Cours d'algèbre

Alain TROESCH

23 juin 2010

Table des matières

1 Fondements des mathématiques **5**
1.1 Rudiments de logique . . . 5
1.1.1 Terminologie . . . 5
1.1.2 Connecteurs logiques – Tables de vérité . . . 5
1.1.3 Quantificateurs . . . 7
1.1.4 Négations . . . 8
1.1.5 Un texte mathématique . . . 8
1.1.6 Types de démonstrations . . . 9
1.2 Ensembles . . . 11
1.2.1 Définitions . . . 11
1.2.2 Constructions d'ensembles . . . 11
1.2.3 Lien avec les connecteurs logiques. . . . 13
1.3 Applications . . . 13
1.3.1 Injectivité, surjectivité, bijectivité . . . 14
1.3.2 Familles . . . 15
1.4 Relations . . . 16
1.4.1 Relations binaires . . . 16
1.4.2 Relations d'équivalence . . . 16
1.4.3 Relations d'ordre . . . 17

2 Polynômes et nombres complexes **19**
2.1 Polynômes à coefficients réels . . . 19
2.1.1 Polynômes formels, opérations arithmétiques . . . 19
2.1.2 Dérivation . . . 20
2.1.3 Degré et valuation . . . 20
2.1.4 Évaluation, racines . . . 21
2.1.5 Division euclidienne . . . 22
2.1.6 Divisibilité et racines . . . 22
2.2 Nombres complexes . . . 23
2.2.1 De l'existence des racines d'un polynôme . . . 23
2.2.2 Propriétés arithmétiques des nombres complexes . . . 24
2.2.3 Rappel : formules trigonométriques . . . 25
2.2.4 L'exponentielle complexe . . . 25
2.2.5 Racines de l'unité, racines d'un complexe . . . 26
2.3 Application à la trigonométrie . . . 26
2.3.1 Formule d'Euler, formules trigonométriques . . . 26

2.3.2 Symétrisation d'une somme de complexes de même module 27
2.3.3 Linéarisation ; polynômes de Tchebychev 27
2.3.4 Calcul de sommes de cosinus ou de sinus 28
2.4 Spécificités des polynômes à coefficients complexes 28
2.4.1 Autour du théorème de d'Alembert-Gauss 28
2.4.2 Racines complexes des polynômes réels 29
2.4.3 Application aux factorisations dans $\mathbb{R}[X]$ 29

3 Espaces vectoriels 31
3.1 Notion d'espace vectoriel 31
3.1.1 Définition 31
3.1.2 Un exemple important : espace de fonctions 32
3.1.3 Sous-espaces vectoriels 32
3.2 Constructions 32
3.2.1 Intersection 32
3.2.2 Produit 33
3.2.3 Somme, somme directe 33
3.3 Familles de vecteurs 33
3.3.1 Combinaisons linéaires 33
3.3.2 Familles libres 34
3.3.3 Familles génératrices 35
3.3.4 Bases 35
3.4 Espaces vectoriels de dimension finie 36
3.4.1 Notion de dimension 36
3.4.2 Dimension, liberté et rang 36
3.4.3 Dimension de sommes 37

4 Applications linéaires 39
4.1 Généralités sur les applications linéaires 39
4.1.1 Définition et arithmétique des applications linéaires 39
4.1.2 Image et noyau 39
4.1.3 Isomorphismes 40
4.1.4 Projecteurs et symétries 40
4.2 Matrices 41
4.2.1 Définition et motivations 41
4.2.2 Somme et produit de matrices 42
4.2.3 Inverse d'une matrice 44
4.2.4 Transposition 45
4.2.5 Produit par blocs 45
4.3 Écriture d'une AL dans une base 45
4.3.1 Définitions et notations 45
4.3.2 Changements de base 46
4.3.3 Cas des endomorphismes 47
4.4 Applications linéaires en dimension finie 47
4.4.1 Rang d'une application linéaire 47
4.4.2 Formes linéaires 48
4.4.3 Rang d'une matrice 48

5 Le pivot de Gauss **49**
5.1 Matrices échelonnées 49
5.1.1 Définition 49
5.1.2 Matrices échelonnées inversibles 50
5.1.3 Rang d'une matrice échelonnée 50
5.2 Le pivot de Gauss 50
5.2.1 Opérations élémentaires 50
5.2.2 L'algorithme du pivot 52
5.2.3 Pivot double 55
5.3 Calcul de l'inverse d'une matrice 55
5.4 Résolution de systèmes linéaires 56
5.4.1 Définitions et généralités 56
5.4.2 Résolution du système homogène associé 57
5.4.3 Trouver une solution particulière 58
5.4.4 De l'existence ou de l'unicité des solutions 58
5.4.5 Systèmes de Cramer 58
5.5 Rang d'une transposée 59
5.6 Complétion d'une famille libre en une base 59

6 Diagonalisation **61**
6.1 Diagonalisation des endomorphismes 61
6.1.1 Objectif 61
6.1.2 Valeurs propres, vecteurs propres 61
6.1.3 Etude des sous-espaces propres 63
6.1.4 Critères de diagonalisation 64
6.1.5 Polynômes annulateurs 64
6.1.6 Méthode de diagonalisation (Bilan) 64
6.2 Diagonalisation des matrices carrées 65
6.2.1 Matrices semblables 65
6.2.2 Principes et critères de diagonalisation 65
6.2.3 Cas des matrices 2×2 66
6.2.4 Une application : suites définies par une récurrence linéaire 66

Chapitre 1

Fondements des mathématiques

1.1 Rudiments de logique

1.1.1 Terminologie

- **Objet** ou **élément** : donnée première intuitive (cela peut être un nombre, une personne, un livre, un endroit, une entité quelconque...). Ce sont les briques (on ne peut pas construire à partir de rien)
- **Ensemble** : une collection d'éléments. Un ensemble de personnes, de nombres, de livres...
- **Appartenance** : un élément appartient à un ensemble ($x \in E$) si cet élément est dans la collection définissant E
- **Constante** : un signe ayant une valeur précise et immuable ; par exemple un entier, ou un réel donné : 1, 2, π etc ; par exemple, une personne donnée.
- **Variable** : un signe pouvant prendre différentes valeurs, parmis un certain ensemble, ou n'ayant pas de valeur prédéfinie.
  Exemple : x vérifiant $x^2 = 1$
- **Proposition** : un énoncé exprimant une certaine propriété (vérifiée ou non par un élément, un ensemble). Une proposition est donnée sans considération de validité : elle peut être vraie ou fausse.
  Exemple : *Le blé est une céréale* est une proposition portant sur l'élément *blé* et l'ensemble *céréales*. Cette proposition est vraie.
- **Valeur de vérité d'une proposition** : une proposition peut être vraie, ou fausse, ou vraie pour certaines valeurs d'une variable et fausse pour d'autres.
- **Variable muette** : c'est une variable qui est définie au sein même de la proposition. Elle n'a pas de sens en dehors de la proposition, et peut être formellement remplacée par n'importe quelle autre variable (dans toute la proposition)
  Remarque : les variables muettes apparaissent aussi dans les sommations : $\displaystyle\sum_{i=1}^{n} i^2$, i est une variable muette (mais pas n) ; $\displaystyle\int_0^1 f(x)\,\mathrm{d}x$, x est une variable muette.
- **Formule close** : une proposition dont toutes les variables sont muettes.

1.1.2 Connecteurs logiques – Tables de vérité

Ce sont des mots ou symboles permettant de définir de nouvelles propositions.

1. La conjonction « et » (notée symboliquement $\wedge$), de table :

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

2. Le « ou » non exculsif (notée symboliquement $\vee$), de table :

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

3. Le « non » (notée symboliquement $\neg$), de table :

P	$\neg P$
V	F
F	V

4. L'implication (notée symboliquement $\Longrightarrow$), de table :

P	Q	$P \Longrightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

5. L'équivalence $P \Longleftrightarrow Q \equiv (P \Longrightarrow Q) \wedge (Q \Longrightarrow P)$.

REMARQUES 1.1.1 1. Si P est fausse, $P \Longrightarrow Q$ est toujours vraie. Ainsi, la véracité de $P \Longrightarrow Q$ ne sous-entend nullement la véracité de P.

2. En particulier, « $\Longrightarrow$ » n'est pas synonyme de « donc », qui sous-entend que ce qui précède est vrai.
3. Pour montrer que $P \Longrightarrow Q$ est vraie, il suffit de se placer dans le cas où P est vraie, et de montrer qu'alors Q est vraie.
4. Ne pas confondre :
   - P est une condition suffisante à Q : $P \Longrightarrow Q$;
   - P est une condition nécessaire à Q : $Q \Longrightarrow P$;
   - P est une condition nécessaire et suffisante à Q : $P \Longleftrightarrow Q$.
5. Pour montrer une équivalence $P \Longleftrightarrow Q$, n'oubliez pas de montrer les *deux* implications $P \Longrightarrow Q$ et $Q \Longrightarrow P$. N'oubliez pas la réciproque SVP.

EXEMPLES 1.1.2 1. La proposition suivante est vraie :

« *Si* $10^n + (-1)^n$ *est divisible par 11, alors* $10^{n+1} + (-1)^{n+1}$ *est divisible par 11.* »

Pourtant, $10^n + (-1)^n$ n'est divisible par 11 pour aucune valeur de n !

2. (Exemple historique) Il existe deux célèbres conjectures, appelons-les A et B. La conjecture A est à ce jour encore à démontrer. La conjecture B a été démontrée en deux temps : un

premier mathématicien a réussi à prouver que si A est vraie, B aussi. Un peu plus tard, un autre mathématicien a prouvé que si A est fausse, alors B est vraie... Ainsi, on a montré la conjecture B a partir de la conjecture A, sans rien connaître de la véracité de la conjecture A !

3. Autour de CN et CS :
   - « n est multiple de 6 » est une CS pour que n soit paire mais pas une CN.
   - $x = 1$ est une CS pour que $x^2 = 1$, mais pas une CN. En revanche, si x est réel, $x = 1$ est une CNS pour que $x^3 = 1$.
   - Si f est dérivable sur $\mathbb{R}$, $f'(0) = 0$ est une CN pour que f admette un extremum local en 0, mais ce n'est pas une CS (exemple : $x \mapsto x^3$)

REMARQUE 1.1.3 On distingue implication formelle et implication sémantique (relation de cause à effet). Par exemple, le grand théorème de Fermat ayant été démontré il y a quelques années, la proposition suivante est vraie :

« *Si le théorème de Fermat est faux, alors les oranges sont bleues* »

En revanche, une telle implication ne traduit aucune relation de cause à effet !

PROPOSITION 1.1.4 *Pour toutes propositions P, Q et R, on a :*

1. $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$ *(associativité de $\wedge$). On note : $P \wedge Q \wedge R$.*
2. $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$ *(associativité de $\vee$). On note : $P \vee Q \vee R$.*
3. $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$ *(distributivité de $\vee$ sur $\wedge$)*
4. $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$ *(distributivité de $\wedge$ sur $\vee$)*

1.1.3 Quantificateurs

Ce sont des symboles d'*abréviation* permettant d'introduire des variables.
Important : Dans toute expression mathématique que vous écrivez, assurez-vous toujours que toutes les variables que vous utilisez soient définies (soit par une valeur particulière, soit par un quantificateur, soit posée dans le texte).

1. $\forall$: quel que soit.
   - Exemple d'utilisation : $\forall x,\ x \geqslant 2 \Longrightarrow x^2 \geqslant 4$.
   - Abus de notation : on écrit « $\forall x \in E,\ P$ » pour « $\forall x,\ (x \in E) \Longrightarrow P$ »
     Ainsi, l'expression précédente s'écrit aussi : $\forall x \geqslant 2,\ x^2 \geqslant 4$.
   - Pour montrer $\forall x\ P(x)$, se donner x quelconque et vérifier $P(x)$ (en toute généralité). La démonstration a donc la structure suivante :
     « Soit x. ... (*démonstration*) ... Alors $P(x)$. Donc $P(x)$ est vérifiée pour tout x. »
2. $\exists$: il existe.
   - Exemple d'utilisation : $\exists x,\ x^2 = 2$.
   - Abus de notation : on écrit « $\exists x \in E,\ P$ » pour « $\exists x,\ (x \in E) \wedge P$ »
   - L'ensemble dans lequel on considère l'existence peut avoir son importance. N'oubliez pas de le préciser en cas d'ambiguïté.
     Exemple : $\exists x \in \mathbb{R},\ x^2 = -1$ et $\exists x \in \mathbb{C},\ x^2 = -1$ n'ont pas vraiment la même véracité !
3. Juxtaposition :
   Attention : $\forall x \exists y,\ P \not\equiv \exists y \forall x,\ P$.

1.1.4 Négations

Proposition 1.1.5 *Soit A et B deux propositions. Alors :*

1. $\neg(A \wedge B) \equiv \neg A \vee \neg B$
2. $\neg(A \vee B) \equiv \neg A \wedge \neg B$
3. $\neg(\neg A) \equiv A$
4. $\neg(A \Longrightarrow B) \equiv A \wedge \neg B$
5. $\neg(\exists x,\ P(x)) \equiv (\forall x, \neg P(x))$
6. $\neg(\forall x,\ P(x)) \equiv (\exists x, \neg P(x))$.

Exemples 1.1.6
1. Non linéarité d'une fonction de $\mathbb{R}^n$ vers $\mathbb{R}^m$; exemple de $f : x^2 \mapsto x$ de $\mathbb{R}$ dans $\mathbb{R}$.
2. Définition de la continuité d'une fonction f en x_0, puis négation. Exemple de la fonction H de Heaviside.

1.1.5 Un texte mathématique

Un texte mathématique est constitué de :

1. **définitions** : des descriptions de certains objets constituant les briques de la théorie. Une définition est un fait, et n'appelle par de démonstration.
2. **résultats** : des énoncés mettant en jeu les objets définis dans la théorie, et donnant des propriétés vérifiées par ces objets. Un résultat s'énonce sous la forme $A \Longrightarrow B$. On distingue :
   - les *axiomes* : des résultats qui sont des vérités fondamentales de la théorie, et qu'on ne démontre pas (à considérer comme le cahier des charges de la théorie : on impose ces résultats, il n'y a donc pas besoin de les montrer) ;
   - les *théorèmes* : les résultats les plus significatifs, démontrés à partir des axiomes et de résultats démontrés antérieurement ;
   - les *propositions* : des résultats de moindre envergure ;
   - les *lemmes* (d'un autre résultat) : des résultats intermédiaires, utiles à la démonstration du résultat dont ils sont le lemme ; ils peuvent être lemme de plusieurs résultats, et peuvent être très utiles pour d'autres démonstrations ;
   - les *corollaires* (d'un autre résultat) : des conséquences assez immédiates dudit résultat, par exemple des cas particuliers intéressants ;
   - les *conjectures* : des résultats qu'on suppose être vrai, mais qu'on n'a pas réussi à prouver.
3. **démonstrations** : des justifications de la véracité des résultats.

Exemples 1.1.7
1. Le célèbre cinquième axiome d'Euclide, fondant la théorie de la géométrie euclidienne, stipule qu'il existe une seule droite parallèle à une droite donnée, et passant par un point donné. Il existe d'autres types de géométrie, définies en changeant cet axiome :
   - la géométrie sphérique, dans laquelle une droite n'admet pas d'autre parallèle qu'elle même ;
   - la géométrie de Lobatchevsky, dans laquelle une droite admet une infinité de parallèles passant par un point donné ;
   - et d'autres encore...
2. Un énoncé s'exprime souvent sous la forme $A \Longrightarrow B$.
   La proposition A regroupe les *hypothèses*
   La proposition B regroupe les *conclusions.*
   Ne pas oublier de bien apprendre toutes les hypothèses d'un résultat. Par exemple, considérons le théorème suivant :

Soit f une fonction dérivable sur un intervalle I. Si f' est positive sur I, alors f est croissante sur I.

Il y a trois hypothèses dans cet énoncé : bien sûr, $f' \geqslant 0$, que personne n'oublie ; mais aussi f dérivable sur I (sans laquelle l'énoncé n'a pas de sens), et (plus souvent oubliée) le fait que I est un intervalle (sans quoi le résultat est faux !).

1.1.6 Types de démonstrations

1. **Le syllogisme.** Pour que B soit vrai, il suffit que A soit vrai et que $A \Longrightarrow B$; le principe du syllogisme s'écrit donc : $(A \wedge (A \Longrightarrow B)) \Longrightarrow B$. C'est une démonstration « directe » Remarquez qu'on ne peut pas se contenter de $A \Longrightarrow B$, il faut aussi la véracité de A.
2. **La transitivité de $\Longrightarrow$.** On utilise une succession de syllogismes :
$$A \wedge (A \Longrightarrow A_1) \wedge (A_1 \Longrightarrow A_2) \wedge (A_{n-1} \Longrightarrow A_n) \wedge (A_n \Longrightarrow B) \Longrightarrow B.$$
3. **Démonstration par la contraposée.** En comparant les tables de vérité, ou en niant les deux propositions, on obtient :
$$A \Longrightarrow B \equiv \neg B \Longrightarrow \neg A$$
L'expression $\neg B \Longrightarrow \neg A$ s'appelle la *contraposée* de $A \Longrightarrow B$. Démontrer une implication $A \Longrightarrow B$ consiste à démontrer l'implication $\neg B \Longrightarrow \neg A$, c'est-à-dire à supposer que B est faux, et montrer qu'alors A est faux aussi.
4. **Cas particulier : démonstration par l'absurde.** C'est le cas où A est la proposition toujours vraie. Alors $A \Longrightarrow B \equiv B$. Ainsi, pour démontrer B, il suffit de démontrer la contraposée $\neg B \Longrightarrow \neg A$, où $\neg A$ est la proposition toujours fausse(= une contradiction). Par conséquent, il suffit de supposer que B est fausse, et d'aboutir à une contradiction.
5. **Disjonction des cas.** Si $A \Longrightarrow C$ et $B \Longrightarrow C$, alors $(A \vee B) \Longrightarrow C$:
$$((A \Longrightarrow C) \wedge (B \Longrightarrow C)) \Longrightarrow ((A \vee B) \Longrightarrow C).$$
Cas particulier : $A \vee B$ est toujours vraie (ainsi A et B regroupe toutes les « possibilités »). Alors, pour montrer C, il suffit de montrer $A \Longrightarrow C$ et $B \Longrightarrow C$, c'est-à-dire de montrer C dans le cas où A est vrai, et C dans le cas où B est vrai.
6. **Raisonnement par récurrence**
   (a) Principe de la récurrence simple : $[\mathcal{P}(0) \wedge (\forall n \in \mathbb{N},\ (\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1))] \Longrightarrow (\forall n \in \mathbb{N},\ \mathcal{P}(n))$
   « $\mathcal{P}(0)$ » est l'initialisation, « $\forall n \in \mathbb{N},\ (\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1))$ » est l'hérédité.
   - Le rang initial peut être un autre entier (éventuellement négatif). Attention à montrer l'hérédité à partir d'un bon rang.
   - Existence de récurrences descendantes
   - Il peut être judicieux d'avoir des quantificateurs dans l'hypothèse de récurrence.
   - N'oubliez pas l'initialisation !
   - Attention à ce que l'hérédité soit valable en toute généralité (problème des crayons de couleur)

   (b) Récurrence d'ordre k :
$$((\mathcal{P}(0) \wedge \cdots \wedge \mathcal{P}(k-1)) \wedge (\forall n \in \mathbb{N},\ \mathcal{P}(n) \wedge \cdots \wedge \mathcal{P}(n+k-1) \Longrightarrow \mathcal{P}(n+k))) \Longrightarrow \forall n \in \mathbb{N},\ \mathcal{P}(n).$$

- Principe : on utilise la propriété aux k rangs précédents pour montrer l'hérédité.
- Ne pas oublier d'initialiser pour les k premières valeurs !
- Adapter le principe dans le cas où le rang initial n'est pas 0.

(c) Récurrence forte : $(\mathcal{P}(0) \wedge (\forall n \geqslant 1,\ \mathcal{P}(0) \wedge \cdots \wedge \mathcal{P}(n-1) \Longrightarrow \mathcal{P}(n))) \Longrightarrow \forall n \in \mathbb{N},\ \mathcal{P}(n)$.

- Principe : on suppose la propriété vraie à tous les rangs précédents pour la montrer à un rang donné.
- Il suffit d'initialiser sur le premier terme.
- Très utile pour toutes les questions de divisibilité.

(d) Récurrences multiples : On opère simultanément des récurrences sur plusieurs variables. On imbrique en général les récurrences les unes dans les autres. Attention à bien énoncé les propriétés à démontrer pour chaque récurrence. Notamment, n'oubliez pas d'indiquer soigneusement les quantificateurs pour les récurrences « externes ».

EXEMPLES 1.1.8 1. (Syllogisme) Ce type de démonstration est utilisé pour tout emploi d'un théorème : $A \wedge (A \Longrightarrow B)$ signifie que comme les hypothèses du théorème $A \Longrightarrow B$ sont vraies, la conclusion B également.

Règle n° 1 d'une bonne rédaction : quand on rédige un tel raisonnement faisant référence à un théorème, il est nécessaire de toujours préciser le théorème utilisé (soit en donnant son nom, soit en rappelant son énoncé), ET de préciser que TOUTES les hypothèses sont satisfaites. De la nécessité de bien apprendre les hypothèses des théorèmes...

2. (Transitivité de l'implication) Résolution des équations du second degré.
3. (Contraposée) Soit $n \in \mathbb{N}$. Montrer que si n^2 est pair, alors n est pair.
4. (Démonstration par l'absurde) Démonstration de l'irrationnalité de $\sqrt{2}$.
5. (Disjonction des cas) Montrer que pour tout $n \in \mathbb{N}$, $\frac{n(n+1)}{2}$ est entier. De même pour $\frac{n(n+1)(2n+1)}{6}$.
6. (Récurrence simple) Montrer que pour tout $n \in \mathbb{N}^*$, $\sum\limits_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.
7. (Récurrence simple) Formule du binôme de Newton.
8. (Récurrence simple, problème de quantificateurs) Soit $n \in \mathbb{N}^*$. Montrer que la somme de deux fonctions n fois dérivables est n fois dérivable (en supposant démontré pour $n = 1$).
9. (Récurrence simple, problème d'initialisation) $10^n + (-1)^n$ est-il divisible par 11 pour tout $n \in \mathbb{N}$?
10. (Récurrence simple, problème d'initialisation) Cherchez l'erreur.

