Dans V_2 muni d'une base orthonormée $\mathcal{B}$, on considère la symétrie orthogonale s d'axe d d'équation $y = x$. Déterminer la matrice de s relativement à $\mathcal{B}$.

5 Symétries vectorielles de l'espace

Soit $(\vec{a};\vec{b};\vec{c})$ trois vecteurs non coplanaires de l'espace.

- L'application s qui associe à tout vecteur $\vec{v}$ son symétrique $s(\vec{v})$ relativement au plan vectoriel $L = \langle\vec{a};\vec{b}\rangle$ parallèlement à la droite vectorielle $K = \langle\vec{c}\rangle$ est une application linéaire.
- L'application t qui associe à tout vecteur $\vec{v}$ son symétrique $t(\vec{v})$ relativement à la droite vectorielle $K = \langle\vec{c}\rangle$ parallèlement au plan vectoriel $L = \langle\vec{a};\vec{b}\rangle$ est une application linéaire.
- Les symétries s et t sont liées par la relation

$$t(\vec{v}) = -s(\vec{v})$$



Proposition 5.1. *Une application linéaire $\alpha : V_3 \to V_3$ est une symétrie si et seulement si elle possède les valeurs propres -1 et 1 et si l'un des espaces propres est de dimension 2.*
Dans ce cas, α est une symétrie relativement à E_1 parallèlement à E_{-1}.

Remarque 5.2. Une symétrie s vérifie forcément $s \circ s = Id$. En effet, on prouvera en exercices que si $s \circ s = Id$, alors les seules valeurs propres possibles sont 1 et -1.

Exemple 5.3. Dans l'exemple 4.5 du cours VII, on considérait l'endomorphisme $\alpha : \mathbb{R}^3 \to \mathbb{R}^3$ dont la matrice relativement à la base canonique était

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

Ses valeurs propres étaient 1 et -1 (double) et la matrice était diagonalisable.
Il s'agit donc

Exemple 5.4. Dans V_3 muni d'une base orthonormée $\mathcal{B}$, on considère la symétrie vectorielle orthogonale s relativement à la droite d d'équation $x = -y = z$.
Déterminer la matrice de s relativement à $\mathcal{B}$.