    « *Dans toute boîte de n crayons, tous les crayons ont la même couleur.* »

11. (Récurrence d'ordre $k > 1$) Soit $(F_n)_{n\in\mathbb{N}}$ définie par $F_0 = 0$, $F_1 = 1$ et pour tout $n \geqslant 0$, $F_{n+2} = F_{n+1} + F_n$ (suite de Fibonacci).
    Soit $n \in \mathbb{N}$. Montrer que F_n est paire si et seulement si n est multiple de 3.
12. (Récurrence forte) Tout nombre entier $n \geqslant 0$ admet une décomposition en nombres de Fibonacci distincts non consécutifs.
13. (Récurrence forte) Tout nombre entier $n \geqslant 1$ admet une décomposition en produit de nombres premiers.

1.2 Ensembles

1.2.1 Définitions

Pour définir rigoureusement la notion d'*ensemble*, il faut une axiomatique très complexe, c'est pourquoi nous admettons cette notion ; intuitivement, il s'agit d'une collection d'objets, ne se contenant pas lui-même (afin d'éviter le paradoxe de l'ensemble des ensembles).
On note l'appartenance de l'objet x à un ensemble E par $x \in E$.
Un ensemble F est *inclus* dans E si tous ses éléments sont aussi des éléments de E : $x \in F \Longrightarrow x \in E$. On note $F \subset E$ pour dire que F est inclus dans E.
Un *sous-ensemble* de E est un ensemble F tel que $F \subset E$.

EXEMPLE 1.2.1 $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}_+$, $\mathbb{R}_-$, $\mathbb{R}^*$, $\mathbb{R}_+^*$ etc.

DÉFINITION 1.2.2 Un singleton est un ensemble ne contenant qu'un élément : $\{x\}$

DÉFINITION 1.2.3 Un ensemble vide, noté $\varnothing$, est un ensemble ne contenant aucun élément. Il est donc défini par : $\forall x, x \notin \varnothing$.
C'est une notion abstraite ; il n'est *a priori* pas évident qu'un tel ensemble existe, ni qu'il soit unique.

Un ensemble est dit *fini* s'il ne contient qu'un nombre fini d'éléments. Le cardinal d'un ensemble fini E, noté $\mathrm{Card}(E)$ ou $|E|$, est le nombre des éléments de E.

Comment décrire un ensemble ?

1. En énumérant ses éléments entre accolades : $\{1, 2, 4\}$;
2. En le décrivant comme le sous-ensemble des éléments d'un ensemble connu vérifiant une certaine propriété $\mathcal{P}$: $\{x \in E \mid \mathcal{P}(x)\}$
3. Par des constructions classiques. On étudie les plus classiques et les plus simples ci-dessous.

1.2.2 Constructions d'ensembles

1.2.2.1 Intersection.

DÉFINITION 1.2.4 Soit E et F deux ensembles. L'intersection de E et F, notée $E \cap F$, est l'ensemble des éléments contenus à la fois dans E et dans F :

$$x \in E \cap F \Longleftrightarrow (x \in E) \wedge (x \in F).$$

PROPOSITION 1.2.5 *Soit E, F, G des ensembles. Alors :*

1. $E \cap F = F \cap E$ *(commutativité)*
2. $(E \cap F) \cap G = E \cap (F \cap G)$ *(associativité)*
3. $E \cap \varnothing = \varnothing$
4. *Si* $E \subset F$, *alors* $E \cap F = E$.

1.2.2.2 Union

Définition 1.2.6 Soit E et F deux ensembles. L'union de E et F, notée $E \cup F$, est l'ensemble des éléments contenus soit dans E soit dans F :

$$x \in E \cup F \iff (x \in E) \vee (x \in F).$$

Proposition 1.2.7 *Soit E, F, G des ensembles. Alors :*

1. $E \cup F = F \cup E$ *(commutativité)*
2. $(E \cup F) \cup G = E \cup (F \cup G)$ *(associativité)*
3. $E \cup \varnothing = E$
4. *Si* $E \subset F$, *alors* $E \cup F = F$.
5. $(E \cup F) \cap G = (E \cap G) \cup (F \cap G)$ *(distributivité de* $\cap$ *sur* $\cup$*)*
6. $(E \cap F) \cup G = (E \cup G) \cap (F \cup G)$ *(distributivité de* $\cup$ *sur* $\cap$*)*

1.2.2.3 Complémentation

Définition 1.2.8 Soit $E \subset F$. Le *complémentaire* de E dans F, noté $\complement_F E$, est l'ensemble des éléments de F qui ne sont pas dans E :

$$x \in \complement_F E \iff (x \in F) \wedge x \notin E.$$

Proposition 1.2.9 *Soit E, F et G des ensembles.*

1. $\complement_F E \cup E = F$
2. $\complement_F E \cap E = \varnothing$
3. *Soit* $E, F \subset G$. *Alors* $\complement_G(E \cup F) = \complement_G E \cap \complement_G F$
4. *Soit* $E, F \subset G$. *Alors* $\complement_G(E \cap F) = \complement_G E \cup \complement_G F$

Théorème 1.2.10 *L'ensemble vide existe et est unique. De plus, il est un sous-ensemble de tout ensemble.*

1.2.2.4 Produit Cartésien

Définition 1.2.11 Soit E et F deux ensembles. Le produit cartésien de E et F, noté $E \times F$, est l'ensemble des couples (a, b), tels que $a \in E$ et $b \in F$.

Notation 1.2.12 On note $E^2 = E \times E$, et plus généralement E^n pour un produit catésien à n termes.

Proposition 1.2.13 *Soit E, E' et F des ensembles. Alors :*

1. $E \times F = \varnothing \iff (E = \varnothing) \vee (F = \varnothing)$;
2. $(E \cup E') \times F = (E \times F) \cup (E' \times F)$;
3. $(E \cap E') \times F = (E \times F) \cap (E' \times F)$;

1.2.2.5 Ensemble des parties d'un ensemble

Une partie d'un ensemble est un autre nom donné à un sous-ensemble. L'ensemble des parties d'un ensemble E est donc l'ensemble de tous les sous-ensembles de E. On note $\mathcal{P}(E)$ cet ensemble.

REMARQUE 1.2.14 $\mathcal{P}(E)$ n'est jamais vide : il contient toujours $\varnothing$ et E. Par exemple, $\mathcal{P}(\varnothing) = \{\varnothing\}$.

DÉFINITION 1.2.15 Une partition de E est un sous-ensemble de $\mathcal{P}(E)$ dont les éléments sont des sous-ensembles non vides de E, deux à deux disjoints et d'union égale à E.
Par exemple, une partition finie, est un ensemble $\{A_1, \ldots, A_n\}$ de sous-ensembles de E tels que :

1. $\forall i \in [\![1, n]\!],\ E_i \neq \varnothing$,
2. $\forall (i,j) \in [\![1, n]\!]^2,\ i \neq j \Longrightarrow E_i \cap E_j = \varnothing$,
3. $E_1 \cup \cdots \cup E_n = E$.

1.2.3 Lien avec les connecteurs logiques.

Bien avoir à l'esprit la correspondance entre opérations ensemblistes et connecteurs logiques :

$$\begin{array}{ll}
\cup \equiv \vee & x \in A \cup B \Longleftrightarrow (x \in A) \vee (x \in B) \\
\cap \equiv \wedge & x \in A \cap B \Longleftrightarrow (x \in A) \wedge (x \in B) \\
\complement \equiv \neg & \text{si } x \in A,\ \big(x \in \complement_A B \Longleftrightarrow \neg(x \in B)\big) \\
\subset \equiv \Longrightarrow & A \subset B \Longleftrightarrow (\forall x,\ x \in A \Longrightarrow x \in B), \\
= \equiv \Longleftrightarrow & A = B \Longleftrightarrow (\forall x,\ x \in A \Longleftrightarrow x \in B).
\end{array}$$

1.3 Applications

DÉFINITION 1.3.1 Une application f est la donnée d'un sous-ensemble G de $E \times F$ (donc une relation) tel que :

$$\forall x \in E,\ \exists! y \in F,\ (x,y) \in G.$$

Ainsi, tout point x de E a une unique image y. Cette image est notée $f(x)$.

DÉFINITION 1.3.2 Soit E et F deux ensembles, et $f : E \longrightarrow F$ une application de E vers F.

1. L'image de f est l'ensemble $\mathrm{Im}(f) = \{y \in F \mid \exists x \in E,\ f(x) = y\}$.
   C'est l'ensemble des points de F qui sont images d'un certain point x.
2. Soit $E' \subset E$ un sous-ensemble de E. L'image directe de E' est l'ensemble : $f(E') = \{y \in F \mid \exists x \in E',\ f(x) = y.\}$. C'est l'ensemble des valeurs qui sont images d'un x de E'.
3. L'application « image directe », notée $\hat{f}$ (parfois f lorsqu'il n'y a pas d'ambiguïté) est l'application de $\mathcal{P}(E)$ dans $\mathcal{P}(F)$ qui à tout sous-ensemble E' de E associe son image directe $f(E') \subset F$.
4. Soit $F' \subset F$ un sous-ensemble de F. L'image réciproque de F' est l'ensemble : $f^{-1}(F') = \{x \in E \mid f(x) \in F'\}$. C'est l'ensemble des éléments s'envoyant dans F'.
5. L'application « image réciproque », notée $\widehat{f^{-1}}$ (parfois f^{-1} lorsqu'il n'y a pas d'ambiguïté) est l'application de $\mathcal{P}(F)$ dans $\mathcal{P}(E)$ qui à tout sous-ensemble F' de F associe son image réciproque $f^{-1}(E') \subset E$.

REMARQUE 1.3.3 Les applications $\hat{f}$ et $\widehat{f^{-1}}$ prennent en argument des ensembles, et renvoient des ensembles. Pour alléger les notations, on s'autorise à écrire $f^{-1}(y)$ pour $f^{-1}(\{y\})$. Il faut être conscient de l'abus de notation que l'on fait en écrivant cela. Il ne faut pas confondre $\widehat{f^{-1}}$ avec la fonction réciproque f^{-1}, qui n'existe que si f est bijective (cf plus bas), et qui est définie de F dans E, et non sur des ensembles.

NOTATION 1.3.4 On note $\mathcal{F}(E, F)$, ou encore F^E l'ensemble des applications de E dans F.

DÉFINITION 1.3.5 Soit E et F deux ensembles, et soit $E' \subset E$ et $F' \subset F$.

1. Soit $f : E \longrightarrow F$ et $g : E' \longrightarrow F$. Si pour tout $x \in E'$, $f(x) = g(x)$ (*i.e.* f et g coincident sur E', on dit que g est la restriction de f à E' (une telle restriction est unique), et on la note $g = f\,|_{E'}$. On dit que f est un prolongement de G (non unique !)
2. soit $f : E \longrightarrow F$ et $g : E \longrightarrow F'$. Si pour tout $x \in E$, $f(x) = g(x)$, alors on dit que g est la corestriction de f à F'. Si elle existe, la corestriction est unique. Elle existe si et seulement si $\mathrm{Im}(f) \subset F'$.

DÉFINITION 1.3.6 Soit $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications. La composée de f et g est la fonction $g \circ f : E \longrightarrow G$ définie pour tout $x \in E$ par $g \circ f(x) = g(f(x))$.

EXEMPLES 1.3.7

1. Application identique (identité)
2. Soit $E \subset F$. L'injection canonique $i : E \to F$.
3. Soit $E \subset F$. La fonction caractéristique de E dans F, $\chi : F \to \{0, 1\}$.
4. La projection canonique $p_E : E \times F \to E$.

1.3.1 Injectivité, surjectivité, bijectivité

DÉFINITION 1.3.8 Une application $f : E \longrightarrow F$ est dite *injective* si une des propositions équivalentes suivantes est vérifiée :

1. tout élément de F admet au plus un antécédent par f ;
2. $\forall y \in F,\ \mathrm{Card}(f^{-1}(y)) \leqslant 1$,
3. $\forall (x, y) \in E^2,\ x \neq y \Longrightarrow f(x) \neq f(y)$,
4. $\forall (x, y) \in E^2,\ f(x) = f(y) \Longrightarrow x = y$.

DÉFINITION 1.3.9 Une application $f : E \longrightarrow F$ est dite *surjective* si une des propositions équivalentes suivantes est vérifiée :

1. tout élément de F admet au moins un antécédent par f ;
2. $\forall y \in F,\ \mathrm{Card}(f^{-1}(y)) \geqslant 1$;
3. $\forall y \in F,\ \exists x \in E,\ f(x) = y$;
4. $\mathrm{Im}(f) = F$.

DÉFINITION 1.3.10 Une application $f : E \longrightarrow F$ est dite *bijective* si elle est à la fois injective et surjective.

EXEMPLES 1.3.11

1. Soit $E \subset F$. L'injection $i : E \to F$ est injective !

2. Soit E et F deux ensembles, $F \neq \varnothing$. La projection $p_E : E \times F \to E$ est surjective.
3. La fonction identité $E \to E$ est bijective.
4. La fonction caractéristique χ_E est surjective si et seulement si $E \neq \varnothing$ et $E \neq F$.

TERMINOLOGIE 1.3.12 Une bijection de E dans lui-même est appelée *permutation* de E. On note $\mathfrak{S}E$ l'ensemble des permutations de E. Si $E = \{1, \ldots, n\}$, on note $\mathfrak{S}_n$ au lieu de $\mathfrak{S}E$. L'ensemble $\mathfrak{S}_n$ est appelé *n-ième groupe symétrique.*

PROPOSITION 1.3.13 *Soit $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications. Alors :*

1. *si f et g sont injective, alors $g \circ f$ aussi ;*
2. *si f et g sont surjectives, alors $g \circ f$ aussi ;*
3. *si f et g sont bijectives, alors $g \circ f$ aussi ;*

PROPOSITION 1.3.14 *Soit $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications. Alors :*

1. *Si $g \circ f$ est injectif, f est injectif ;*
2. *Si $g \circ f$ est surjectif, g est surjective ;*

THÉORÈME 1.3.15 *Soit $f : E \longrightarrow F$ une application. Alors f est bijective si et seulement s'il existe une application $g : F \to E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$. La fonction g est appelée réciproque de f, et notée f^{-1}. À ne pas confondre avec l'application image réciproque !*

REMARQUE 1.3.16 La réciproque du théorème est une application immédiate de la proposition précédente. Si une telle application g existe, comme id_F (donc $g \circ f$) est surjective, g est surjective ; comme id_G (donc $f \circ g$)) est injective, f est injective.

1.3.2 Familles

DÉFINITION 1.3.17 Soit E et I deux ensembles. Une famille d'éléments de E indexée par I est une application $I \longrightarrow E$. On utilise généralement une notation indicielle plutôt que fonctionnelle : $(a_i)_{i \in I}$ plutôt que $i \mapsto a(i)$.

REMARQUE 1.3.18 Ne pas confondre $(a_i)_{i \in I}$ qui désigne la fonction a, et a_i qui désigne l'image de i par a (même distinction qu'entre f et $f(x)$: attention à la rédaction).

EXEMPLE 1.3.19 Une suite $(u_n)_{n \in \mathbb{N}}$ est une famille indexée par $\mathbb{N}$.

DÉFINITION 1.3.20 Une *sous-famille* de $(a_i)_{i \in I}$ est une famille $(a_i)_{i \in J}$, où $J \subset I$.

À mettre en rapport avec la notion de suite extraite, dans le cas où $I = \mathbb{N}$:

DÉFINITION 1.3.21 Soit $(u_n)_{n \in \mathbb{N}}$ et $(v_n)_{n \in \mathbb{N}}$ deux suites. On dit que $(v_n)_{n \in \mathbb{N}}$ est une *suite extraite* de $(u_n)_{n \in \mathbb{N}}$ s'il existe une application strictement croissante $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ telle que pour tout $n \in \mathbb{N}$, $v_n = u_{\varphi(n)}$.

On dit qu'une famille $(a_i)_{i \in I}$ est finie si I est un ensemble fini.

Constructions dans le cas de familles finies

- Familles de réels ou de complexes : $\sum_{i\in I} a_i$, $\prod_{i\in I} a_i$.
- Familles d'ensembles : $\bigcap_{i\in I} A_i$, $\bigcup_{i\in I} A_i$, $\prod_{i\in I} A_i$

THÉORÈME 1.3.22

$$\left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in J} B_j\right) = \bigcup_{(i,j)\in I\times J} (A_i \cap B_j); \qquad \left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{j\in J} B_j\right) = \bigcap_{(i,j)\in I\times J} (A_i \cup B_j)$$

THÉORÈME 1.3.23 $\mathcal{F}\left(E, \prod_{i\in I} A_i\right) \cong \prod_{i\in I} \mathcal{F}(E, A_i)$.

REMARQUE 1.3.24 Ces différents objets ne sont pas toujours bien définis lorsque I n'est pas fini (sommes infinies : voir la notion de série).

1.4 Relations

1.4.1 Relations binaires

DÉFINITION 1.4.1 Une relation binaire entre deux ensembles E et F est un sous-ensemble G de $E \times F$. On dit que $y \in Y$ est en relation avec $x \in E$ si $(x, y) \in G$. On note souvent $x\mathcal{R}y$, ou, pour certains types particuliers de relations, $x \equiv y$, ou $x \sim y$, ou $x \leqslant y$...

DÉFINITION 1.4.2 Soit $\mathcal{R}$ une relation entre E et lui-même (= relation *sur* E). On dit que :
- $\mathcal{R}$ est reflexive si pour tout $x \in E$, $x\mathcal{R}x$;
- $\mathcal{R}$ est symétrique si pour tout $(x, y) \in E^2$, $x\mathcal{R}y \Longrightarrow y\mathcal{R}x$;
- $\mathcal{R}$ est antisymétrique si pour tout $(x, y) \in E^2$, $(x\mathcal{R}y) \wedge (y\mathcal{R}x) \Longrightarrow (x = y)$;
- $\mathcal{R}$ est transitive si pour tout $(x, y, z) \in E^3$, $(x\mathcal{R}y) \wedge (y\mathcal{R}z) \Longrightarrow (x\mathcal{R}z)$.

1.4.2 Relations d'équivalence

DÉFINITION 1.4.3 Une relation d'équivalence sur E est une relation reflexive, symétrique et transitive. On note souvent $x \equiv y$ ou $x \sim y$ pour indiquer que x et y sont en relation.

EXEMPLE 1.4.4
1. Congruences modulo n : $\equiv_{[n]}$;
2. Appartenance à la même part d'une partition ;
3. La relation définissant $\mathbb{Q}$ sur $\mathbb{Z} \times \mathbb{N}^*$: $(p, q) \equiv_{\mathbb{Q}} (p', q')$ si et seulement $pq' = p'q$ (ces deux couples vont définir le même rationnel).
4. Conjugaison dans $\mathfrak{S}_n$

DÉFINITION 1.4.5 Soit $\mathcal{R}$ une relation d'équivalence sur E, et $x \in E$. La *classe d'équivalence de x sous la relation $\mathcal{R}$* est le sous-ensemble C_x de E constitué des éléments en relation avec x :

$$C_x = \{y \in E \mid x\mathcal{R}y\}.$$

THÉORÈME 1.4.6 *Soit E un ensemble, et $\mathcal{R}$ une relation d'équivalence sur E. L'ensemble des classes d'équivalence sous $\mathcal{R}$ forment une partition de E.*

DÉFINITION 1.4.7 L'ensemble des classes sous la relation $\mathcal{R}$ s'appelle *l'ensemble quotient de E par $\mathcal{R}$*, et est noté $E/\mathcal{R}$. C'est un sous-ensemble de $\mathcal{P}(E)$.

EXEMPLE 1.4.8 On définit $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\equiv_{[n]}$. C'est un ensemble à n éléments.

EXEMPLE 1.4.9 On définit $\mathbb{Q}$ comme étant le quotient $(\mathbb{Z} \times \mathbb{N}^*)/\equiv_{\mathbb{Q}}$.

1.4.3 Relations d'ordre

DÉFINITION 1.4.10 Une relation d'ordre sur E est une relation reflexive, antisymétrique et transitive. On note souvent $x \leqslant y$ pour indiquer que y est en relation avec x. Les écritures $x \leqslant y$ et $y \geqslant x$ sont équivalentes. On note $x < y$ pour $(x \leqslant y) \wedge (x \neq y)$.

EXEMPLE 1.4.11

1. sur $\mathbb{N}$, ou sur $\mathbb{R}$: l'ordre habituel ;
2. sur $\mathbb{N}^*$: la relation de divisibilité $x \mid y$;
3. sur $\mathbb{N} \times \cdots \times \mathbb{N}$: l'ordre lexicographique ;
4. sur $\mathcal{P}(E)$: l'inclusion $A \subset B$;
5. etc.

DÉFINITION 1.4.12 Soit $(E, \leqslant)$ un ensemble muni d'une relation d'ordre.

1. Un élément m de E est appelé *plus petit élément de E* (ou *élément minimum*) si : $\forall m' \in E,\ m \leqslant m'$.
2. Un élément M de E est appelé *plus grand élément de E* (ou *élément maximum*) si : $\forall m' \in E,\ M \geqslant m'$.

PROPOSITION 1.4.13 *S'il existe, le plus petit élément de E est unique. De même pour le plus grand élément.*

DÉFINITION 1.4.14 Soit $(E, \leqslant)$ un ensemble muni d'une relation d'ordre. Soit $A \subset E$.

1. Un minorant m de A est un élément $m \in E$ tel que : $\forall a \in A,\ a \geqslant m$
2. Un majorant M de A est un élément $M \in E$ tel que : $\forall a \in A,\ a \leqslant M$

DÉFINITION 1.4.15 Soit $(E, \leqslant)$, et soit $A \subset E$.

1. La borne inférieure de A dans E, notée $\inf_{x \in A}{}_E\, x$ ou $\inf_{x \in A} x$ ou $\inf A$ est le plus grand des minorants de A, **s'il existe**.
2. La borne supérieure de A dans E, notée $\sup_{x \in A}{}_E\, x$ ou $\sup_{x \in A} x$ ou $\sup A$ est le plus petit des majorants de A, **s'il existe**.

EXEMPLE 1.4.16 **Propriété fondamentale de** $\mathbb{R}$: Tout sous-ensemble non vide majoré de $\mathbb{R}$ admet une borne supérieure. Cette propriété soit doit être prise comme axiome pour la construction de $\mathbb{R}$, soit découle immédiatement d'axiomes équivalents (il y a plusieurs façons équivalentes de construire $\mathbb{R}$, en imposant dans le cahier des charges des propriétés différentes)

REMARQUE 1.4.17 Attention à l'ensemble dans lequel on considère la borne supérieure.

THÉORÈME 1.4.18 *(Caractérisation de la borne supérieure) Pour que b soit la borne supérieure de A dans E, il faut et il suffit que :*

1. $\forall a \in A,\ a \leqslant b$ *(* i.e. *b est un majorant de A) ;*
2. $\forall c \in E,\ c < b \Longrightarrow (\exists a \in A,\ a > c)$ *(* i.e. *b est le plus petit des majorants)*

Énoncé similaire pour la borne inférieure.

Dans $\mathbb{R}$, on exprime souvent la deuxième condition sous la forme suivante :

$$\forall \varepsilon > 0,\ \exists x \in A,\ b - \varepsilon < x \leqslant b.$$

PROPOSITION 1.4.19 *Soit $(E, \leqslant)$, et $A \subset E$. A admet un maximum M (plus grand élément) si et seulement si A admet une borne supérieure b et si $b \in A$. Dans ce cas $M = b$. Énoncé similaire pour le minimum.*

EXEMPLE 1.4.20 **Propriété fondamentale de $\mathbb{N}$:** Toute partie non vide de $\mathbb{N}$ admet minimum. Toute partie non vide majorée de $\mathbb{N}$ admet un maximum.
Le principe de récurrence est une conséquence de la propriété fondamentale de $\mathbb{N}$.

Chapitre 2

Polynômes et nombres complexes

Le but de ce chapitre est d'étudier les fonctions polynomiales $x \mapsto a_d x^d + \cdots + a_1 x + a_0$. On s'interesse notamment aux propriétés arithmétiques (produit, somme, divisibilité...) et aux propriétés analytiques (racines, dérivation...)
On se placera dans un cadre plus formel dans le but notamment de généraliser des constructions *a priori* uniquement valables pour des polynômes à coefficients réels (comme la dérivation) à des polynômes à coefficients complexes.
Nous étudions dans un premier temps uniquement les polynômes à coefficients réels. En effet, nous motivons l'introduction des nombres complexes par l'étude des racines des polynômes à coefficients dans $\mathbb{R}$. Après une étude sommaire des nombres complexes et de leur application à la trigonométrie, on précise les spécificités des polynômes à coefficients complexes, sachant que toutes les règles énoncées dans la première partie sur les polynômes réels sont aussi vraies pour les polynômes à coefficients complexes.

2.1 Polynômes à coefficients réels

Toute cette section se généralise sans problème aux polynômes à coefficients complexes.

2.1.1 Polynômes formels, opérations arithmétiques

Remarque 2.1.1 Une fonction polynomiale est entièrement déterminée par la suite de ses coefficients. Les différentes constructions telles la somme, le produit, la dérivation, peuvent s'écrire uniquement sur les coefficients. Cela motive la définition suivante.

Définition 2.1.2 Un polynôme formel P à coefficients dans $\mathbb{R}$ est une suite de réels $(a_n)_{n\in\mathbb{N}}$, nulle à partir d'un certain rang.
Le réel a_k est appelé k-ième coefficient de P, ou coefficient du monôme de degré k de P.
L'ensemble des polynômes (formels) à coefficients réels est noté $\mathbb{R}[X]$.

Opérations arithmétiques

Définition 2.1.3 La *somme* de deux polynômes $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ est la suite $P+Q = (a_n + b_n)_{n\in\mathbb{N}}$, qui est nulle bien à partir d'un certain rang.

Définition 2.1.4 Le produit de $P = (a_n)_{n\in\mathbb{N}}$ par le scalaire $\lambda \in \mathbb{R}$ est $\lambda P = (\lambda a_n)_{n\in\mathbb{N}}$.

DÉFINITION 2.1.5 Soit $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes. Soit pour tout $n \in \mathbb{N}$, $c_n = \sum_{k=0}^{n} a_k b_{n-k}$. Alors $(c_n)_{n\in\mathbb{N}}$ est un polynôme. On définit alors $PQ = (c_n)_{n\in\mathbb{N}}$.

PROPOSITION 2.1.6 *Soit P, Q, R trois polynômes. Alors $P(Q+R) = PQ + RQ$.*

DÉFINITION 2.1.7 On définit le polynôme $X = (0, 1, 0, 0, \ldots)$.

PROPOSITION 2.1.8 *Pour tout $n \in \mathbb{N}$, on a $X^n = (0, \ldots, 0, 1, 0, \ldots)$, le 1 étant au rang n.*

COROLLAIRE 2.1.9 *Soit $P = (a_n)_{n\in\mathbb{N}}$ un polynôme. Alors $P = \sum_{k=0}^{+\infty} a_k X^k$, cette somme ayant un sens puisqu'elle est en fait finie, les a_k étant nuls à partir d'un certain rang.*

On adopte désormais cette notation.

2.1.2 Dérivation

DÉFINITION 2.1.10 Soit $P = \sum_{k=0}^{d} a_k X^k$ un polynôme. Le *polynôme dérivé* est :
$P' = \sum_{k=1}^{d} k a_k X^{k-1}$.

PROPOSITION 2.1.11 *Soit P, Q deux polynômes, λ un réel.*

1. $(P+Q)' = P' + Q'$.
2. $(\lambda P)' = \lambda P'$.

PROPOSITION 2.1.12

1. *Soit P et Q deux polynômes. Alors $(PQ)' = P'Q + PQ'$.*
2. *Soit $P_1, \ldots, P_n$ des polynômes. Alors $(P_1 \cdots P_n)' = \sum_{i=1}^{n} P_1 \cdots P_{i-1} P_i' P_{i+1} \cdots P_n$.*
3. *(Formule de Leibniz) Soit P et Q deux polynômes. Alors $P^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.*

REMARQUE 2.1.13 Ces propriétés sont obtenues de manière entièrement formelle, et sans aucune utilisation de la définition analytique de la dérivation. Ainsi, elles sont vraies aussi pour les polynômes à coefficients complexes.

2.1.3 Degré et valuation

DÉFINITION 2.1.14 Soit $P = (a_n)_{n\in\mathbb{N}}$ un polynôme.

1. Le *degré de P* est $\deg(P) = \max\{n \in \mathbb{N} \mid a_n \neq 0\}$.
   Si P est non nul, cet ensemble est non vide, et majoré. Ainsi, $\deg(P) \in \mathbb{N}$.
   Si $P = 0$, par convention, $\deg(P) = -\infty$.
2. La *valuation de P* est $\mathrm{val}(P) = \min\{n \in \mathbb{N} \mid a_n \neq 0\}$.
   Si P est non nul, cet ensemble est non vide, et minoré. Ainsi, $\mathrm{val}(P) \in \mathbb{N}$.
   Si $P = 0$, par convention, $\mathrm{val}(P) = +\infty$.

PROPOSITION 2.1.15 *Soit P et Q deux polynômes de $\mathbb{R}[X]$. Alors :*

1. $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$.
   Si $\deg P \neq \deg Q$, *alors* $\deg(P+Q) = \max(\deg P, \deg Q)$.
2. *Si* $\lambda \neq 0$, $\deg \lambda P = \deg P$.
3. *Si* P *et* Q *sont non nuls,* $\deg(PQ) = \deg P + \deg Q$.
4. *Si* $\deg P > 0$ *(* i.e. *P n'est pas constant), alors* $\deg P' = \deg P - 1$.

Proposition 2.1.16 *Soit P et Q deux polynômes de $\mathbb{R}[X]$. Alors :*

1. $\mathrm{val}(P+Q) \geqslant \min(\deg P, \deg Q)$.
   Si $\mathrm{val}P \neq \mathrm{val}Q$, *alors* $\mathrm{val}(P+Q) = \min(\deg P, \deg Q)$.
2. *Si* $\lambda \neq 0$, $\mathrm{val}\lambda P = \mathrm{val}P$.
3. *Si* P *et* Q *sont non nuls,* $\mathrm{val}(PQ) = \mathrm{val}P + \mathrm{val}Q$.
4. *Si* $\mathrm{val}P > 0$, *alors* $\mathrm{val}P' = \mathrm{val}P - 1$.

2.1.4 Évaluation, racines

Soit l'application

$$\begin{array}{rrcl} \varphi : & \mathbb{R}[X] & \longrightarrow & \{\text{fonctions polynomiales de } \mathbb{R} \text{ dans } \mathbb{R}\} \\ & P = \sum_{k=0}^{d} a_k X^k & \longmapsto & \left(\widetilde{P} : x \mapsto \sum_{k=0}^{d} a_k x^k\right). \end{array}$$

Théorème 2.1.17 *L'application φ est une bijection.*

Remarque 2.1.18 Ce n'est pas le cas pour les polynômes à coefficients dans d'autres « corps » que $\mathbb{R}$, par exemple $\mathbb{F}_2 = \{0, 1\}$.

Les définitions des diverses constructions dans $\mathbb{R}[X]$ amènent directement :

Proposition 2.1.19 *Pour tous polynômes P, Q de $\mathbb{R}[X]$, et tout $\lambda \in \mathbb{R}$,*

$$\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}; \qquad \widetilde{PQ} = \widetilde{P} \cdot \widetilde{Q}; \qquad \widetilde{\lambda P} = \lambda \widetilde{P}; \qquad \widetilde{P'} = \widetilde{P}'.$$

Autrement dit, les opérations définies formellement coïncident avec les opérations sur les fonctions polynomiales.

Définition 2.1.20 1. Soit $P \in \mathbb{R}[X]$ et $a \in \mathbb{R}$. L'évaluation de P en a est $\widetilde{P}(a)$. On note souvent simplement $P(a)$ pour $\widetilde{P}(a)$.
2. On dit que $r \in \mathbb{R}$ est *racine* du polynôme P si $P(r) = 0$.

Algorithme de Hörner

Il est basé sur la factorisation : $\sum_{k=0}^{d} a_k x^k = a_0 + x(a_1 + x(a_2 + \cdots + x(a_{d-1} + x a_d)))$.
Ainsi, si les coefficients de P sont stockés dans un tableau `P` (défini comme un type `polynome`), on obtient l'algorithme d'évaluation suivant, qui est linéaire :

```
function evaluation (P:polynome;d:integer; a:real):real;
var k:integer;
    Pa:real;
```

```
begin
  Pa:=P[d];             {initialisation}
  for k:=d-1 downto 0 do
    Pa:=P[k] + x*Pa;
  evaluation:=Pa;
end;
```

2.1.5 Division euclidienne

THÉORÈME 2.1.21 *Soit A et B deux polynômes de $\mathbb{R}[X]$, $B \neq 0$. Alors il existe un unique couple $(Q, R) \in \mathbb{R}[X]^2$ tel que :*

$$A = BQ + R \qquad et \qquad \deg R < \deg B.$$

DÉFINITION 2.1.22 Q est appelé *quotient de la division euclidienne* de A par B ;
R est appelé *reste de la division euclidienne* de A par B.

Algorithme de division euclidienne
Soit d et d' les degrés de A et B. Si $d < d'$, alors $Q = 0$ et $R = A$ conviennent.
Si $d \geqslant d'$, on commence par trouver $\lambda \in \mathbb{R}$ et $\alpha \in \mathbb{N}$ tels que $\deg(A - \lambda X^\alpha) < \deg(A)$. Il suffit de prendre $\lambda = \frac{a}{b}$ et $\alpha = d - d'$, où a et b sont les coefficients dominants de A et B. On recommence ensuite en remplaçant A par $A - \lambda X^\alpha$ jusqu'à obtenir un degré strictement plus petit que celui de B.
On implémente cet algorithme. On suppose qu'on dispose de fonctions effectuant la somme de polynômes et la multiplication par un scalaire, et on se permet de noter ces opérations à l'aide des signes d'opération habituels (ce qui n'est syntaxiquement pas tout à fait correct)

```
procedure DE(A,B:polynome; dA,dB:integer; var Q,R:polynome; dQ,dR:integer);
var k:integer;
begin
  for k:=dA downto dB do
    begin
      Q[k-dB]:= A[k]/B[dB];
      A:=A- (A[k]/B[dB])*B;
    end;
  R:=A;
  dQ:=dA-dB;
  dR:=dB-1;
end;
```

2.1.6 Divisibilité et racines

DÉFINITION 2.1.23 Soit $A, B \in \mathbb{R}[X]$, $B \neq 0$. On dit que B *divise* A (ou A *divisible par* B) s'il existe Q tel que $A = BQ$, autrement dit si le reste de la division euclidienne de A par B est 0.

PROPOSITION 2.1.24 *Si B divise A, alors* $\deg(B) \leqslant \deg(A)$.

THÉORÈME 2.1.25 *Soit $r \in \mathbb{R}$. Alors r est racine de P si et seulement si $X - r$ divise P.*

DÉFINITION 2.1.26 On dit que r est racine d'ordre de multiplicité $k \in \mathbb{N}^*$ si et seulement si $(X-r)^k$ divise P mais pas $(X-r)^{k+1}$. Autrement dit il existe $Q \in \mathbb{R}[X]$ tel que $P=(X-r)^k Q$, avec $Q(r) \neq 0$.

LEMME 2.1.27 *Soit $P \in \mathbb{R}[X]$ et $r \in \mathbb{R}$. Si r est racine d'ordre k de P, alors r est racine d'ordre $k-1$ de P'.*

THÉORÈME 2.1.28 *Soit $P \in \mathbb{R}[X]$ et $r \in \mathbb{R}$. Le réel r est racine d'ordre k de P si et seulement si : $P(r)=P'(r)=\cdots=P^{(k-1)}(r)=0$ et $P^{(k)}(r) \neq 0$.*

LEMME 2.1.29 *Soit r_1 et r_2 deux racines distinctes de P de multiplicité α_1 et α_2. Alors il existe un polynôme Q tel que $P=(X-r_1)^{\alpha_1}Q$, et r_2 est racine de multiplicité α_2 de Q.*

THÉORÈME 2.1.30 *Soit $P \in \mathbb{R}[X]$, et $r_1,\ldots,r_k$ des racines deux à deux distinctes de P, de multiplicités respectives $\alpha_1,\ldots,\alpha_k$. Alors $(X-r_1)^{\alpha_1}\cdots(X-r_k)^{\alpha_k}$ divise P.*

COROLLAIRE 2.1.31 *Soit $P \in \mathbb{R}[X]$ de degré n. Alors P admet au plus n racines (comptées avec multiplicité).*

COROLLAIRE 2.1.32 *Soit P un polynôme de degré au plus n. Alors, si P admet strictement plus de n racines, $P=0$.*

2.2 Nombres complexes

2.2.1 De l'existence des racines d'un polynôme

$\mathbb{C}$ est défini comme le plus petit ensemble contenant $\mathbb{R}$, muni d'une addition et d'une multiplication ayant les mêmes propriétés que celles de $\mathbb{R}$ (c'est ce qu'on appelle un sur-corps) et dans lequel tout polynôme non constant admet une racine. On dit que $\mathbb{C}$ est la *clôture algébrique de* $\mathbb{R}$. La propriété fondamentale de $\mathbb{C}$ est donc :

THÉORÈME 2.2.1 *(d'Alembert-Gauss) Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine.*

COROLLAIRE 2.2.2 *Tout polynôme de $\mathbb{C}[X]$ de degré n admet exactement n racines, comptées avec multiplicité.*

DÉFINITION 2.2.3 On dit que $P \in \mathbb{K}[X]$ est scindé ($\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$) s'il existe des complexes (non forcément deux à deux distints) λ et $r_1,\ldots,r_n$ tels que : $P=\lambda(X-r_1)\cdots(X-r_n)$.

COROLLAIRE 2.2.4 *Tout polynôme de $\mathbb{C}[X]$ est scindé.*

DÉFINITION 2.2.5 On définit i comme une racine du polynôme X^2+1. Une telle racine existe d'après le théorème de d'Alembert-Gauss.

THÉORÈME 2.2.6 *(admis) L'application de $\mathbb{R}^2$ dans $\mathbb{C}$ définie par $(x,y)\mapsto x+\mathrm{i}\,y$ est une bijection.*

2.2.2 Propriétés arithmétiques des nombres complexes

PROPRIÉTÉ 2.2.7 *Soit $z, z' \in \mathbb{C}$, $z = a + \mathrm{i}\, b$ et $z' = a' + \mathrm{i}\, b'$. Alors :*

1. $z + z' = (a + a') + \mathrm{i}(b + b')$ *;*
2. $zz' = (aa' - bb') + \mathrm{i}(ab' + a'b)$ *;*
3. *Si $(a, b) \neq 0$, alors z et inversible, et $z^{-1} = \frac{a - \mathrm{i}\, b}{a^2 + b^2}$.*

DÉFINITION 2.2.8 Soit $z = a + \mathrm{i}\, b$ un nombre complexe. On définit :

1. le conjugué de z par $\overline{z} = a - \mathrm{i}\, b$;
2. le module de z par $|z| = \sqrt{a^2 + b^2}$.

PROPRIÉTÉ 2.2.9 *Soit z et z' deux nombres complexes. Alors :*

1. $\overline{\overline{z}} = z$ *;*
2. $z = \overline{z} \Longleftrightarrow z \in \mathbb{R}$ *;*
3. $z = -\overline{z} \Longleftrightarrow z$ *imaginaire pur ;*
4. $\mathrm{Re}(z) = \frac{z + \overline{z}}{2}$ *et* $\mathrm{Im}(z) = \frac{z - \overline{z}}{2\,\mathrm{i}}$ *;*
5. $\overline{z + z'} = \overline{z} + \overline{z'}$ *et* $\overline{zz'} = \overline{z} \cdot \overline{z'}$ *;*
6. $|z|^2 = z \cdot \overline{z}$.

PROPRIÉTÉ 2.2.10 *Soit z et z' deux nombres complexes. Alors :*

1. $z = 0 \Longleftrightarrow |z| = 0$ *;*
2. $|zz'| = |z| \cdot |z'|$ *et* $\left|\frac{z}{z'}\right| = \frac{|z|}{|z'|}$ *;*
3. $|\mathrm{Re} z| \leqslant |z|$ *et* $|\mathrm{Im}\, z| \leqslant |z|$ *;*
4. $|z + z'| \leqslant |z| + |z'|$ *(inégalité triangulaire).*

2.2.3 Rappel : formules trigonométriques

Nous rappelons ici les principales formules trigonométriques. Soit a, b, p, q, θ des réels :

$\cos^2 a + \sin^2 a = 1$

$\sin(a+b) = \sin a \cos b + \sin b \cos a$
$\sin(a-b) = \sin a \cos b - \sin b \cos a$
$\cos(a+b) = \cos a \cos b - \sin a \sin b$
$\cos(a-b) = \cos a \cos b + \sin a \sin b$
$\tan(a+b) = \frac{\tan a + \tan b}{1 - \tan a \tan b}$
$\tan(a-b) = \frac{\tan a - \tan b}{1 + \tan a \tan b}$

$\sin 2a = 2 \sin a \cos a$
$\cos 2a = \cos^2 a - \sin^2 a = 1 - 2\sin^2 a = 2\cos^2 a - 1.$
$\tan 2a = \frac{2 \tan a}{1 - \tan^2 a}$

$\cos^2 a = \dfrac{1 + \cos 2a}{2}$
$\sin^2 a = \dfrac{1 - \cos 2a}{2}$

$\sin a \sin b = \frac{1}{2}[\cos(a-b) - \cos(a+b)]$
$\cos a \cos b = \frac{1}{2}[\cos(a-b) + \cos(a+b)]$
$\sin a \cos b = \frac{1}{2}[\sin(a+b) + \sin(a-b)]$

$\sin p + \sin q = 2 \sin \frac{p+q}{2} \cos \frac{p-q}{2}$
$\sin p - \sin q = 2 \cos \frac{p+q}{2} \sin \frac{p-q}{2}$
$\cos p + \cos q = 2 \cos \frac{p+q}{2} \cos \frac{p-q}{2}$
$\cos p - \cos q = -2 \sin \frac{p+q}{2} \sin \frac{p-q}{2}$

$\cos\theta = \frac{1-t^2}{1+t^2}$, où $t = \tan\frac{\theta}{2}$
$\sin\theta = \frac{2t}{1+t^2}$
$\tan\theta = \frac{2t}{1-t^2}$.

2.2.4 L'exponentielle complexe

DÉFINITION 2.2.11 On définit l'exponentielle complexe pour tout $\theta \in \mathbb{R}$ par :

$$\mathrm{e}^{\mathrm{i}\,\theta} = \cos\theta + \mathrm{i}\sin\theta.$$

LEMME 2.2.12 *Soit a et b deux réels tels que $a^2 + b^2 = 1$. Alors il existe un unique $\theta \in [0, 2\pi[$ tel que $a = \cos\theta$ et $b = \sin\theta$.*

PROPOSITION 2.2.13 *Soit $z \in \mathbb{C}^*$. Il existe un unique réel strictement positif $r \in \mathbb{R}_+^*$ et un unique $\theta \in [0, 2\pi[$ tel que $z = r\mathrm{e}^{\mathrm{i}\,\theta}$.*
Le reél r est le module de z, et θ est appelé argument principal *de z.*

THÉORÈME 2.2.14 *Pour tout $(\theta, \theta') \in \mathbb{R}^2$, $\mathrm{e}^{\mathrm{i}(\theta+\theta')} = \mathrm{e}^{\mathrm{i}\,\theta}\mathrm{e}^{\mathrm{i}\,\theta'}$.*

COROLLAIRE 2.2.15 *(Formule de Moivre) Pour tout $\theta \in \mathbb{R}$ et $n \in \mathbb{N}$:*

$$\mathrm{e}^{\mathrm{i}\,n\theta} = (\mathrm{e}^{\mathrm{i}\,\theta})^n \qquad \textit{soit:} \qquad \cos(n\theta) + \mathrm{i}\sin(n\theta) = (\cos\theta + \mathrm{i}\sin\theta)^n.$$

COROLLAIRE 2.2.16 *Soit $z = r\mathrm{e}^{\mathrm{i}\,\theta}$. Alors $\overline{z} = r\mathrm{e}^{-\mathrm{i}\,\theta}$.*

THÉORÈME 2.2.17 *(admis provisoirement) Soit $x \in \mathbb{R}$. Alors :*

$$\mathrm{e}^{\mathrm{i}\,x} = \sum_{n=0}^{+\infty} \frac{(\mathrm{i}\,x)^n}{n!} = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!} + \mathrm{i}\sum_{n=0}^{+\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}.$$

COROLLAIRE 2.2.18 *On en déduit les développements de* cos *et* sin *:*

$$\forall x \in \mathbb{R}, \quad \cos x = \sum_{n=0}^{+\infty} \frac{(-1)^n x^{2n}}{(2n)!} \qquad et \qquad \sin x = \sum_{n=0}^{+\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}.$$

2.2.5 Racines de l'unité, racines d'un complexe

DÉFINITION 2.2.19 Soit $n \in \mathbb{N}^*$ et $z \in \mathbb{C}$. Une racine n-ième de z est une racine (complexe) du polynôme $X^n - z$.
Une racine n-ième de l'unité est une racine n-ième de 1.

Soit $P = X^n - z$. Puisque la seule racine de P' est 0, les racines de P sont simples, et d'après le théorème de d'Alembert-Gauss, on obtient :

PROPOSITION 2.2.20 *Tout nombre complexe z admet exactement n racines n-ièmes deux à deux distinctes.*

PROPOSITION 2.2.21 *Les racines n-ièmes de l'unité sont $\{\omega_0, \dots, \omega_{n-1}\}$ où :*

$$\forall k \in [\![0, n-1]\!], \quad \omega_k = \mathrm{e}^{\mathrm{i}\,\frac{2\pi k}{n}}.$$

PROPOSITION 2.2.22 *Soit z un nombre complexe et z_0 une racine n-ième particulière de z. Alors les n racines n-ièmes de z sont les nombres complexes $z_0\omega_k$, $k \in [\![0, n-1]\!]$.*

Si $z = r\mathrm{e}^{\mathrm{i}\,\theta}$, $r \in \mathbb{R}_+^*$, $\theta \in \mathbb{R}$, une racine n-ième particulière est par exemple : $z_0 = \sqrt[n]{r} \cdot \mathrm{e}^{\mathrm{i}\,\frac{\theta}{n}}$.

PROPOSITION 2.2.23 *Soit $k \in [\![1, n-1]\!]$. Alors $\sum\limits_{i=0}^{n-1} \omega_k^i = 0$.*

En particulier, puisque pour tout $k \in [\![0, n]\!]$, $\omega_k = \omega_1^k$, on obtient :

COROLLAIRE 2.2.24 $\sum\limits_{k=0}^{n-1} \omega_k = 0$.

2.3 Application à la trigonométrie

2.3.1 Formule d'Euler, formules trigonométriques

De la définition des exponentielles complexes, on déduit immédiatement les formules d'Euler :

PROPOSITION 2.3.1 *Pour tout $\theta \in \mathbb{R}$, $\cos\theta = \dfrac{\mathrm{e}^{\mathrm{i}\,\theta} + \mathrm{e}^{-\mathrm{i}\,\theta}}{2}$ et $\sin\theta = \dfrac{\mathrm{e}^{\mathrm{i}\,\theta} - \mathrm{e}^{-\mathrm{i}\,\theta}}{2\,\mathrm{i}}$.*

Ces formules permettent de passer d'un cosinus ou sinus à une exponentielle, donc à une objet géométrique, pour lequel les calculs sont plus aisés.
Elles permettent par exemple de retrouver certaines formules trigonométriques, par exemple $\cos a \cos b = \frac{1}{2}(\cos(a+b) + \cos(a-b))$.

2.3.2 Symétrisation d'une somme de complexes de même module

Pour mettre sous forme trigonométrique une somme de deux nombres complexes de même module donnés sous forme trigonométrique (et donc pour déterminer ensuite les parties réelles et imaginaires), on a tout intérêt à utiliser le principe de symétrisation des arguments. Par exemple :

$$r\mathrm{e}^{\mathrm{i}\,a} + r\mathrm{e}^{\mathrm{i}\,b} = r(\mathrm{e}^{\mathrm{i}\,a} + \mathrm{e}^{\mathrm{i}\,b}) = r\mathrm{e}^{\mathrm{i}\,\frac{a+b}{2}}\left(\mathrm{e}^{\mathrm{i}\,\frac{a-b}{2}} + \mathrm{e}^{-\mathrm{i}\,\frac{a-b}{2}}\right) = 2r\mathrm{e}^{\mathrm{i}\,\frac{a+b}{2}}\cos\frac{a-b}{2}.$$

Ainsi, $\mathrm{Re}(r\mathrm{e}^{\mathrm{i}\,a} + r\mathrm{e}^{\mathrm{i}\,b}) = 2r\cos\frac{a+b}{2}\cos\frac{a-b}{2}$, et $\mathrm{Im}(r\mathrm{e}^{\mathrm{i}\,a} + r\mathrm{e}^{\mathrm{i}\,b}) = 2r\sin\frac{a+b}{2}\cos\frac{a-b}{2}$.
On a donc tout intérêt à utiliser cette symétrisation plutôt que de se lancer dans des calculs utilisant des fomules trigonométriques. Par exemple :

$$1 + \cos\theta + \mathrm{i}\sin\theta = 1 + \mathrm{e}^{\mathrm{i}\,\theta} = \mathrm{e}^{\mathrm{i}\,\frac{\theta}{2}}(\mathrm{e}^{-\mathrm{i}\,\frac{\theta}{2}} + \mathrm{e}^{\mathrm{i}\,\frac{\theta}{2}}) = 2\cos\frac{\theta}{2}\cdot\mathrm{e}^{\mathrm{i}\,\frac{\theta}{2}}.$$

2.3.3 Linéarisation ; polynômes de Tchebychev

On s'intéresse ici à la façon d'exprimer $\cos^n\theta$ ou $\sin^n\theta$ en fonction de $\cos(k\theta)$ et $\sin(k\theta)$, $k \in \mathbb{N}$ (linéarisation), et inversement.
On s'occupe dans un premier temps de la linéarisation. Le principe général consiste à utiliser la formule de Moivre et la formule du binôme. Nous présentons ce calcul sur deux exemples. Soit $\theta \in \mathbb{R}$.

$$\begin{aligned}
\cos^4\theta = \left(\frac{\mathrm{e}^{\mathrm{i}\,\theta} + \mathrm{e}^{-\mathrm{i}\,\theta}}{2}\right)^4 &= \frac{1}{2^4}\left(\mathrm{e}^{\mathrm{i}\,4\theta} + 4\mathrm{e}^{\mathrm{i}\,2\theta} + 6 + 4\mathrm{e}^{\mathrm{i}\,-2\theta} + \mathrm{e}^{-\mathrm{i}\,4\theta}\right)\\
&= \frac{1}{2^4}\left((\mathrm{e}^{\mathrm{i}\,4\theta} + \mathrm{e}^{-\mathrm{i}\,4\theta}) + 4(\mathrm{e}^{\mathrm{i}\,2\theta} + \mathrm{e}^{-\mathrm{i}\,2\theta}) + 6\right)\\
&= \frac{\cos(4\theta)}{8} + \frac{\cos(2\theta)}{2} + \frac{3}{8}.
\end{aligned}$$

Pour le deuxième exemple, on linéarise $\sin^5\theta$:

$$\begin{aligned}
\sin^5\theta = \left(\frac{\mathrm{e}^{\mathrm{i}\,\theta} - \mathrm{e}^{-\mathrm{i}\,\theta}}{2\,\mathrm{i}}\right)^5 &= \frac{1}{2^5\,\mathrm{i}}\left(\mathrm{e}^{\mathrm{i}\,5\theta} - 5\mathrm{e}^{\mathrm{i}\,3\theta} + 10\mathrm{e}^{\mathrm{i}\,\theta} - 10\mathrm{e}^{-\mathrm{i}\,\theta} + 5\mathrm{e}^{-\mathrm{i}\,3\theta} + \mathrm{e}^{-\mathrm{i}\,5\theta}\right)\\
&= \frac{1}{2^5\,\mathrm{i}}\left((\mathrm{e}^{\mathrm{i}\,5\theta} - \mathrm{e}^{-\mathrm{i}\,5\theta}) - 5(\mathrm{e}^{\mathrm{i}\,3\theta} - \mathrm{e}^{-\mathrm{i}\,2\theta}) + 10(\mathrm{e}^{\mathrm{i}\,\theta} - \mathrm{e}^{-\mathrm{i}\,\theta})\right)\\
&= \frac{1}{2^4}\left(\sin(5\theta) - 5\sin(3\theta) + 10\sin\theta\right)
\end{aligned}$$

Inversement, on peut exprimer $\cos(n\theta)$ en un polynôme en $\cos\theta$ (polynôme de Tchebychev, cf DM), et de même pour $\sin(n\theta)$. On va donner en exemple le cas de $\cos(5\theta)$ et $\sin(5\theta)$, pour illustrer la méthode. On utilise la formule de Moivre et la formule du binôme :

$$\begin{aligned}
&\cos(5\theta) + \mathrm{i}\sin(5\theta) = (\cos\theta + \mathrm{i}\sin\theta)^5\\
&\qquad = \cos^5\theta + 5\,\mathrm{i}\cos^4\theta\sin\theta - 10\cos^3\theta\sin^2\theta - 10\,\mathrm{i}\cos^2\theta\sin^3\theta + 5\cos\theta\sin^4\theta + \mathrm{i}\sin^5\theta\\
&\qquad = \cos^5\theta - 10\cos^3\theta\sin^2\theta + 5\cos\theta\sin^4\theta + \mathrm{i}(5\cos^4\theta\sin\theta - 10\cos^2\theta\sin^3\theta + \sin^5\theta)
\end{aligned}$$

Ainsi :

$$\begin{aligned}
\cos(5\theta) &= \cos^5\theta - 10\cos^3\theta\sin^2\theta + 5\cos\theta\sin^4\theta\\
&= \cos^5\theta - 10\cos^3\theta(1 - \cos^2\theta) + 5\cos\theta(1 - \cos^2\theta)^2\\
&= 16\cos^5\theta - 20\cos^3\theta + 5\cos\theta,
\end{aligned}$$

et une expression similaire pour $\sin(5\theta)$, soit en un polynôme en $\sin(\theta)$, soit en un produit de $\sin\theta$ et d'un polynôme en $\cos(\theta)$.

2.3.4 Calcul de sommes de cosinus ou de sinus

Pour calculer des sommes de cosinus ou sinus, on a tout intérêt à introduire des exponentielles complexes, c'est-à-dire à voir $\cos a$ comme la partie réelle de $\mathrm{e}^{\mathrm{i}\,a}$. Par exemple, soit a et b deux réels, et soit :

$$C = \cos a + \cos(a+b) + \cos(a+2b) + \cdots + \cos(a+nb) = \sum_{k=0}^{n} \cos(a+kb).$$

Alors :

$$\begin{aligned}
C &= \mathrm{Re}\left(\sum_{k=0}^{n} \mathrm{e}^{\mathrm{i}(a+kb)}\right) = \mathrm{Re}\left(\mathrm{e}^{\mathrm{i}\,a} \sum_{k=0}^{n} \mathrm{e}^{\mathrm{i}\,kb}\right) \\
&= \mathrm{Re}\left(\mathrm{e}^{\mathrm{i}\,a} \cdot \frac{1-\mathrm{e}^{\mathrm{i}\,b(n+1)}}{1-\mathrm{e}^{\mathrm{i}\,b}}\right) \\
&= \mathrm{Re}\left(\mathrm{e}^{\mathrm{i}\,a}\mathrm{e}^{\mathrm{i}\,\frac{bn}{2}} \cdot \frac{\mathrm{e}^{-\mathrm{i}\,b\frac{n+1}{2}} - \mathrm{e}^{\mathrm{i}\,b\frac{n+1}{2}}}{\mathrm{e}^{-\mathrm{i}\,\frac{b}{2}} - \mathrm{e}^{\mathrm{i}\,\frac{b}{2}}}\right) \\
&= \mathrm{Re}\left(\mathrm{e}^{\mathrm{i}(a+\frac{bn}{2})} \cdot \frac{\sin\left(\frac{n+1}{2}\cdot b\right)}{\sin\frac{b}{2}}\right) = \cos\left(a+\frac{bn}{2}\right) \cdot \frac{\sin\left(\frac{n+1}{2}\cdot b\right)}{\sin\frac{b}{2}}.
\end{aligned}$$

Remarquez qu'on a exploité dans ce calcul le principe de symétrie énoncé plus haut.

2.4 Spécificités des polynômes à coefficients complexes

Les résultats énoncés dans la première partie de ce chapitre pour les polynômes à coefficients réels sont aussi valables pour les polynômes à coefficients complexes. Il est certaines spécificités des polynômes de $\mathbb{C}[X]$ que nous donnons ci-dessous. En application, on trouve certaines propriétés de factorisation des polynômes à coefficients réels.

2.4.1 Autour du théorème de d'Alembert-Gauss

Nous rappelons le résultat essentiel découlant immédiatement de la définition de $\mathbb{C}$:

THÉORÈME 2.4.1 *(d'Alembert-Gauss). Tout polynôme P de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$.*

COROLLAIRE 2.4.2 *Tout polynôme de $\mathbb{C}[X]$ est scindé.*

DÉFINITION 2.4.3 Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On dit que $P \in \mathbb{K}[X]$ est irréductible si et seulement si P n'est pas constant et P n'est divisible par aucun polynôme autre qu'un polynôme constant ou que λP, $\lambda \in \mathbb{C}^*$. Ainsi, P ne se factorise pas non trivialement.

On déduit immédiatement du théorème de d'Alembert-Gauss que :

COROLLAIRE 2.4.4 *Dans $\mathbb{C}[X]$, les seuls polynômes irréductibles sont les polynômes de degré 1, c'est-à-dire $aX+b$, $a \neq 0$.*

2.4.2 Racines complexes des polynômes réels

D'après le théorème de d'Alembert-Gauss, tout polynôme à coefficients réels admet exactement n racines complexes, comptées avec multiplicité.

Proposition 2.4.5 *Soit $P \in \mathbb{R}[X]$. Soit $z \in \mathbb{C}$. Si z est racine de P de multiplicité m, alors $\overline{z}$ est aussi racine de P de multiplicité m.*

Remarquez que cette proposition n'a de pertinence que si $z \notin \mathbb{R}$. Dans le cas contraire, $z = \overline{z}$, et le résultat est évident.

2.4.3 Application aux factorisations dans $\mathbb{R}[X]$

Théorème 2.4.6 *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant négatif. Ainsi, tout polynôme $P \in \mathbb{R}[X]$ peut être factorisé en produit de polynômes de $\mathbb{R}[X]$ de degré 1, ou de degré 2, de discriminant négatif.*

Chapitre 3

Espaces vectoriels

3.1 Notion d'espace vectoriel

3.1.1 Définition

Dans tout ce qui suit, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Définition 3.1.1 Soit E un ensemble. On dit que E est un espace vectoriel sur $\mathbb{K}$ (en abrégé $\mathbb{K}$-ev) si E est muni de deux lois :
- une loi interne $+ \ : \ E \times E \longrightarrow E$ qui à (x, y) associe $x + y$;
- une loi externe $\cdot \ : \ \mathbb{K} \times E \longrightarrow E$ qui à (λ, y) associe $\lambda \cdot y$;

telles que pour tous $\alpha_1, \alpha_2, \lambda, \mu$ dans $\mathbb{K}$, tous x, x_1, x_2, x_3 dans E :

(i) $(x_1 + x_2) + x_3 = x_1 + (x_2 + x_3)$ (associativité de $+$) ;

(ii) il existe un élément neutre $0 = 0_E$ pour $+$, vérifiant : $\forall y \in E, \ 0 + y = y + 0 = y$;

(iii) il existe un opposé $-x$ de x, vérifiant : $x + (-x) = (-x) + x = 0$;

(iv) $x_1 + x_2 = x_2 + x_1$ (commutativité de $+$) ;

(v) $(\lambda\mu)x = \lambda(\mu x)$ (associativité de $\cdot$) ;

(vi) $1 \cdot x = x$ (compatibilité du neutre multiplicatif de $\mathbb{K}$) ;

(vii) $\lambda(x_1 + x_2) = \lambda x_1 + \lambda x_2$ (distributivité de $\cdot$ sur la loi interne) ;

(viii) $(\lambda + \mu)x = \lambda x + \mu x$ (distributivité de $\cdot$ sur la somme de $\mathbb{K}$).

Propriétés 3.1.2 *Soit E un $\mathbb{K}$-ev. Pour tout $x \in E$:*

1. $0 \cdot x = 0$, *c'est-à-dire* $0_{\mathbb{K}} \cdot x = 0_E$;
2. $\lambda \cdot 0_E = 0_E$
3. $(-1) \cdot x = -x$.

Terminologie 3.1.3 • Les éléments de E sont appelés *vecteurs*
- Les éléments de $\mathbb{K}$ sont appelés *scalaires*
- Deux éléments x et y de E sont colinéaires s'il existe $(\lambda, \mu) \in \mathbb{K}^2$ tels que $(\lambda, \mu) \neq (0, 0)$ et $\lambda x + \mu y = 0$.

3.1.2 Un exemple important : espace de fonctions

Proposition 3.1.4 *Soit F un ensemble quelconque. Alors l'ensemble de fonctions $\mathbb{K}^F$ est un espace vectoriel sur $\mathbb{K}$.*

Proposition 3.1.5 *Plus généralement, soit E un espace vectoriel sur $\mathbb{K}$ et F un ensemble quelconque. Alors l'ensemble de fonctions E^F est un espace vectoriel sur $\mathbb{K}$.*

Exemples 3.1.6
1. $\mathbb{K}^{\varnothing} = \{0\}$;
2. $\mathbb{K}^{[\![1,n]\!]} = \mathbb{K}^n$;
3. $\mathbb{K}^{\mathbb{N}}$ l'ensemble des suites à valeurs dans $\mathbb{K}$;
4. $\mathbb{K}_n[X]$ l'espace des polynômes de degré au plus n ;
5. $\mathbb{C} = \mathbb{R}^2$ est un $\mathbb{R}$-ev ;
6. $E_2^{E_1}$ les applications entre deux espaces vectoriels ;

3.1.3 Sous-espaces vectoriels

Définition 3.1.7 Soit E un espace vectoriel sur $\mathbb{K}$. Un sous-ensemble $F \subset E$ de E est un sous-espace vectoriel de E si les lois $+$ et $\cdot$ de E laissent F stables, et induisent une structure d'espace vectoriel sur F.

Théorème 3.1.8 *Un sous-ensemble $F \subset E$ de E est un sev de E si et seulement si F est non vide et :*

$$\forall x, y \in F^2,\ \forall \lambda \in \mathbb{K},\ \lambda x + y \in F$$

(F stable par combinaison linéaire).

Remarque 3.1.9 Si F vérifie les hypothèses ci-dessus, alors, F étant un espace vectoriel, $O \in F$. Réciproquement, si $F \subset E$, $0 \in F$, et F stable par les lois de E, alors puisque $0 \in F$, F est non vide, et F satisfait encore les hypothèses ci-dessus. Ainsi, on peut remplacer l'hypothèse $F \neq \varnothing$ par l'hypothèse $0 \in F$.

Exemples 3.1.10
1. $\mathbb{R}[X]$ espace des polynômes
2. $\mathcal{C}(\mathbb{R}, \mathbb{R})$ ensemble des fonctions continues ;
3. $\mathcal{C}^n(\mathbb{R}, \mathbb{R})$ ensemble des fonctions de classe $\mathcal{C}^n$.

3.2 Constructions

3.2.1 Intersection

Proposition 3.2.1 *Soit E et F deux sev d'un $\mathbb{K}$-ev G. Alors $E \cap F$ est un sev de G.*

En revanche, l'union de deux sev n'est en général pas un sev.

3.2.2 Produit

PROPOSITION 3.2.2 *Soit $E_1, \ldots, E_n$ des espaces vectoriels sur le corps $\mathbb{K}$. Alors le produit cartésien $E_1 \times \cdots \times E_n$ est un espace vectoriel sur $\mathbb{K}$, muni des lois définies par :*
- $\forall \lambda \in \mathbb{K},\ \forall (x_1, \ldots, x_n) \in E_1 \times \cdots \times E_n,\quad \lambda \cdot (x_1, \ldots, x_n) = (\lambda x_1, \cdots, \lambda x_n)$;
- $\forall (x_1, \ldots, x_n), (y_1, \ldots, y_n) \in E_1 \times \cdots \times E_n,\quad (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$.

3.2.3 Somme, somme directe

DÉFINITION 3.2.3 Soit G un $\mathbb{K}$-ev, et E et F deux sev de G. Alors la somme de $E + F$ est le plus petit sous-espace vectoriel de G (au sens de l'inclusion), contenant à la fois F et G

PROPOSITION 3.2.4 *(Peut être pris comme définition) Soit G un $\mathbb{K}$-ev, et E et F deux sev de G. Alors :*

$$E + F = \{x + y \mid x \in E, y \in F\}.$$

Plus généralement, la somme de n sev $E_1, \ldots, E_n$ est :

$$\sum_{i=1}^{n} E_i = E_1 + \cdots + E_n = \{x_1 + \cdots + x_n \mid x_1 \in E_1, \ldots, x_n \in E_n\}.$$

DÉFINITION 3.2.5 Soit E et F deux sev de G. On dit que la somme $E + F$ est *directe*, et on note $E \oplus F$, si $E \cap F = \{0\}$.
Plus généralement, $E_1 + \cdots + E_n$ est directe si $E_1 \oplus E_2$, puis $(E_1 + E_2) \oplus E_3$, etc. On note $\bigoplus_{i=1}^{n} E_i$.

PROPOSITION 3.2.6 *La somme $E_1 + \cdots + E_n$ est directe si et seulement si pour tout $k \in [\![2, n]\!]$,*

$$F_k \cap \sum_{i<k} F_i = \{0\}.$$

PROPOSITION 3.2.7 *La somme $\sum E_i$ de sous-espaces vectoriels de E est directe si et seulement si l'application ci-dessous est injective :*

$$\begin{array}{rccl} \varphi \ : & E_1 \times \cdots \times E_n & \longrightarrow & E \\ & (x_1, \ldots, x_n) & \longmapsto & x_1 + \cdots + x_n. \end{array}$$

DÉFINITION 3.2.8 Soit E un espace vectoriel, et F et G deux sev de E. On dit que F et G sont supplémentaires dans E si $F \oplus G = E$.

THÉORÈME 3.2.9 *(admis) Soit E un espace vectoriel quelconque, et F un sev de E. Alors F admet au moins un supplémentaire G.*

Ce théorème sera démontré plus loin dans le cas où E est de dimension finie (seul cas au programme).

3.3 Familles de vecteurs

3.3.1 Combinaisons linéaires

Dans tout ce qui suit, on a traité le cas de familles quelconques, qu'elles soient finies ou infinies. Le seul cas au programme est le cas de familles finies.

Soit I un ensemble quelconque.

DÉFINITION 3.3.1 Soit $(\lambda_i)_{i\in I}$ une famille de scalaires. On dit que cette famille est constituée de scalaires *presque tous nuls* si seul un nombre fini de ces scalaires est non nul.

On remarquera que dans le seul cas au programme (I fini), toute famille de scalaires $(\lambda_i)_{i\in I}$ vérifie cette propriété, et il est donc inutile de la préciser. Cette observation permet de simplifier la rédaction des théorèmes lorsqu'on se restreint à ce cas.

DÉFINITION 3.3.2 Soit E un espace vectoriel, et $(x_i)_{i\in I}$ une famille de vecteurs de E. Une *combinaison linéaire* des x_i, $i \in I$ est un élément $x \in E$ tel qu'il existe une famille $(l_i)_{i\in I}$ de scalaires presque tous nuls tels que :

$$x = \sum_{i\in I} \lambda_i x_i.$$

On remarquera que, les λ_i étant presque tous nuls, cette somme est toujours finie, donc bien définie.

DÉFINITION 3.3.3 Soit E un espace vectoriel, et $(x_i)_{i\in I}$ une famille de vecteurs de E. L'*espace vectoriel engendré par la famille* $(x_i)_{i\in I}$ est l'ensemble des combinaisons linéaires des x_i, $i \in I$. Il s'agit de manière évidente d'un sev de E. Il est noté $\mathrm{Vect}((x_i)_{i\in I})$

REMARQUE 3.3.4 Si $I = [\![1, n]\!]$, $\mathrm{Vect}(x_1, \dots, x_n) = \mathbb{R}x_1 + \cdots + \mathbb{R}x_n$.

PROPOSITION 3.3.5 *Soit $(x_i)_{i\in I}$ et $(x_j)_{j\in J}$ deux familles (pas nécessairement disjointes). Alors :*

$$\mathrm{Vect}((x_i)_{i\in I\cup J}) = \mathrm{Vect}((x_i)_{i\in I}) + \mathrm{Vect}((x_j)_{i\in J}).$$

3.3.2 Familles libres

DÉFINITION 3.3.6 Une famille $(x_i)_{i\in I}$ de vecteurs de E est *libre* si une des propriétés équivalentes suivantes est vérifiée :

1. Pour toute famille $(\lambda_i)_{i\in I}$ de scalaires presque tous nuls : $\sum\limits_{i\in I} \lambda_i x_i = 0 \Longrightarrow \forall i \in I, \lambda_i = 0$;
2. Pour tout $x \in \mathrm{Vect}((x_i)_{i\in I})$, il existe une *unique* famille $(\lambda_i)_{i\in I}$ de scalaires presque tous nuls tels que $x = \sum\limits_{i\in I} \lambda_i x_i$;
3. (si I est fini, $I = \{1, \dots, n\}$) La somme $\mathbb{R}x_1 \oplus \cdots \oplus \mathbb{R}x_n$ est directe.

Une famille qui n'est pas libre est dite *liée.*

Remarque : une famille contenant 0 ne peut pas être libre.

PROPOSITION 3.3.7 *Toute sous-famille d'une famille libre est libre.*

La proposition suivante permet de ramener l'étude de la liberté des familles infinies à l'étude de la liberté de familles finies. Ce résultat est, si on se réfère au programme, le seul à connaître concernant les familles infinies.

PROPOSITION 3.3.8 *Une famille $(x_i)_{i\in I}$ est libre si et seulement si toutes ses sous-familles finies sont libres. Une famille $(x_i)_{i\in\mathbb{N}}$ est libre si et seulement si pour tout $n \in \mathbb{N}$, la famille $(x_1, \dots, x_n)$ est libre.*

PROPOSITION 3.3.9 *Soit $(x_i)_{i\in I}$ une famille libre de E et x_j ($j \notin I$) un élément de E. Alors, la famille $(x_i)_{i\in I\cup\{j\}}$ (obtenue en ajoutant x_j à la famille libre $(x_i)_{i\in I}$) est libre si et seulement si $x_j \notin \mathrm{Vect}((x_i)_{i\in I})$*

(Démontré dans le cours uniquement pour des familles finies).

PROPOSITION 3.3.10 *Soit $E_1, \dots, E_n$ des sev de E. Alors la somme $E_1 \oplus \cdots \oplus E_n$ est directe si et seulement si tout n-uplet $(x_1, \dots, x_n)$ d'éléments tous non nuls de $E_1 \times \cdots \times E_n$ est une famille libre dans E.*

3.3.3 Familles génératrices

DÉFINITION 3.3.11 Une famille $(x_i)_{i\in I}$ de vecteurs de E est une famille *génératrice* de E si l'une des propriétés équivalentes suivantes est satisfaite :

1. tout $x \in E$ est une combinaison linéaire des x_i, $i \in I$;
2. $\mathrm{Vect}((x_i)_{i\in I}) = E$;
3. (si I est fini, $I = [\![1, n]\!]$) $E = \sum_{i=1}^{n} \mathbb{R}x_i = E$.

3.3.4 Bases

DÉFINITION 3.3.12 Soit $(x_i)_{i\in I}$ une famille de vecteurs d'un ev E. On dit que $(x_i)_{i\in I}$ est une *base* de E si elle est une famille à la fois libre et génératrice de E.

PROPOSITION 3.3.13 *Les propriétés suivantes sont équivalentes :*

1. *La famille $(x_i)_{i\in I}$ est une base de E ;*
2. *La famille $(x_i)_{i\in I}$ est une famille génératrice minimale de E ;*
3. *La famille $(x_i)_{i\in I}$ est une famille libre maximale de E.*

On justifiera le théorème suivant dans le prochain paragraphe :

THÉORÈME 3.3.14 *(théorème de la dimension) Si E admet au moins une base de cardinal fini, alors toutes ses bases sont finies, de même cardinal.*

DÉFINITION 3.3.15 Ce cardinal commun est appelé *dimension de E*, et noté $\dim E$.

3.4 Espaces vectoriels de dimension finie

Dans tout ce paragraphe $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$.

3.4.1 Notion de dimension

DÉFINITION 3.4.1 Un espace vectoriel E sur $\mathbb{K}$ est dit *de dimension finie* s'il existe une famille génératrice de cardinal fini $(x_i)_{i\in I}$ de E. Une famille génératrice finie est souvent appelé *système de générateurs.*

PROPOSITION 3.4.2 *Soit E un espace vectoriel de dimension finie. Alors de toute famille génératrice de E, on peut extraire une famille génératrice finie.*

THÉORÈME 3.4.3 *(Complétion d'une famille libre en une base par ajout de vecteurs d'une famille génératrice donnée). Soit E un espace vectoriel de dimension finie. Soit $L \subset E$ une famille libre de E, et $G \subset E$ une famille génératrice de E. Alors on peut compléter L en une base de E par ajout de vecteurs de G. Autrement dit, il existe une sous-famille $G' \subset G$ telle que $L \cup G$ soit une base de E.*

COROLLAIRE 3.4.4 *Soit E un espace vectoriel de dimension finie. Toute famille libre de E est de cardinal fini. En particulier, toute base est de cardinal fini.*

COROLLAIRE 3.4.5 *Soit E un espace vectoriel de dimension finie.*

1. *De toute partie génératrice de E on peut extraire une base de E.*
2. *E admet au moins une base.*

COROLLAIRE 3.4.6 *(Théorème de la base incomplète) Toute famille libre d'un espace de dimension fini E peut être complétée en une base de E.*

LEMME 3.4.7 *(Théorème d'échange) Soit E un espace vectoriel. Soit F une famille de vecteurs de E, et x et y dans E tels que $x \notin \mathrm{Vect}(F)$ et $x \in \mathrm{Vect}(F\cup\{y\})$. Alors $\mathrm{Vect}(F\cup\{x\}) = \mathrm{Vect}(F\cup\{y\})$.*

THÉORÈME 3.4.8 *(Théorème de la dimension) Soit E un espace vectoriel de dimension finie. Alors toutes les bases de E sont finies et de même cardinal.*

DÉFINITION 3.4.9 Le cardinal commun de toutes les bases de E est appelé *dimension de E*, et est noté $\dim E$. Si E n'est pas de dimension finie, on dira que $\dim E = +\infty$.

3.4.2 Dimension, liberté et rang

DÉFINITION 3.4.10 Soit E un espace vectoriel, $k \in \mathbb{N}^*$, et $(x_1, \ldots, x_k)$ une famille de vecteurs de E. Le *rang* de la famille $(x_1, \ldots, x_k)$ est la dimension de $\mathrm{Vect}(x_1, \ldots, x_k)$ (cet espace est de dimension finie, puisque engendré par une famille finie). On note :

$$\mathrm{rg}(x_1, \ldots, x_k) = \dim \mathrm{Vect}(x_1, \ldots, x_k).$$

PROPOSITION 3.4.11 $\mathrm{rg}(x_1, \ldots, x_k) \leqslant k$, *avec égalité si et seulement si la famille $(x_1, \ldots, x_k)$ est libre.*

PROPOSITION 3.4.12 *Soit E un espace vectoriel de dimension n. Alors :*

1. *toute famille libre de E est de cardinal au plus n ;*
2. *toute famille génératrice de E est de cardinal au moins n.*

COROLLAIRE 3.4.13 *Soit E un espace vectoriel de dimension n. Alors :*

1. *toute famille libre de E de cardinal n est une base de E ;*
2. *toute famille génératrice de E de cardinal n est une base de E.*

COROLLAIRE 3.4.14 *Soit E un espace vectoriel de dimension finie n. Soit $F \subset E$ un sous-espace vectoriel de E. Alors F est de dimension finie, et $\dim F \leqslant \dim E$. On a égalité si et seulement si $F = E$.*

3.4.3 Dimension de sommes

THÉORÈME 3.4.15 *Soit E un espace vectoriel, et F et G des sous-espaces vectoriels de dimension finie de E, en somme directe. Alors $F \oplus G$ est de dimension finie, et :*

$$\dim F \oplus G = \dim F + \dim G.$$

COROLLAIRE 3.4.16 *Soit E un espace vectoriel, et $(E_1, \ldots, E_n)$ une famille de sous-espaces vectoriels de dimension finie de E, en somme directe. Alors $\bigoplus_{i=1}^{n} E_i$ est de dimension finie, et :*

$$\dim \bigoplus_{i=1}^{n} E_i = \sum_{i=1}^{n} \dim E_i.$$

THÉORÈME 3.4.17 *(Existence d'un supplémentaire) Soit E un espace vectoriel de dimension finie, et F un sous-espace vectoriel de E. Alors il existe un supplémentaire S de F dans E, et :*

$$\dim S = \dim E - \dim F.$$

PROPOSITION 3.4.18 *Soit E un espace vectoriel, et F et G deux sous-espaces de dimension finie de E. Alors :*

$$\dim(F + G) = \dim F + \dim G - \dim F \cap G.$$

Chapitre 4

Applications linéaires

4.1 Généralités sur les applications linéaires

4.1.1 Définition et arithmétique des applications linéaires

DÉFINITION 4.1.1 Une application $f : E \to F$ entre deux $\mathbb{K}$-ev est appelée *application $\mathbb{K}$-linéaire*, ou plus simplement *application linéaire* (en abrégé : AL), si :

$$\forall \lambda \in \mathbb{K},\ \forall x \in E,\quad f(\lambda x) = \lambda f(x) \qquad \text{et} \qquad \forall (x,y) \in E^2,\ f(x+y) = f(x) + f(y).$$

PROPOSITION 4.1.2 *Une application $f : E \to F$ est une application linéaire si et seulement si :*

$$\forall \lambda \in \mathbb{K},\ \forall (x,y) \in E^2,\quad f(\lambda x + y) = \lambda f(x) + f(y).$$

REMARQUE 4.1.3 Soit $f : E \to F$ une AL. Alors $f(0) = 0$.

DÉFINITION 4.1.4 Soit E et F deux $\mathbb{K}$-ev. On note $\mathcal{L}(E,F)$ l'ensemble des applications linéaires de E vers F. Si $E = F$, on note $\mathcal{L}(E)$ l'ensemble des applications linéaires de E dans lui-même. Une telle application linéaire de E dans lui-même est appelée *endomorphisme* de E.

PROPOSITION 4.1.5 *$\mathcal{L}(E,F)$ est un espace vectoriel sur $\mathbb{K}$.*

PROPOSITION 4.1.6 *Soit $f \in \mathcal{L}(E,F)$ et $g \in \mathcal{L}(F,G)$. Alors $g \circ f$ est une application linaire de E vers G.*

DÉFINITION 4.1.7 Une *forme linéaire* sur un espace vectoriel E est une application linéaire de E dans $\mathbb{K}$. L'ensemble $\mathcal{L}(E,\mathbb{K})$ des formes linéaires sur $\mathbb{K}$ est souvent noté E^*, et appelé *dual de E*.

4.1.2 Image et noyau

Dans ce paragraphe, E et F sont deux espaces vectoriels, et $f \in \mathcal{L}(E,F)$.

DÉFINITION 4.1.8

1. L'image de f est $\mathrm{Im}(f) = \{y \in F \mid \exists x \in E,\ f(x) = y\} = f(E)$;
2. Le noyau de f est $\mathrm{Ker}(f) = \{x \in E \mid f(x) = 0\} = f^{-1}(\{0\})$

LEMME 4.1.9 *1. Soit E' un sev de E. Alors $f(E')$ est un sev de F.*

2. Soit F' un sev de F. Alors $f^{-1}(F')$ est un sev de E.

En appliquant ce lemme avec $E' = E$ et $F' = \{0\}$, on obtient :

PROPOSITION 4.1.10 $\mathrm{Im}(f)$ *est un sev de F.* $\mathrm{Ker}(f)$ *est un sev de E.*

THÉORÈME 4.1.11 *Soit $f \in \mathcal{L}(E, F)$. Alors f est injective ssi* $\mathrm{Ker}(f) = \{0\}$.

4.1.3 Isomorphismes

DÉFINITION 4.1.12 1. Une application linéaire bijective de E vers F est appelée un *isomorphisme.*

2. On dit que deux espaces vectoriels E et F sont isomorphes s'il existe un isomorphisme $f : E \to F$.
3. Un isomorphisme de E dans lui-même est appelé *automorphisme de E*. L'ensemble des automorphismes de E est noté $\mathrm{Aut}(E)$.

THÉORÈME 4.1.13 *Soit f un isomorphisme entre E et F. Alors f^{-1} est une application linéaire, et donc un isomorphisme de F vers E.*

PROPOSITION 4.1.14 *1. L'image d'une famille libre par une application linéaire injective est une famille libre*

2. L'image d'une famille génératrice par une application linéaire surjective est une famille génératrice

3. L'image d'une base par un isomorphisme est une base

COROLLAIRE 4.1.15 *(en admettant le théorème de la dimension) Soit E et F deux espaces isomorphes. Alors si E ou F est de dimension finie, les deux le sont, et ont même dimension.*

On peut donner une version plus précise de la proposition :

PROPOSITION 4.1.16 *Soit f une application linéaire de E dans F. Alors, les propositions suivantes sont équivalentes :*

(i) f est un isomorphisme ;

(ii) L'image par f de toute base de E est une base de F ;

(iii) Il existe une base de E dont l'image par f est une base de F.

4.1.4 Projecteurs et symétries

DÉFINITION 4.1.17 1. Soit $p \in \mathcal{L}(E)$. On dit que p est un projecteur de E ssi $p \circ p = p$.

2. Soit $s \in \mathcal{L}(E)$. On dit que s est une symétrie ssi $s \circ s = \mathrm{id}$.

THÉORÈME 4.1.18 *1. Soit $p \in \mathcal{L}(E)$. Alors p est un projecteur si et seulement s'il existe deux sev F et G de E tels que $F \oplus G = E$ (ils sont supplémentaires), et :*

$$\forall u \in F,\ \forall v \in G,\ p(u+v) = u.$$

(p est la projection sur F parallèlement à G)

2. *Soit $s \in \mathcal{L}(E)$. Alors s est un projecteur si et seulement s'il existe deux sev F et G de E tels que $F \oplus G = E$, et :*
$$\forall u \in F,\ \forall v \in G,\ s(u+v) = u - v.$$
(s est la symétrie par rapport à F parallèlement à G)

4.2 Matrices

4.2.1 Définition et motivations

La motivation essentielle de l'introduction des matrices provient de l'exemple suivant, décrivant toutes les applications linéaires de $\mathbb{K}^n$ vers $\mathbb{K}^m$:

EXEMPLE 4.2.1 Soit $f \in \mathcal{L}(\mathbb{K}^n, \mathbb{K}^m)$, et soit $(e_1, \cdots, e_n)$ la base canonique de $\mathbb{K}^n$. Alors $f(e_1), \ldots, f(e_n)$ sont des vecteurs de $\mathbb{K}^m$, donc s'écrivent :
$$f(e_1) = \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{m,1} \end{pmatrix}, \quad f(e_2) = \begin{pmatrix} a_{1,2} \\ \vdots \\ a_{m,2} \end{pmatrix}, \quad \ldots \quad f(e_n) = \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{m,n} \end{pmatrix}.$$
(ce sont les coordonnées de ces vecteurs dans la base canonique de $\mathbb{K}^m$)

Soit maintenant $X \in \mathbb{K}^n$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 e_1 + \cdots + x_n e_n$. Alors, par linéarité,
$$f(X) = x_1 f(e_1) + \cdots + x_n f(e_n) = \begin{pmatrix} \sum\limits_{i=1}^{n} x_i a_{1,i} \\ \vdots \\ \sum\limits_{i=1}^{n} x_i a_{m,i} \end{pmatrix}.$$
Par conséquent, l'application linéaire f est entièrement déterminée par la donnée d'une famille $(a_{i,j})_{\substack{1\leqslant i\leqslant m \\ 1\leqslant j\leqslant n}}$ de scalaires (donc une famille « rectangulaire »). Réciproquement, toute telle famille définit une application linéaire de $\mathbb{K}^n$ dans $\mathbb{K}^m$.

DÉFINITION 4.2.2 Une matrice de taille $n \times m$ (n lignes et m colonnes) à coefficients dans $\mathbb{K}$ est la donnée d'une famille $A = (a_{i,j})_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}}$ d'éléments de $\mathbb{K}$. On utilise la représentation planaire suivante :
$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}.$$

DÉFINITION 4.2.3 L'ensemble des matrices de taille $n \times m$ (on dit aussi *de type* (n, m)) à coefficients dans $\mathbb{K}$ est noté $\mathcal{M}_{n,m}(\mathbb{K})$. Si $n = m$, on dit que la matrice est *carrée*, et on note simplement $\mathcal{M}_n(\mathbb{K})$ l'ensemble des matrices carrées de taille n.

PROPOSITION 4.2.4 *L'ensemble $\mathcal{M}_{n,m}(\mathbb{K})$ est un espace vectoriel, isomorphe à $\mathbb{K}^{nm}$.*

DÉFINITION 4.2.5 Soit $f \in \mathcal{L}(\mathbb{K}^n, \mathbb{K}^m)$. On définit la matrice $[f]_{b.c.}$ de f (autre notation fréquente : $\mathrm{Mat}_{b.c.}(f)$) comme étant la matrice de $\mathcal{M}_{m,n}(\mathbb{K})$ définie par :

$$[f]_{b.c.} = (a_{i,j})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}},$$

où les $a_{i,j}$ sont décrits ci-dessus. Ainsi, la i-ième colonne de $[f]_{b.c.}$ est constituée des coordonnées du vecteur $f(e_i)$ dans la base canonique de $\mathbb{K}^m$. La décomposition en colonnes de la matrice $[f]_{b.c.}$ est donc :

$$[f]_{b.c.} = (\ f(e_1) \mid \cdots \mid f(e_n)\ ).$$

REMARQUES 4.2.6

1. Le *b.c.* est là pour indiquer que toutes les coordonnées sont prises dans la base canonique. Il s'agit de la matrice de f relativement aux bases canoniques. On généralisera plus loin cette définition à des bases quelconques.
2. Attention à l'inversion des indices : une application linéaire de $\mathbb{K}^n$ dans $\mathbb{K}^m$ fournit une matrice à m lignes et n colonnes.

4.2.2 Somme et produit de matrices

On peut sommer deux matrices de même taille, et leur somme est définie par la somme coefficient par coefficient :

DÉFINITION 4.2.7 Soit $m, n \in \mathbb{N}^*$ Soit $A = (a_{i,j})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$ et $B = (b_{i,j})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}} \in \mathcal{M}_{n,p}(\mathbb{K})$. Alors $A + B$ est la matrice :

$$A + B = (a_{i,j} + b_{i,j})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}.$$

Les propriétés de l'addition de $\mathbb{K}$ se transfèrent immédiatement aux matrices :

PROPOSITION 4.2.8 *La somme ainsi définie sur $\mathcal{M}_{m,n}(\mathbb{K})$ est associative, commutative, admet un élément neutre (la matrice $(0)_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$) et toute matrice admet un opposé, obtenu en prenant l'opposé dans $\mathbb{K}$ de tous ses coefficients.*

Nous définissons dans un premier temps le produit d'une matrice par une matrice colonne.

DÉFINITION 4.2.9 Soit $M \in \mathcal{M}_{n,m}(\mathbb{K})$ et $X \in \mathcal{M}_{m,1}(\mathbb{K})$. On note $X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$ les coordonnées de X, et $M = (\ C_1 \mid \cdots \mid C_m\ )$ la décomposition en colonnes de M (ainsi, pour tout $i \in [\![1, m]\!]$, $C_i \in \mathcal{M}_{n,1}$ est la i-ème colonne de M). Alors

$$M \cdot X = x_1 C_1 + \cdots + x_m C_m = \sum_{i=1}^{m} x_i C_i.$$

De l'exemple 4.2.1, on déduit immédiatement :

PROPOSITION 4.2.10 *Soit $f \in \mathcal{L}(\mathbb{K}^n, \mathbb{K}^m)$; alors, pour tout $X \in \mathbb{K}^n$, $f(X) = [f]_{b.c.} \cdot X$.*

On définit maintenant le produit général de deux matrices. Vous remarquerez que le produit n'est pas commutatif, et que le nombre de colonnes de la matrice de gauche doit être égal au nombre de lignes de la matrice de droite pour que le produit soit défini.

DÉFINITION 4.2.11 Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$ et $B \in \mathcal{M}_{n,p}(\mathbb{K})$. Alors le produit AB est la matrice de $\mathcal{M}_{m,p}(\mathbb{K})$ dont la décomposition par colonnes est donnée par :

$$AB = (\ A \cdot B_1 \mid \cdots \mid A \cdot B_p\ ),$$

où $B_1, \ldots, B_p$ sont les colonnes de la matrice B.

THÉORÈME 4.2.12 *Soit $f \in \mathcal{L}(\mathbb{K}^m, \mathbb{K}^n)$ et $g \in \mathcal{L}(\mathbb{K}^n, \mathbb{K}^p)$. Alors l'application linéaire $g \circ f$ de $\mathcal{L}(\mathbb{K}^m, \mathbb{K}^p)$ est de matrice dans la base canonique :*

$$[g \circ f]_{b.c.} = [g]_{b.c.} \cdot [f]_{b.c.}.$$

Ainsi, le produit des matrices correspond à la composition des applications linéaires.

PROPOSITION 4.2.13 *Soit $A = (a_{i,j})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}} \in \mathcal{M}_{m,n}(\mathbb{K})$ et $B = (b_{j,k})_{\substack{1 \leqslant j \leqslant n \\ 1 \leqslant k \leqslant p}} \in \mathcal{M}_{n,p}(\mathbb{K})$. Soit $AB = (c_{i,k})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant k \leqslant p}} \in \mathcal{M}_{m,p}(\mathbb{K})$ la matrice produit. Alors :*

$$\forall i \in [\![1, m]\!],\ \forall k \in [\![1, p]\!],\quad c_{i,k} = \sum_{j=1}^{n} a_{i,j} b_{j,k} = L_i \cdot C_k,$$

où L_i est la i-ème ligne de A, et C_k la k-ième colonne de B_k.

On obtient une version duale des définitions 4.2.9 et 4.2.11 en inversant le rôle des lignes et des colonnes (cela provient de la description complètement symétrique donnée dans la proposition précédente) :

PROPOSITION 4.2.14

1. *Soit $A \in \mathcal{M}_{1,n}(\mathbb{K})$, $A = (\ x_1\ \ldots\ x_n\ )$ et $B \in \mathcal{M}_{n,p}(\mathbb{K})$ dont les lignes sont $L_1, \ldots, L_n$. Alors AB est la matrice ligne obtenue par la combinaison linéaire suivante :*

$$AB = x_1 L_1 + \cdots + x_n L_n = \sum_{i=1}^{n} x_i L_i.$$

2. *Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$, dont les lignes sont $A_1, \ldots, A_m$, et $B \in \mathcal{M}_{n,p}(\mathbb{K})$. Alors AB est la matrice dont les lignes sont $A_1 \cdot B, \ldots, A_m \cdot B$.*

PROPOSITION 4.2.15 *Propriétés du produit. Soit $m, n, p, q \in \mathbb{N}^*$;*

1. *Associativité : $\forall M \in \mathcal{M}_{m,n}(\mathbb{K})$, $\forall N \in \mathcal{M}_{n,p}(\mathbb{K})$, $\forall P \in \mathcal{M}_{p,q}(\mathbb{K})$, $(MN)P = M(NP)$.*
2. *Distributivité : $\forall M \in \mathcal{M}_{m,n}(\mathbb{K})$, $\forall (N_1, N_2) \in \mathcal{M}_{n,p}(\mathbb{K})^2$, $M(N_1 + N_2) = MN_1 + MN_2$;*
   $\forall (M_1, M_2) \in \mathcal{M}_{m,n}(\mathbb{K})^2$, $\forall N \in \mathcal{M}_{n,p}(\mathbb{K})$, $(M_1 + M_2)N = M_1 N + M_2 N$;
3. *Neutre : Soit $I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$ la matrice carrée de taille n constituée de 1 sur la diagonale et de 0 partout ailleurs. Alors :*

$$\forall M \in \mathcal{M}_{m,n}(\mathbb{K}),\ MI_n = M \qquad \text{et} \qquad \forall N \in \mathcal{M}_{n,p}(\mathbb{K}),\ I_n N = N.$$

En particulier, I_n est un élément neutre pour le produit restreint à $\mathcal{M}_n(\mathbb{K})$.

REMARQUE 4.2.16 I_n est la matrice de l'endomorphisme identité de $\mathbb{K}^n$.

4.2.3 Inverse d'une matrice

DÉFINITION 4.2.17 On dit qu'une matrice de $\mathcal{M}_{m,n}(\mathbb{K})$ est inversible si elle est la matrice dans la base canonique d'une application linéaire $f \in \mathcal{L}(\mathbb{K}^n, \mathbb{K}^m)$ qui est un isomorphisme.

REMARQUE 4.2.18 Un isomorphisme f envoie une base sur une base. Ainsi, en particulier, f est une application linéaire entre deux espaces de même dimension. Ainsi, dans la définition ci-dessus, il vient forcément $n = m$. Ainsi, toute matrice inversible est carrée. De plus, si f est un automorphisme de $\mathbb{K}^n$ on obtient : $[f^{-1}] \cdot [f] = [\mathrm{id}] = [f] \cdot [f^{-1}]$. On obtient donc la définition équivalente suivante :

DÉFINITION 4.2.19 (équivalente) Une matrice inversible A est une matrice carrée, disons de taille n, telle qu'il existe une matrice $B \in \mathcal{M}_n(\mathbb{K})$ vérifiant $AB = BA = I_n$. La matrice B est appelée *inverse de* A, et notée $B = A^{-1}$. Si A est la matrice d'un automorphisme f dans la base canonique, alors A^{-1} est la matrice de f^{-1}.

NOTATION 4.2.20 L'ensemble des matrices inversibles de $\mathcal{M}_n(\mathbb{K})$ est noté $\mathrm{GL}_n(\mathbb{K})$, et est appelé *$n$-ième groupe linéaire.*

PROPOSITION 4.2.21 *Soit A et B deux matrices inversibles de $\mathcal{M}_n(\mathbb{K})$. Alors AB est inversible, et son inverse est $B^{-1}A^{-1}$.*

Calcul pratique de l'inverse (première méthode)
L'équation $f(X) = Y$ est équivalente à $Y = f^{-1}(X)$. Matriciellement, cela se traduit ainsi : l'équation $AX = Y$, qui est un système linéaire dont les inconnues sont les coordonnées de X, est équivalente à l'équation $A^{-1}Y = X$, qui est un système linéaire dont les inconnues sont les coordonnées de Y. Ainsi, le principe du calcul de A^{-1} est de résoudre le système $AX = Y$, ce qui fournit un système en l'inconnue Y. Les coefficients de ce système sont les coefficients de la matrice A^{-1}.

Inverse des matrices 2×2

THÉORÈME 4.2.22 *Soit* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{K})$. *Alors M est inversible si et seulement si $ad - bc \neq 0$, et*

$$M^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

DÉFINITION 4.2.23 La quantité $ad - bc$ est appelée *déterminant* de M, et est noté $\det M$ ou $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$.

REMARQUE 4.2.24 Il existe une notion de déterminant pour des matrices carrées de taille quelconque n. N'essayez pas de la deviner, ni de faire croire à quiconque que vous la connaissez. Cette notion, pour $n > 2$, est résolument hors programme. Ne tombez pas dans le piège de certains correcteurs qui voudraient tester vos connaissance. Mieux vaut avouer son ignorance que raconter n'importe quoi.

4.2.4 Transposition

DÉFINITION 4.2.25 Soit $A = (a_{i,j})_{\substack{1\leqslant i\leqslant m \\ 1\leqslant j\leqslant n}} \in \mathcal{M}_{m,n}(\mathbb{K})$. Alors la matrice transposée de A, notée ${}^tA$, est la matrice de $\mathcal{M}_{n,m}\mathbb{K}$ définie par :

$$ {}^tA = (b_{j,i})_{\substack{1\leqslant j\leqslant n \\ 1\leqslant i\leqslant m}}, \qquad \text{où} \qquad \forall i \in [\![1,m]\!],\ \forall j \in [\![1,n]\!],\ \ b_{j,i} = a_{i,j}. $$

PROPOSITION 4.2.26 *Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$ et $B \in \mathcal{M}_{n,p}(\mathbb{K})$. Alors :*

$$ {}^t(MN) = {}^tN{}^tM. $$

DÉFINITION 4.2.27 Soit $A \in \mathcal{M}_n(\mathbb{K})$.

1. On dit que A est *symétrique* si $A = {}^tA$.
2. On dit que A est *antisymétrique* si $A = -{}^tA$.

4.2.5 Produit par blocs

On peut faire des produits matriciels en regroupant les coefficients par sous-matrices, à condition d'avoir compatibilité des tailles. Ainsi, en particulier, si $M = \begin{pmatrix} M_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & M_k \end{pmatrix}$, les M_i étant des matrices carrées (on dit que M est diagonale par blocs), alors :

$$ M^n = \begin{pmatrix} M_1^n & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & M_k^n \end{pmatrix}. $$

4.3 Écriture d'une AL dans une base

4.3.1 Définitions et notations

Soit E et F deux espaces vectoriels de dimensions finies

DÉFINITION 4.3.1 Soit $\mathcal{C} = (c_1, \ldots, c_n)$ une base de F, et $X \in F$. Alors il existe d'uniques scalaires $x_1, \ldots, x_n$ tels que $X = x_1c_1 + \cdots + x_nc_n$. La matrice colonne de X dans la base $\mathcal{C}$ est alors la matrice colonne constituée de ces scalaires :

$$ [X]_{\mathcal{C}} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \text{(notation personnelle).} $$

DÉFINITION 4.3.2 Sous les mêmes hypothèses, soit $(X_1, \ldots, X_m)$ une famille de vecteurs de F. Alors la matrice de cette famille dans la base $\mathcal{C}$ est :

$$ [X_1, \ldots, X_m]_{\mathcal{C}} = (\ [X_1]_{\mathcal{C}} \mid \cdot \mid [X_m]_{\mathcal{C}}\ ). $$

Ainsi, il s'agit de la matrice dont la i-ème colonne comporte les coordonnées dans la base $\mathcal{C}$ du vecteur X_i.

DÉFINITION 4.3.3 Soit $f \in \mathcal{L}(E, F)$, et soit $\mathcal{B} = (b_1, \dots, b_m)$ une base de de E et $\mathcal{C} = (c_1, \dots, c_n)$ une base de F. Alors la matrice de f relativement aux bases $\mathcal{B}$ et $\mathcal{C}$ est la matrice $[f]_{\mathcal{B},\mathcal{C}}$ de la famille $(f(b_1), \dots, f(b_m))$ dans la base $\mathcal{C}$:

$$[f]_{\mathcal{B},\mathcal{C}} = [f(b_1), \dots, f(b_m)]_{\mathcal{C}} = (\ [f(b_1)]_{\mathcal{C}} \mid \cdot \mid [f(b_m)]_{\mathcal{C}}\ ).$$

Ainsi, il s'agit de la matrice de type (n, m) dont la i-ème colonne donne les coordonnées du vecteur $f(b_i)$ dans la base $\mathcal{C}$. On trouve souvent la notation $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$.

REMARQUE 4.3.4 Si on prend $E = \mathbb{R}^m$, $F = \mathbb{R}^n$, et pour $\mathcal{B}$ et $\mathcal{C}$ les bases canoniques de ces espaces, on retrouve la matrice $[f]_{b.c.}$.

PROPOSITION 4.3.5 *Sous les hypothèses de la définition :*

$$\forall X \in E, \quad [f(X)]_{\mathcal{C}} = [f]_{\mathcal{B},\mathcal{C}} \cdot [X]_{\mathcal{B}}.$$

PROPOSITION 4.3.6 ***(La formule magique)*** *Soit E, F et G trois espaces vectoriels de dimension finie, munis respectivement des bases $\mathcal{B}$, $\mathcal{C}$ et $\mathcal{D}$. Soit $f \in \mathcal{L}(E, F)$ et $g \in \mathcal{L}(F, G)$. Alors :*

$$[g \circ f]_{\mathcal{B},\mathcal{D}} = [g]_{\mathcal{C},\mathcal{D}} \cdot [f]_{\mathcal{B},\mathcal{C}}.$$

4.3.2 Changements de base

DÉFINITION 4.3.7 Soit E un espace vectoriel, et $\mathcal{B}_1$ et $\mathcal{B}_2$ deux bases de E. Alors la matrice de passage de la base $\mathcal{B}_1$ à la base $\mathcal{B}_2$ est la matrice :

$$[\mathcal{B}_1 \to \mathcal{B}_2] = \mathrm{Mat}(\mathcal{B}_1, \mathcal{B}_2) = [\mathrm{id}]_{\mathcal{B}_2,\mathcal{B}_1}.$$

Ainsi, la i-ème colonne de cette matrice est constituée des coordonnées du i-ème vecteur de la base $\mathcal{B}_2$ dans la base $\mathcal{B}_1$.

PROPOSITION 4.3.8 *Toute matrice de passage $[\mathcal{B}_1 \to \mathcal{B}_2]$ est inversible. Son inverse est la matrice de passage $[\mathcal{B}_2 \to \mathcal{B}_1]$*

Puisque $[X]_{\mathcal{B}_1} = [\mathrm{id}]_{\mathcal{B}_2,\mathcal{B}_1}[X]_{\mathcal{B}_2}$, on obtient l'expression de l'effet d'un changement de base sur les coordonnées d'un vecteur :

PROPOSITION 4.3.9 *Soit $X \in E$. Alors $[X]_{\mathcal{B}_1} = [\mathcal{B}_1 \to \mathcal{B}_2] \cdot [X]_{\mathcal{B}_2}$.*

THÉORÈME 4.3.10 *(Formule de changement de base)*
Soit E un espace vectoriel de dimension finie, muni de deux bases $\mathcal{B}_1$ et $\mathcal{B}_2$, et F un espace vectoriel de dimension finie, muni de deux bases $\mathcal{C}_1$ et $\mathcal{C}_2$. Soit $f \in \mathcal{L}(E, F)$. Alors :

$$[f]_{\mathcal{B}_2,\mathcal{C}_2} = [\mathcal{C}_2 \to \mathcal{C}_1] \cdot [f]_{\mathcal{B}_1,\mathcal{C}_1} \cdot [\mathcal{B}_1 \to \mathcal{B}_2]$$

4.3.3 Cas des endomorphismes

Dans le cas d'un endomorphisme f, on exprime souvent sa matrice dans la même base au départ et à l'arrivée. On note alors $[f]_{\mathcal{B}}$ au lieu de $[f]_{\mathcal{B},\mathcal{B}}$. On obtient alors la formule de changement de base suivante :

Théorème 4.3.11 *Soit $f \in \mathcal{L}(E)$, E étant un espace vectoriel de dimension finie, muni de deux bases $\mathcal{B}_1$ et $\mathcal{B}_2$. Soit $P = [\mathcal{B}_1 \to \mathcal{B}_2]$ la matrice de passage de la base $\mathcal{B}_1$ à la base $\mathcal{B}_2$. Alors :*

$$[f]_{\mathcal{B}_2} = P^{-1}[f]_{\mathcal{B}_1}P.$$

Définition 4.3.12 On dit que deux matrices $A, B \in \mathcal{M}_n(\mathbb{K})$ sont semblables s'il existe une matrice inversible $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $B = P^{-1}AP$.

Ainsi, les matrices d'un endormorphisme dans différentes bases de E sont semblables.

4.4 Applications linéaires en dimension finie

4.4.1 Rang d'une application linéaire

Remarque 4.4.1 Soit E et F deux espaces vectoriels, et $f \in \mathcal{L}(E, F)$. Si $(g_i)_{i\in I}$ est une famille génératrice de E, alors $(f(g_i))_{i\in I}$ est une famille génératrice de $\operatorname{Im} f$. En particulier, si E est de dimension finie, alors $\operatorname{Im} f$ est de dimension finie.

Définition 4.4.2 Soit E et F deux espaces vectoriels, E étant de dimension finie. Soit $f \in \mathcal{L}(E, F)$. Le rang de f, noté $\operatorname{rg} f$, est la dimension de $\operatorname{Im} f$:

$$\operatorname{rg} f = \dim \operatorname{Im} f.$$

Lemme 4.4.3 *Soit E et F deux espaces vectoriels quelconques, et $f \in \mathcal{L}(E, F)$. Les propositions suivantes sont équivalentes :*

(i) f est injective ;

(ii) f envoie toute famille libre sur une famille libre ;

(iii) il existe une base de E envoyée par f sur une famille libre de F.

Proposition 4.4.4 *Soit E et F deux espaces vectoriels, E étant de dimension finie. Soit $f \in \mathcal{L}(E, F)$.*

1. $\operatorname{rg} f \leqslant \dim E$*, avec égalité si et seulement si f est injective.*
2. *Si F est de dimension finie,* $\operatorname{rg} f \leqslant \dim F$*, avec égalité si et seulement si f est surjective.*

Théorème 4.4.5 *(Caractérisation des isomorphismes entre espaces de même dimension) Soit E et F deux espaces vectoriels de même dimension finie n, et soit $f \in \mathcal{L}(E, F)$. Alors les propositions suivantes sont équivalentes :*

(i) f est un isomorphisme ;

(ii) $\operatorname{rg}(f) = n$;

(iii) f est injective ;

(iv) f est surjective.

En particulier, si E est de dimension finie, un endomorphisme $f \in \mathcal{L}(E)$ est un automorphisme si et seulement si f est injective si et seulement si f est surjective.

THÉORÈME 4.4.6 *(Théorème du rang) Soit E un espace vectoriel de dimension finie, et F un espace vectoriel quelconque. Soit $f \in \mathcal{L}(E, F)$. Alors :*

$$\dim \operatorname{Ker} f + \operatorname{rg} f = \dim E.$$

4.4.2 Formes linéaires

DÉFINITION 4.4.7 Une forme linéaire sur un $\mathbb{K}$-espace vectoriel E est une application linéaire de E vers $\mathbb{K}$.

PROPOSITION 4.4.8 *Soit E un espace vectoriel de dimension finie. Soit $f \in \mathcal{L}(E, \mathbb{K})$ une forme linéaire. Alors* $\operatorname{Ker} f$ *est soit égal à E (dans l'unique cas où $f = 0$), soit égal à un hyperplan de E.*

PROPOSITION 4.4.9 *Réciproquement, tout hyperplan d'un espace vectoriel de dimension finie E est le noyau d'une forme linéaire non nulle.*

PROPOSITION 4.4.10 *Plus généralement, soit E un espace vectoriel de dimension finie n, et F un sous-espace vectoriel de E de dimension k. Alors il existe une application linéaire $f \in \mathcal{L}(E, \mathbb{K}^{n-k})$ telle que $F = \operatorname{Ker} f$.*

4.4.3 Rang d'une matrice

DÉFINITION 4.4.11 Soit $M \in \mathcal{M}_{n,m}(\mathbb{K})$, et $M_1, \ldots, M_m \in \mathcal{M}_{n,1}(\mathbb{K})$ ses colonnes. Alors le *rang de la matrice* M est le rang de la famille $(M_1, \ldots, M_k)$ de vecteurs de $\mathbb{K}^n$. Il est noté $\operatorname{rg} M$

PROPOSITION 4.4.12 *Soit $M \in \mathcal{M}_{n,m}(\mathbb{K})$. Alors* $\operatorname{rg} M \leqslant \min(n, m)$.

PROPOSITION 4.4.13 *Soit $M \in \mathcal{M}_n(\mathbb{K})$, et $X_1, \ldots, X_n$ les colonnes de M. Alors les propositions suivantes sont équivalentes :*

(i) M *est inversible*

(ii) $\operatorname{rg} M = n$

(iii) $(X_1, \ldots, X_n)$ *est une base de* $\mathbb{K}^n$.

THÉORÈME 4.4.14 *Soit E et F des espaces vectoriels de dimension finie, $\mathcal{B}$ et $\mathcal{C}$ des bases de E et F. Alors le rang de f est égal au rang de la matrice de f relativement aux bases $\mathcal{B}$ et $\mathcal{C}$:*

$$\operatorname{rg} f = \operatorname{rg}[f]_{\mathcal{B},\mathcal{C}}.$$

En particulier toutes les matrices représentant la même application linéaire dans des choix de bases différents ont le même rang.

COROLLAIRE 4.4.15 *Soit $M \in \mathcal{M}_{n,m}(\mathbb{K})$, et $P \in \mathrm{GL}_n(\mathbb{K})$, $Q \in \mathrm{GL}_m(\mathbb{K})$ des matrices inversibles. Alors :*

$$\operatorname{rg}(PM) = \operatorname{rg} M = \operatorname{rg}(MQ).$$

Chapitre 5

Le pivot de Gauss

Dans tout ce chapitre, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

5.1 Matrices échelonnées

5.1.1 Définition

Définition 5.1.1 Soit m et n deux entiers non nuls, et $M = (a_{i,j})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$ dans $\mathcal{M}_{m,n}(\mathbb{K})$. On dit que M est une matrice échelonnée s'il existe un entier $k \in [\![1, m]\!]$ et une suite croissante $j_1 < j_2 < \cdots < j_k$ d'éléments de $[\![1, n]\!]$ tels que :

(i) $\forall i \in [\![1, k]\!]$, $a_{i,j_i} \neq 0$;

(ii) $\forall i \in [\![1, k]\!]$, $\forall j \in [\![1, j_i - 1]\!]$, $a_{i,j} = 0$;

(iii) $\forall i \in [\![k + 1, m]\!]$, $\forall j \in [\![1, n]\!]$, $a_{i,j} = 0$

Autrement dit, les lignes nulles sont regroupées au bas de la matrice (lignes $k+1$ à m), les autres lignes sont classées suivant la position de leur premier élément non nul, ces positions étant deux à deux distinctes. Une matrice échelonnée admet donc la représentation suivante :

$$M = \begin{pmatrix} 0 & \cdots\ 0 & a_{1,j_1} & \bullet & & & & \cdots & & \bullet \\ 0 & \cdots & \cdots & 0 & a_{2,j_2} & \bullet & & & \cdots & \bullet \\ \vdots & & & & & & & & & \vdots \\ 0 & & \cdots & \cdots & & 0 & a_{k,j_k} & \bullet & \cdots & \bullet \\ 0 & & & \cdots & & & \cdots & & & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & & & \cdots & & & \cdots & & & 0 \end{pmatrix},$$

les coefficients indiqués d'un $\bullet$ étant quelconques.

Exemples 5.1.2 $\begin{pmatrix} 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ est échelonnée, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 5 & 6 & 7 \\ 0 & 8 & 9 & 10 \\ 0 & 0 & 0 & 11 \end{pmatrix}$ ne l'est pas.

5.1.2 Matrices échelonnées inversibles

THÉORÈME 5.1.3 *Une matrice échelonnée est inversible si et seulement si c'est une matrice carrée, triangulaire supérieure, à coefficients diagonaux non nuls.*

EXEMPLE 5.1.4 Soit $(P_0, \ldots, P_n)$ une famille de polynômes de $\mathbb{R}_n[X]$ tels que pour tout $k \in [\![1, n]\!]$, $\deg(P_k) = k$, alors $(P_0, \ldots, P_n)$ est une base de $\mathbb{R}_n[X]$. En effet la matrice de cette famille dans la base canonique de $\mathbb{R}_n[X]$ est triangulaire supérieure à ceofficients diagonaux non nuls, donc inversible. Les colonnes sont donc les coefficients dans la base canonique de vecteurs formant une base de $\mathbb{R}_n[X]$.

5.1.3 Rang d'une matrice échelonnée

THÉORÈME 5.1.5 *Soit $M \in \mathcal{M}_{m,n}(\mathbb{K})$ une matrice échelonnée, et k tel que dans la définition. Alors* $\mathrm{rg}(M) = k$.
Autrement dit, le rang d'une matrice échelonnée est égal au nombre de ses lignes non nulles.

REMARQUE 5.1.6 Soit $M \in \mathcal{M}_{m,n}(\mathbb{K})$ échelonnée, et $f \in \mathcal{L}(\mathbb{K}^n, \mathbb{K}^m)$ canoniquement associée à M. Soit $(f_1, \ldots, f_m)$ la base canonique de $\mathbb{K}^m$. Alors $(f_1, \ldots, f_k)$ est une base de $\mathrm{Im}\, f$.

PROPOSITION 5.1.7 *Soit M une matrice échelonnée, et $j_1 < \cdots < j_k$ comme dans la définition. Soit f l'application linéaire canoniquement associée à M. On définit :*

$$\begin{array}{rccc} \varphi : & \mathrm{Ker}\, f & \longrightarrow & \mathbb{K}^{n-k} \\ & X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \longmapsto & \begin{pmatrix} x_1 \\ \vdots \\ x_{j_i-1} \\ x_{j_i+1} \\ \vdots \\ x_n \end{pmatrix} \end{array} \qquad \textit{(on oublie les coordonnées } x_{j_1}, \ldots, x_{j_k}\textit{)}$$

Alors φ est un isomorphisme. En particulier, on trouve une base de $\mathrm{Ker}\, f$ *en prenant l'image réciproque par φ d'une base de $\mathbb{K}^{n-k}$, par exemple de la base canonique.*

EXEMPLE 5.1.8

Soit $M = \begin{pmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 & 2 \end{pmatrix}$, et f canoniquement associée. Une base de $\mathrm{Ker}\, f$ est $\left(\begin{pmatrix} 1 \\ 0 \\ -2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -2 \\ 0 \\ 1 \end{pmatrix} \right)$.

5.2 Le pivot de Gauss

5.2.1 Opérations élémentaires

Soit M une matrice de $\mathcal{M}_{m,n}(\mathbb{K})$, et soit $L_1, \ldots, L_m$ les lignes de M.

DÉFINITION 5.2.1 On appelle opération élémentaire sur la matrice M une des trois opérations suivantes :

(i) l'échange de deux lignes L_i et L_j (notée $L_i \leftrightarrow L_j$),

(ii) le remplacement d'une ligne L_i par la combinaison linéaire $L_i + \lambda L_j$, où $i \neq j$, $\lambda \in \mathbb{K}$ (notée $L_i \leftarrow L_i + \lambda L_j$)

(iii) le remplacement de L_i par λL_i où $\lambda \in \mathbb{K}^*$ (notée $L_i \leftarrow \lambda L_i$).

On définit, pour tout $l \in \mathbb{K}$, pour tous $i \neq j$ dans $[\![1, m]\!]$, les matrices $E_{i,j}$, $E_{i,j}(\lambda)$ et $E_i(\lambda)$ dans $\mathcal{M}_m(\mathbb{K})$:

$$E_{i,j} = \begin{array}{cc} \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & & & & & & \vdots \\ \vdots & \ddots & 1 & \ddots & & & & & & & \vdots \\ \vdots & & \ddots & 0 & \ddots & & & 1 & & & \vdots \\ \vdots & & & \ddots & 1 & \ddots & & & & & \vdots \\ \vdots & & & & \ddots & \ddots & \ddots & & & & \vdots \\ \vdots & & & & & \ddots & 1 & \ddots & & & \vdots \\ \vdots & & & 1 & & & \ddots & 0 & \ddots & & \vdots \\ \vdots & & & & & & & \ddots & 1 & \ddots & \vdots \\ \vdots & & & & & & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix} & \begin{matrix} \\ \\ \\ i \\ \\ \\ \\ j \\ \\ \\ \\ \end{matrix} \\ \begin{matrix} & & & i & & & & j & & & \end{matrix} & \end{array}$$

(les coefficients diagonaux sont tous égaux à 1, sauf ceux en position (i, i) et (j, j), égaux à 0 ; les coefficients non diagonaux sont tous nuls, sauf ceux en position (i, j) et (j, i) égaux à 1) ;

$$E_{i,j}(\lambda) = \begin{array}{cc} \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & \lambda & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix} & \begin{matrix} \\ i \\ \\ \\ \\ \\ \end{matrix} \\ \begin{matrix} & & & j & & \end{matrix} & \end{array}$$

(les coefficients diagonaux sont égaux à 1, tous les autres sont nuls, sauf celui en position (i, j), égal à 1) ;

$$E_i(\lambda) = \begin{array}{cc} \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & & \vdots \\ \vdots & \ddots & 1 & \ddots & & & \vdots \\ \vdots & & \ddots & \lambda & \ddots & & \vdots \\ \vdots & & & \ddots & 1 & \ddots & \vdots \\ \vdots & & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix} & \begin{matrix} \\ \\ \\ i \\ \\ \\ \\ \end{matrix} \\ \begin{matrix} & & & i & & & \end{matrix} & \end{array}$$

(matrice diagonale à coefficients diagonaux tous égaux à 1, sauf celui en position (i, i), égal à λ).

THÉORÈME 5.2.2 *Soit $M \in \mathcal{M}_{m,n}(\mathbb{K})$. Soit $i \neq j$ dans $[\![1, m]\!]$, et $\lambda \in \mathbb{K}$.*

(i) La matrice N obtenue de M par l'opération $L_i \leftrightarrow L_j$, est $N = E_{i,j} \cdot M$;

(ii) La matrice N obtenue de M par l'opération $L_i \leftarrow L_i + \lambda L_j$ est $N = E_{i,j}(\lambda) \cdot M$;

(iii) La matrice N obtenue de M par l'opération $L_i \leftarrow \lambda L_i$, $\lambda \neq 0$, est $N = E_i(\lambda) \cdot M$.

Autrement dit, faire les opérations $L_i \leftrightarrow L_j$, $L_i \leftarrow L_i + \lambda L_j$ et $L_i \leftarrow \lambda L_i$ revient respectivement à multiplier M par la gauche par les matrices $E_{i,j}$, $E_{i,j}(\lambda)$ et $E_i(\lambda)$.

PROPOSITION 5.2.3

1. *Pour tous $i \neq j$ dans $[\![1, m]\!]$, $E_{i,j}$ est inversible, d'inverse $E_{i,j}^{-1} = E_{i,j}$.*
2. *Pour tous $i \neq j$ dans $[\![1, m]\!]$, et tout $\lambda \in \mathbb{K}$, et $E_{i,j}(\lambda)$ est inversible, et $E_{i,j}(\lambda)^{-1} = E_{i,j}(-\lambda)$.*
3. *Pour tout $i \in [\![1, m]\!]$, et tout $\lambda \in \mathbb{K}^*$, $E_i(\lambda)$ est inversible, d'inverse $E_i(\lambda)^{-1} = E_i(\frac{1}{\lambda})$.*

COROLLAIRE 5.2.4 *Soit $M \in \mathcal{M}_{m,n}(\mathbb{K})$, et N une matrice obtenue à partir de M en effectuant une succession d'opérations élémentaires. Alors $\mathrm{rg}(M) = \mathrm{rg}(N)$.*

5.2.2 L'algorithme du pivot

DÉFINITION 5.2.5 Soit M une matrice de $\mathcal{M}_{m,n}(\mathbb{K})$. Une réduite de Gauss de M est une matrice échelonnée N obtenue à partir de M en effectuant des opérations élémentaires.

THÉORÈME 5.2.6 *(algorithme du pivot de Gauss) Toute matrice M admet une réduite de Gauss (on n'a pas unicité).*

La démonstration de ce théorème est tout aussi importante, sinon plus, que le résultat lui-même, puisqu'elle consiste en la description de l'algorithme du pivot de Gauss. C'est pourquoi, une fois n'est pas coutume, je rédige ici cette démonstration.

$\triangleleft$ *Démonstration.*

On raisonne par récurrence sur $n \in \mathbb{N}$, le nombre de colonnes de A.

Soit, pour tout n dans $\mathbb{N}$, la propriété $\mathcal{P}(n)$: toute matrice A ayant n colonnes admet une réduite de Gauss.

$\mathcal{P}(0)$ est trivial, puisqu'une matrice ayant 0 colonne est une matrice vide, donc déjà réduite !

Soit $n \in \mathbb{N}$ tel que $\mathcal{P}(n)$ soit vrai. Soit A une matrice ayant $n+1$ colonnes. Soit m son nombre de lignes.

- Si la première colonne de A est nulle, il existe une matrice $A' \in \mathcal{M}_{m,n}(\mathbb{K})$ telle que :

$$A = \left(\begin{array}{c|c} 0 & \\ \vdots & A' \\ 0 & \end{array}\right).$$

Comme A' a n colonnes, on peut lui appliquer l'hypothèse de récurrence : A' admet une réduite de Gauss M', obtenu en effectuant certaines opérations élémentaires sur les lignes. En effectuant ces mêmes opérations élémentaires sur la matrice A (cela ne modifie pas la colonne de 0), on trouve une matrice :

$$M = \left(\begin{array}{c|c} 0 & \\ \vdots & M' \\ 0 & \end{array}\right).$$

Cette matrice est échelonnée, et est donc une réduite de Gauss de A.

- Si la première colonne de A est non nulle, notons-là $C_1 = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$. Il existe alors $i \in [\![1, m]\!]$ tel que $x_i \neq 0$. Commençons par faire l'opération $L_1 \leftrightarrow L_i$. On obtient une matrice :

$$\begin{pmatrix} x_i & \bullet & \cdots & \cdots & \bullet \\ x_2 & \vdots & & & \vdots \\ \vdots & \vdots & & & \vdots \\ x_1 & \vdots & & & \vdots \\ \vdots & \vdots & & & \vdots \\ x_m & \bullet & \cdots & \cdots & \bullet \end{pmatrix}$$

Les points correspondent à des coefficients quelconques. On effectue maintenant les opérations :

$$\begin{cases} \forall k \in [\![2, m]\!] \setminus \{i\},\ L_k \leftarrow L_k - \frac{x_k}{x_i} L_1 \\ L_i \leftarrow L_i - \frac{x_1}{x_i}. \end{cases}$$

On se retrouve avec une matrice dont le seul élément non nul sur la première colonne est le pivot x_i :

$$\begin{pmatrix} x_i & \bullet & \cdots & \bullet \\ 0 & & & \\ \vdots & & \boxed{A'} & \\ 0 & & & \end{pmatrix},$$

où $A' \in \mathcal{M}_{m-1,n}$. On peut appliquer l'hypothèse de récurrence sur A' : elle admet une réduite de Gauss M', obtenue en faisant des opérations élémentaires sur les lignes de A'. En faisant ces mêmes opérations sur les lignes correspondantes de A (donc avec un décalage de 1), on obtient une matrice :

$$\begin{pmatrix} x_i & \bullet & \cdots & \bullet \\ 0 & & & \\ \vdots & & \boxed{M'} & \\ 0 & & & \end{pmatrix}.$$

Cette matrice est échelonnée. Il s'agit donc d'une réduite de Gauss de A'.

Par conséquent, $\mathcal{P}(1)$ est vraie, et pour tout n dans $\mathbb{N}$, $\mathcal{P}(n)$ entraîne $\mathcal{P}(n+1)$. D'après le principe de récurrence, $\mathcal{P}(n)$ est vraie pour tout n dans $\mathbb{N}$.

▷

DÉFINITION 5.2.7 On appelle *pivot* les différents éléments de la réduite de Gauss ayant servi à annuler les éléments situés en-dessous, donc les premiers éléments non nuls de chaque ligne.

Récapitulatif : Desciption de l'algorithme du pivot de Gauss

1. On cherche la première colonne non nulle de la matrice A.
2. Sur cette colonne, on effectue un choix de pivot : n'importe quel coefficient non nul de la colonne convient, mais on a intérêt à choisir un pivot donnant le moins de calculs possible. Il y a trois critères pour cela :

- Le pivot lui-même doit être facile à inverser. L'idéal est un pivot égal à 1.
- Les autres coefficients de la ligne du pivot doivent être « simples », de préférence des entiers.
- Plus il y a de zéros sur la ligne contenant le pivot, moins il y aura de calculs !

3. On fait un échange de lignes pour ramener le pivot choisi sur la première ligne.
4. On annule tous les coefficients situées sous le pivot à l'aide d'opérations élémentaires $L_i \leftarrow L_i + \lambda L_1$.
5. Tant que c'est possible, on recommence au 1 avec la sous-matrice A' obtenue en considérant les colonnes strictement à droite de celles du pivot, et les lignes strictement sous celle du pivot.

EXEMPLE 5.2.8 Rechercher une réduite de Gauss de la matrice $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & -1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$

Pour cela, effectuons un pivot de Gauss sur la matrice A

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & -1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \qquad L_2 \leftarrow L_2 - 2L_1$$

$$\longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & -3 & -9 & -9 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \qquad L_2 \leftrightarrow L_3$$

$$\longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & -3 & -9 & -9 \end{pmatrix} \qquad L_3 \leftarrow L_3 + 3L_2$$

$$\longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & -6 & -9 \end{pmatrix}$$

Ainsi, la matrice $M = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & -6 & -9 \end{pmatrix}$ est une réduite de Gauss de A.

COROLLAIRE 5.2.9 *Le rang d'une matrice est égal au rang d'une de ses réduites de Gauss, c'est-à-dire au nombre de lignes non nulles d'une de ses réduites de Gauss.*

EXEMPLE 5.2.10 Le rang de la matrice A de l'exemple 5.2.8 est 3.

THÉORÈME 5.2.11 *En particulier, une matrice est inversible si et seulement si elle admet une réduite de Gauss triangulaire supérieure à coefficients diagonaux non nuls.*

Cela donne une façon très commode, et très systématique, d'étudier l'inversibilité d'une matrice.

EXEMPLES 5.2.12 1. Inversibilité de $M = \begin{pmatrix} 0 & 2 & 1 & 0 \\ 1 & 0 & 0 & 2 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$?

2. Inversibilité de $M = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 2 & 1 & 4 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 4 & -2 \end{pmatrix}$?

Remarque 5.2.13 • On peut toujours obtenir une réduite de Gauss de M en ne s'autorisant que les opérations élémentaires $L_i \leftrightarrow L_j$ et $L_i \leftarrow L_i + \lambda L_j$. L'algorithme du pivot que l'on a décrit n'utilise en effet par d'opération de normalisation $L_i \leftarrow \lambda L_i$.

• En s'autorisant de plus l'opération élémentaire $L_i \leftarrow \lambda L_i$, on peut toujours obtenir une réduite de Gauss « normalisée », c'est-à-dire dont tous les pivots sont égaux à 1.

5.2.3 Pivot double

Théorème 5.2.14 *1. Toute matrice M admet une réduite de Gauss telle que tous les éléments situés au-dessus des pivots soient nuls. Une telle réduite de Gauss peut toujours être obtenue à l'aide uniquement d'opérations élémentaires du type $L_i \leftrightarrow L_j$ et $L_i \leftarrow L_i + \lambda L_j$.*

2. Si on s'autorise également l'opération élémentaire $L_i \leftarrow \lambda L_i$, on peut trouver une réduite de Gauss de M telle que tous les éléments situés au-dessus des pivots soient nuls, et telle que tous les pivots soient égaux à 1.

Corollaire 5.2.15 *Soit M une matrice inversible dans $\mathcal{M}_n(\mathbb{K})$. Alors la matrice I_n est une réduite de Gauss de M. On peut trouver I_n à partir de M en effectuant un pivot double sur M.*

5.3 Calcul de l'inverse d'une matrice

Soit M une matrice inversible. D'après le corollaire 5.2.15, on peut se ramener I_n à l'aide d'un pivot de Gauss double. Ainsi, il existe des matrices $E_1, \dots, E_\ell$ correspondant aux opérations élémentaires effectuées sur M, telles que :

$$E_\ell \cdots E_1 \cdot M = I_n.$$

Ainsi, en multipliant à droite par M^{-1} :

$$M^{-1} = E_\ell \cdots E_1 \cdot I_n.$$

Ainsi, M^{-1} est la matrice obtenue de I_n en y faisant les mêmes opérations élémentaires (corespondant aux matrices $E_1, \dots, E_\ell$), dans le même ordre, que celles effectuées pour réduire M à I_n. On résume :

Théorème 5.3.1 *Soit M une matrice. M est inversible si et seulement si elle admet une réduite de Gauss triangulaire supérieure à coefficients diagonaux non nuls. Dans ce cas, I_n est une réduite de Gauss de M, obtenue en effectuant un pivot double sur M, et M^{-1} est la matrice obtenue à partir de I_n en effectuant les mêmes opérations élémentaires, dans le même ordre.*

Disposition pratique :
On dispose côte à côte la matrice M et la matrice I_n, et on effectue un pivot sur M, en faisant simultanément les opérations également sur la matrice I_n. Au moment où on obtient une réduite de Gauss triangulaire supérieure à coefficients diagonaux non nuls, on peut conclure quant à l'inversibilité de M. Dans ce cas, on continue le pivot double, simultanément sur les deux matrices, jusqu'à l'obtention de la matrice I_n à gauche. Alors la matrice située à droite est la matrice M^{-1}.

EXEMPLE 5.3.2 Calcul de l'inverse de $M = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 3 & 2 \\ 2 & 1 & 0 \end{pmatrix}$.

On effectue un pivot double sur la matrice obtenue en juxtaposant la matrice I_n :

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 1 & 3 & 2 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \qquad \begin{array}{l} L_2 \leftarrow L_2 - L_1 \\ L_3 \leftarrow L_3 - 2L_1 \end{array}$$

$$\longrightarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 1 & 0 \\ 0 & -3 & -2 & -2 & 0 & 1 \end{array}\right) \qquad L_3 \leftarrow L_3 + 3L_2$$

$$\longrightarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -5 & 3 & 1 \end{array}\right) \qquad \begin{array}{l} L_2 \leftarrow L_2 - L_3 \\ L_1 \leftarrow L_1 - L_3 \end{array}$$

$$\longrightarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 6 & -3 & -1 \\ 0 & 1 & 0 & 4 & -2 & -1 \\ 0 & 0 & 1 & -5 & 3 & 1 \end{array}\right) \qquad L_1 \leftarrow L_1 - 2L_2$$

$$\longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -2 & 1 & 1 \\ 0 & 1 & 0 & 4 & -2 & -1 \\ 0 & 0 & 1 & -5 & 3 & 1 \end{array}\right) \qquad \text{Ainsi, } M^{-1} = \begin{pmatrix} -2 & 1 & 1 \\ 4 & -2 & -1 \\ -5 & 3 & 1 \end{pmatrix}.$$

5.4 Résolution de systèmes linéaires

5.4.1 Définitions et généralités

DÉFINITION 5.4.1 Soit m et n deux entiers non nuls. Un système de m équations à n inconnues est une équation en l'inconnue X du type :

$$AX = B,$$

où $A \in \mathcal{M}_{m,n}(\mathbb{K})$, $B \in \mathcal{M}_{m,1}(\mathbb{K})$ (matrice colonne), $X \in \mathcal{M}_{n,1}(\mathbb{K})$.

En écrivant $A = (a_{i,j})_{\substack{1\leqslant i\leqslant m \\ 1\leqslant j\leqslant n}}$, $B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ et $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, et en identifiant ce produit matriciel coefficient par coefficient, on retrouve l'expression usuelle sous forme d'un système :

$$\left\{ \begin{array}{ccccccc} a_{1,1}x_1 & + & \cdots & + & a_{1,n}x_n & = & b_1 \\ \vdots & & & & & & \vdots \\ a_{m,1}x_1 & + & \cdots & + & a_{m,n}x_n & = & b_m. \end{array} \right.$$

DÉFINITION 5.4.2 Soit $AX = B$ un système linéaire de m équations à n inconnues. L'équation $AX = 0$ est appelé *système (ou équation) homogène associée au système AX=B.*

THÉORÈME 5.4.3 *Soit $AX = B$ un système linéaire de m équations à n inconnues. Soit $\mathcal{S}$ l'ensemble des solutions du système $AX = B$, et $\mathcal{S}_0$ l'ensemble des solutions du système homogène associé $AX = 0$.*

1. *$\mathcal{S}_0$ est un sous-espace vectoriel de $\mathbb{R}^n$.*

2. Si $AX = B$ admet au moins une solution X_0 (appelée solution particulière), alors :

$$\mathcal{S} = \{X_0 + X,\ X \in \mathcal{S}_0\} = \text{« } \mathcal{S}_0 + X_0 \text{ ».}$$

5.4.2 Résolution du système homogène associé

THÉORÈME 5.4.4 *Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$, et M une réduite de Gauss de A. Alors l'ensemble des solutions de l'équation homogène $AX = B$ est égal l'ensemble des solutions de l'équation $MX = 0$.*

Par conséquent, il suffit de savoir trouver les solutions d'une équation $MX = 0$, où M est échelonnée, ou encore mieux, où M est échelonnée, nulle au dessus des pivots, et de pivots tous égaux à 1.
On utilise alors le théorème 5.1.7 pour trouver une base de l'ensemble des solutions de $MX = 0$: il suffit de considérer la base canonique de $\mathbb{R}^{n-k}$ (coordonnées ne correspondant pas aux pivots), et pour chaque élément de la base canonique, d'exprimer les autres coordonnées (correspondant aux pivots). La famille de vecteurs de $\mathbb{R}^n$ ainsi obtenue est une base de l'ensemble des solutions de $MX = 0$, donc de $AX = 0$.

EXEMPLE 5.4.5 Soit $A = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \end{pmatrix}$. Déterminer l'ensemble des vecteurs $X \in \mathbb{R}^5$ tels que $AX = 0$.
En effectuant un pivot double sur A, on obtient une réduite de Gauss M de A :

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

Ainsi, l'ensemble des solutions dépend des deux paramètres x_4, x_5 formant un couple (x_4, x_5) dans $\mathbb{R}^2$. Considérons la base canonique $\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$ de $\mathbb{R}^2$. Les deux solutions correspondant aux valeurs $\begin{pmatrix} x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $\begin{pmatrix} x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ forment une base de l'espac des solutions de $AX = 0$.

- Si $\begin{pmatrix} x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, de la première ligne du produit $MX = 0$, on tire $x_1 + x_4 - 2x_5 = 0$, donc $x_1 = -1$. De la deuxième ligne, on tire $x_2 = -3x_5$, donc $x_2 = 0$, puis de même $x_3 = 0$. Ainsi, on obtient le vecteur $\begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$.
- Si $\begin{pmatrix} x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, on en déduit de même le vecteur $\begin{pmatrix} 0 \\ -3 \\ 2 \\ 0 \\ 1 \end{pmatrix}$.

Ainsi, $\left(\begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -3 \\ 2 \\ 0 \\ 1 \end{pmatrix}\right)$ est une base de l'espace des solutions de $AX = 0$

5.4.3 Trouver une solution particulière

THÉORÈME 5.4.6 *Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$, et $B \in \mathbb{K}^m$. Soit M une réduite de Gauss de A, et soit k le rang de M, c'est-à-dire le nombre de lignes non nulles de M. Soit $B' = \begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix}$ la matrice colonne obtenue à partir de B en effectuant les mêmes opérations élémentaires sur les lignes de B que celles effectuées sur A pour parvenir à M.*

1. *L'ensemble des solutions de $AX = B$ est égal à l'ensemble des solutions de $MX = B'$.*
2. *Le système $AX = B$ en l'inconnue $X \in \mathbb{K}^n$ admet au moins une solution si et seulement si pour tout $i \in [\![k+1, m]\!]$, $b'_i = 0$.*
3. *De plus, si M est échelonnée, nulle au dessus des pivots, et de pivots tous égaux à 1, en notant $j_1 < \cdots < j_k$ l'emplacement des k pivots, alors une solution particulière de $AX = B$ est donnée par :*

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \qquad \textit{avec} \qquad \begin{cases} \forall i \in [\![1, k]\!], \quad x_{j_i} = b'_i \\ \forall j \in [\![1, n]\!] \setminus \{j_1, \dots, j_k\}, \quad x_j = 0. \end{cases}$$

Pour effectuer les mêmes opérations sur A que sur B, on dispose la colonne B à côté de la matrice A, et on effectue simultanément les opérations élémentaires sur la matrice A et sur la matrice B. Bien sûr, ce pivot de Gauss peut aussi servir pour l'étude de l'équation homogène (ne faites pas deux fois le même pivot !)

EXEMPLE 5.4.7 Résoudre l'équation $\begin{pmatrix} 1 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$.

5.4.4 De l'existence ou de l'unicité des solutions

PROPOSITION 5.4.8 *Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$.*

1. *Pour que $AX = B$ admette au moins une solution pour tout $B \in \mathbb{K}^m$, il faut que $m \leqslant n$.*
2. *Pour que $AX = 0$ admette une unique solution (donc pour que $AX = B$ admette au plus une solution, pour tout $B \in \mathbb{K}^m$), il faut que $n \leqslant m$*
3. *Pour que $AX = B$ admette une unique solution pour tout $B \in \mathbb{K}^m$, il faut que $m = n$.*

Attention, ce sont des conditions nécessaires, mais **pas suffisantes !**

5.4.5 Systèmes de Cramer

DÉFINITION 5.4.9 Un système $AX = B$ est dit *de Cramer* si et seulement si A est une matrice carrée (c'est-à-dire $m = n$, il y a autant d'équations que d'inconnues), et que $AX = B$ admet une unique solution.

PROPOSITION 5.4.10 *Le système $AX = B$ est de Cramer si et seulement si A est inversible.*

REMARQUE 5.4.11 Le fait pour un système d'être de Cramer ne dépend pas de B. Ainsi, pour tout autre vecteur colonne B', $AX = B'$ est aussi de Cramer. Pour espérer obtenir un tel résultat, il était donc bien nécessaire de supposer que A est une matrice carré, au regard de la proposition 5.4.8

5.5 Rang d'une transposée

LEMME 5.5.1 *Soit M une matrice échelonnée. Alors* $\mathrm{rg}(M) = \mathrm{rg}({}^tM)$.

REMARQUE 5.5.2 Nous avons présenté le pivot de Gauss, ainsi qu'on a l'habitude de le faire, à l'aide d'opérations sur les lignes. Remarquez que faire des opérations élémentaires similaires sur les colonnes est aussi possible, et revient à multiplier (à droite cette fois) par certaines matrices élémentaires inversibles. Ainsi, faire des opérations élémentaires sur les colonnes ne change pas le rang des matrices.

THÉORÈME 5.5.3 *Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$ une matrice quelconque. Alors* $\mathrm{rg}(A) = \mathrm{rg}({}^tA)$.

5.6 Complétion d'une famille libre en une base

Soit E un espace vectoriel sur $\mathbb{K}$, de dimension finie n. Soit $(e_1, \dots, e_\ell)$ une famille libre de E, et $\mathcal{B} = (b_1, \dots, b_n)$ une base de E. D'après le théorème de complétion d'une famille libre en une base par ajout de vecteurs d'une famille génératrice donnée, on sait qu'en ajoutant des vecteurs bien choisis parmi $b_1, \dots, b_n$ à la famille $(e_1, \dots, e_\ell)$, on peut obtenir une base de E. Ci-dessous, je présente une méthode permettant de savoir quels vecteurs ajouter.
Les résultats ci-dessous ne sont pas au programme ; la méthode est à connaître et à savoir expliquer.

Soit $A = [e_1, \dots, e_\ell]_{\mathcal{B}}$ la matrice de la famille $(e_1, \dots, e_\ell)$ dans la base $\mathcal{B}$.

LEMME 5.6.1 *Soit M une matrice obtenue de A en effectuant une succession d'opérations élémentaires sur les colonnes de A. Soit $c_1, \dots c_\ell$ les vecteurs de E dont les coordonnées dans la base $\mathcal{B}$ sont les colonnes de M. Alors $(c_1, \dots, c_\ell)$ est une base de* $\mathrm{Vect}(e_1, \dots, e_\ell)$.

On a donc stabilité de l'espace vectoriel engendré par les colonnes lorsqu'on fait des opérations sur les colonnes, ce qui revient à faire des opérations sur les lignes de la transposée ${}^tA$. On obtient :

PROPOSITION 5.6.2 *Soit M une réduite de Gauss de ${}^tA$. Soit $j_1 < \dots < j_\ell$ la position des pivots. Alors on obtient une base en complétant $(e_1, \dots, e_\ell)$ par les vecteurs b_i, $i \notin \{j_1, \dots, j_\ell\}$.*

EXEMPLE 5.6.3 Soit $x_1 = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \\ 2 \end{pmatrix}$, $x_2 = \begin{pmatrix} 2 \\ 4 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $x_3 = \begin{pmatrix} 1 \\ 2 \\ 1 \\ 0 \\ 1 \end{pmatrix}$, et soit $\mathcal{B} = (e_1, e_2, e_3, e_4, e_5)$ la base canonique de $\mathbb{R}^5$. Montrer que (x_1, x_2, x_3) est libre, et compléter cette famille en une base de $\mathbb{R}^5$ par ajout de vecteurs de la base $\mathcal{B}$.

Chapitre 6

Diagonalisation

Dans tout le chapitre, $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$.

6.1 Diagonalisation des endomorphismes

6.1.1 Objectif

Soit E un espace vectoriel sur $\mathbb{K}$, et soit f un endomorphisme de E. Le but de la diagonalisation est de trouver, si cela est possible, une base $\mathcal{B}$ de E dans laquelle la matrice de E est diagonale :

$$[f]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}.$$

On notera $\mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$ la matrice diagonale dont les coefficients diagonaux sont $\lambda_1, \ldots, \lambda_n$. *Diagonaliser* f consiste à donner une telle base ainsi que la matrice de f dans cette base.

Les intérêts de la diagonalisation sont multiples. Par exemple :

- Étudier f^n, et donc calculer des puissances de matrices A^n
- Trouver des racines de matrices ou d'endomorphismes : si la matrice de f dans une base $\mathcal{B}$ est $\mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$, alors l'endomorphisme g dont la matrice dans $\mathcal{B}$ est $\mathrm{Diag}(\mu_1, \ldots, \mu_n)$ telle que pour tout $i \in [\![1, n]\!]$, $\mu_i^n = \lambda_i$, vérifie $g^n = f$. On parvient ainsi à calculer des racines de matrices à coefficients complexes, ou réels sous des conditions plus fortes. On prendra garde au fait qu'on n'obtient pas ainsi toutes les racines d'une matrice. Par exemple, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- Application à l'étude des suites récurrentes linéaires, des récurrences simultanées d'ordre 1, etc.

Dans tout le reste de cette partie, E désigne un espace vectoriel de dimension n, et f un endomorphisme de E.

6.1.2 Valeurs propres, vecteurs propres

Soit $\mathcal{B} = (b_1, \cdots, b_n)$ une base de E. Dire que $[f]_{\mathcal{B}} = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$ signifie que pour tout $i \in [\![1, n]\!]$, $f(b_i) = \lambda_i b_i$. Ainsi :

$$(f - \lambda_i \mathrm{id})(b_i) = 0 \qquad \text{soit:} \qquad b_i \in \mathrm{Ker}(f - \lambda_i \mathrm{id}).$$

En particulier, $\mathrm{Ker}(f - \lambda_i \mathrm{id}) \neq \{0\}$
Réciproquement, si $l \notin \{\lambda_1, \dots, \lambda_n\}$, alors la matrice de $f - \lambda\mathrm{id}$ dans la base $\mathcal{B}$ est :

$$[f - \lambda\mathrm{id}]_{\mathcal{B}} = \mathrm{Diag}(\lambda_1 - \lambda, \lambda_2 - \lambda, \dots, \lambda_n - \lambda).$$

Il s'agit d'une matrice diagonale (dont triangulaire supérieure) à coefficients diagonaux non nuls. Elle est donc inversible, et $\mathrm{Ker}(f - \lambda\mathrm{id}) = \{0\}$.
Cela nous amène à la propostion et à la définition suivantes :

PROPOSITION 6.1.1 *S'il existe une base $\mathcal{B}$ dans laquelle $f = \mathrm{Diag}(\lambda_1, \dots, \lambda_n)$, alors l'ensemble $\{\lambda_i, i \in [\![1, n]\!]\}$ est l'ensemble des $\lambda \in \mathbb{K}$ tels que* $\mathrm{Ker}(f - \lambda\mathrm{id}) \neq 0$.

DÉFINITION 6.1.2

1. On appelle *valeur propre* de f un scalaire λ tel que $\mathrm{Ker}(f - \lambda\mathrm{id}) \neq \{0\}$.
2. Le *spectre* de f est l'ensemble de ses valeurs propres :

$$\mathrm{Spec}(f) = \{\lambda \in \mathbb{K} \mid \mathrm{Ker}(f - \lambda\mathrm{id}) \neq \{0\}\}.$$

3. Un *vecteur propre* associé à la valeur propre λ est un vecteur non nul de $\mathrm{Ker}(f - \lambda\mathrm{id})$. C'est donc un vecteur non nul x vérifiant : $f(x) = \lambda x$.
4. Le *sous-espace propre* associé à la valeur propre λ, généralement noté E_λ, est $E_\lambda = \mathrm{Ker}(f - \lambda\mathrm{id})$. C'est donc l'ensemble des vecteurs propres associés à λ, ajoutés de 0.

Ainsi, si f est diagonale dans une base $\mathcal{B}$, les coefficients diagonaux sont (toutes) les valeurs propres, éventuellement répétées, de f, et les vecteurs de la base $\mathcal{B}$ sont des vecteurs propres associées à ces valeurs propres. Par conséquent, pour diagonaliser un endomorphisme, la première chose à faire est de trouver les valeurs propres, puis une base du sous-espace propre associé.

Méthode générale pour trouver les valeurs propres
On résout l'équation à paramètre $f(x) - \lambda x = 0$. Si on dispose de la matrice A de f dans une certaine base, cela revient à résoudre un système $(A - \lambda I_n)X = 0$, donc un système linéaire de n équations à n inconnues, avec un paramètre λ
On cherche les paramètres λ pour lesquels ce système n'admet pas que 0 comme solution, c'est-à-dire pour lesquels la solution n'est pas unique, donc pour lesquels le système n'est pas de Cramer. Ainsi, on recherche les paramètres λ pour lesquels $A - \lambda I_n$ n'est pas inversible.

- Si $n = 2$, on a un critère d'inversiblité donné par le déterminant, et est très efficace dans le cas présent.
- Si $n > 2$, on étudie l'inversibilité en effectuant un pivot de Gauss sur la matrice $A - \lambda I_n$. Le principe sera le suivant : on recherche les valeurs de λ pour lesquels cette matrice est inversible, ce qui impose qu'il y ait un pivot (non nul) sur chaque colonne. L'existence de ce pivot nous amène, au cours du pivot, à supposer la non nullité de certaines expression, et donc d'exclure certaines valeurs de λ, en nombre fini. Ces valeurs λ sont les seules valeurs propres *possibles* de f, ce qui ne signifie pas qu'elles sont effectivement des valeurs propres. Il faut ensuite résoudre le système associé à chacune de ces valeurs, pour s'assurer que 0 n'est pas la seule solution. Remarquez qu'on sait trouver une base de l'ensemble des solutions d'un tel système, donc **une base de l'espace propre associé à chacune des valeurs propres**.

EXEMPLE 6.1.3 Trouver les valeurs propres de f canoniquement associée à $\begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}$, et donner une base des espaces propres correspondant.

Exemple 6.1.4 Même question avec f de matrice $\begin{pmatrix} 3 & -4 & 4 \\ 1 & -1 & 8 \\ 0 & 0 & 2 \end{pmatrix}$.

Exemple 6.1.5 Un endomorphisme sur un espace vectoriel réel peut ne pas admettre de valeur propre (réelle). Exemple : f canoniquement associé à $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Cas des matrices triangulaires (inférieures ou supérieures)

Théorème 6.1.6 *Soit M une matrice triangulaire, alors les valeurs propres de f canoniquement associée à M sont exactement les coefficients diagonaux de M*

Exemple 6.1.7 $\operatorname{Spec}\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix} = \{1, 2\}$.

Proposition 6.1.8 *Un endomorphisme diagonalisable n'ayant qu'une valeur propre est une homothétie*

Corollaire 6.1.9 *Il existe des endomorphismes non diagonalisables.*

Exemple 6.1.10 Soit f de matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Alors la seule valeur propre de f est 1, mais f n'est pas une homothétie. Donc f n'est pas diagonalisable, d'après la propriété précédente.

6.1.3 Etude des sous-espaces propres

Théorème 6.1.11 *Les sous-espaces propres sont en somme directe :* $\displaystyle\sum_{\lambda\in\operatorname{Spec}(f)} E_\lambda = \bigoplus_{\lambda\in\operatorname{Spec}(f)} E_\lambda$.

Théorème 6.1.12 *Soit $\lambda \in \operatorname{Spec}(f)$. Alors E_λ est stable par f.*

Corollaire 6.1.13 *Soit $\lambda \in \operatorname{Spec}(f)$. Alors f définit par restriction un endomorphisme de $\mathcal{L}(E_\lambda)$. Cette restriction est égale à $\lambda\mathrm{id}_{E_\lambda}$.*

Corollaire 6.1.14 *Soit $F = \displaystyle\bigoplus_{\lambda\in\operatorname{Spec}(f)}$. Alors F est stable par f. Soit g la restriction de f en un endomorphisme de F. Soit $\operatorname{Spec}(f) = \{l_1, \ldots, \lambda_k\}$, et soit pour tout $i \in [\![1, k]\!]$, n_i la dimension de E_λ, et $\mathcal{B}_i$ une base de E_λ. Enfin, on note $\mathcal{B}$ la base de F, $\mathcal{B} = (\mathcal{B}_1, \ldots, \mathcal{B}_k)$, obtenue en juxtaposant les bases $\mathcal{B}_i$. Alors, en adoptant la notation par blocs :*

$$[g]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 I_{n_1} & 0 & \ldots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_k I_{n_k} \end{pmatrix}$$

Il s'agit d'une matrice diagonale dont les coefficients diagonaux sont les λ_i, répétés chacun n_i fois.

6.1.4 Critères de diagonalisation

THÉORÈME 6.1.15 *Les propositions suivantes sont équivalentes :*

1. $\sum_{\lambda \in \mathrm{Spec}(f)} \dim E_\lambda = \dim E$;
2. f *est diagonalisable ;*
3. f *est diagonalisable dans une base de vecteurs propres ;*

COROLLAIRE 6.1.16 *(E de dimension n)*

1. f *admet au plus n valeurs propres distinctes.*
2. *Si f admet n valeurs propres distinctes, alors f est diagonalisable.*

6.1.5 Polynômes annulateurs

DÉFINITION 6.1.17 Un *polynôme annulateur de f* est un polynôme $P \in \mathbb{K}[X]$ tel que $P(f) = 0$, les puissances de f étant les puissances de composition.

THÉORÈME 6.1.18 *Soit P un polynôme annulateur de f. Alors toute valeur propre de f est racine de P. La réciproque est fausse.*

Cela fournit une autre méthode de recherche des valeurs propres : on trouve un polynôme annulateur, cela nous permet de nous restreindre à un nombre fini de valeurs propres possibles pour f, à savoir les racines de ce polynôme. Il faut ensuite étudier chacune de ces racines pour savoir si oui ou non elles sont valeurs propres.

EXEMPLE 6.1.19 Valeurs propres des projecteurs et des symétries, et diagonalisation.

6.1.6 Méthode de diagonalisation (Bilan)

Je résume la méthode pour diagonaliser un endomorphisme ($\dim E = n$)

1. **Rechercher les valeurs propres**
   - A-t-on facilement une base dans laquelle la matrice de f est triangulaire ?
   - A-t-on de manière évidente un polynôme annulateur ?
   - Sinon, à quelle condition sur λ le système $(f - \lambda \mathrm{id})(x) = 0$ est-il de Cramer ? (déterminant si $\dim E = 2$, pivot si $\dim E > 2$)
2. **Diagonalisabilité**
   - A-t-on n valeurs propres distinctes ? Si oui, f est diagonalisable. Cela ne donne que la diagonalisabilité ; si on veut une base de diagonalisation, il faut aussi faire les étapes suivantes.
   - Pour toute valeur propre, trouver une base de E_λ, et donc sa dimension, par la récolution d'un système linéaire.
   - Si $\sum_{\lambda \in \mathrm{Spec}(f)} \dim E_\lambda < n$, alors f n'est pas diagonalisable.
   - Si $\sum_{\lambda \in \mathrm{Spec}(f)} \dim E_\lambda = n$, alors f est diagonalisable.
3. **Diagonalisation** (le cas échéant)
   - Décrire la base de diagonalisation, obtenue en juxtaposant les bases des espaces propres.
   - Donner la matrice (diagonale) de f dans cette base.

6.2 Diagonalisation des matrices carrées

6.2.1 Matrices semblables

DÉFINITION 6.2.1 Deux matrices A et B de $\mathcal{M}_n(\mathbb{K})$ sont semblables s'il existe $P \in \mathrm{GL}_n(\mathbb{K})$ tel que $A = P^{-1}BP$.

PROPOSITION 6.2.2 *Il s'agit d'une relation d'équivalence.*

REMARQUE 6.2.3 Lien avec les changements de base.

DÉFINITION 6.2.4 On dit que $A \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable si A est semblable à une matrice diagonale, donc s'il existe $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $D = P^{-1}AP$ soit diagonale.

Diagonaliser A consiste à :

1. donner la matrice diagonale D ;
2. donner la matrice de passage P ;
3. rappeler l'égalité $D = P^{-1}AP$.

Dans ce qui suit, A est une matrice de $\mathcal{M}_n(\mathbb{K})$ et f est l'endomorphisme de $\mathcal{L}(\mathbb{K}^n)$ canoniquement associé à A.

6.2.2 Principes et critères de diagonalisation

La diagonalisation de A est équivalente à la diagonalisation de f. En effet :

- S'il existe P telle que $D = P^{-1}AP$ soit diagonale : P est une matrice inversible, donc une matrice de passage, plus exactement la matrice de passage de la base canonique à la base $\mathcal{B}$ formée des colonnes de P. Ainsi :

  $$D = P^{-1}AP = [b.c. \to \mathcal{B}]^{-1}[f]_{b.c.}[b.c. \to \mathcal{B}] = [f]_{\mathcal{B}}.$$

  Par conséquent, on a trouvé une base $\mathcal{B}$ dans laquelle la matrice de f est diagonale.
- Réciproquement, si on a diagonalisé f, donc trouvé une base $\mathcal{B}$ dans laquelle la matrice D de f est diagonale, alors il suffit de poser $P = [b.c. \to \mathcal{B}]$ pour avoir la relation de changement de base : $D = P^{-1}AP$. Cela fournit la diagonalisation de A.

On définit donc de même que pour les endomorphismes :

DÉFINITION 6.2.5 1. Une *valeur propre de* A est $\lambda \in \mathbb{K}$ tel que $A - \lambda I_n$ est non inversible.

2. $\mathrm{Spec}(A)$ est l'ensemble des valeurs propres de A.
3. Un *vecteur propre* $X \in \mathbb{K}^n$ associé à la valeur propre λ est un vecteur non nul tel que $AX = \lambda X$.
4. Le *sous-espace propre* E_λ associé à la valeur propre λ est l'ensemble des vecteurs propres, plus 0 : $E_\lambda = \{X \in \mathbb{K}^n \mid AX = \lambda X\}$.

Les critères de diagonalisation, ainsi que les méthodes sont les mêmes. Notamment :

1. Si A est triangulaire, les valeurs propres de A sont les coefficients diagonaux.
2. Si A admet n valeurs propres distinctes, alors A est diagonalisable.

3. A diagonalisable $\iff \bigoplus_{\lambda \in \mathrm{Spec}(A)} E_\lambda = \mathbb{K}^n \iff \sum_{\lambda \in \mathrm{Spec}(A)} \dim E_\lambda = n$.
4. Soit $P \in \mathbb{K}[X]$. Si $P(A) = 0$, alors toute valeur propre de A est racine de P.

6.2.3 Cas des matrices 2×2

THÉORÈME 6.2.6 *Toute matrice M de $\mathcal{M}_2(\mathbb{C})$ est :*

1. *soit égale à λI_2, pour une certaine valeur $\lambda \in \mathbb{C}$;*
2. *soit semblable à une matrice $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, où $\lambda_1 \neq \lambda_2$ sont deux complexes ;*
3. *soit semblable à une matrice $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, $\lambda \in \mathbb{C}$;*

ces trois possibilités étant exclusives l'une de l'autre.

Les cas 1 et 2 correspondent aux cas où M est diagonalisable. Les cas 1 et 3 correspondent aux cas où M admet une unique valeur propre. Le cas 2 correspond au cas où M admet deux valeurs propres distinctes λ_1 et λ_2.

6.2.4 Une application : suites définies par une récurrence linéaire

Soit $(u_n)_{n\in\mathbb{N}}$ une suite définie par une récurrence d'ordre p : $\forall n \geqslant 0,\ u_{n+p} = a_{p-1}u_{n+p-1} + \cdots + a_0 u_n$. Cette relation peut s'écrire matriciellement. Soit :

$$\forall n \in \mathbb{N},\ U_n = \begin{pmatrix} u_{n+p-1} \\ u_{n+p-2} \\ \vdots \\ u_n \end{pmatrix} \qquad \text{et} \qquad M = \begin{pmatrix} a_{p-1} & a_{p-2} & \cdots & \cdots & a_0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & 0 & \vdots & \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

Alors, pour tout $n \geqslant 0$, $U_{n+1} = MU_n$, donc $U_n = M^n U_0$
Pour expliciter la suite U_n, on peut donc diagonaliser M, si elle est diagonalisable, pour calculer ses puissances (remarquez que la dernière ligne de M^n suffit, économisez-vous les calculs)

PROPOSITION 6.2.7 *Les valeurs propres de M sont les racines du polynôme caractéristique.*

COROLLAIRE 6.2.8 *Si les racines du polynôme caractéristique sont simples, M est diagonalisable, et (u_n) est une combinaison linéaire de suites géométriques de raisons ces racines.*

EXEMPLE 6.2.9 Cas d'une récurrence d'ordre 2 : cas de deux racines simples ; d'une racine double.