



Daniel FREDON  
Myriam MAUMY-BERTRAND  
Frédéric BERTRAND

# Mathématiques

## Algèbre et géométrie

### en 30 fiches

**Comprendre  
et s'entraîner  
facilement**

DUNOD

Daniel FREDON

Myriam MAUMY-BERTRAND

Frédéric BERTRAND

# Mathématiques

Algèbre et géométrie  
**en 30 fiches**

DUNOD

# Consultez nos parutions sur [dunod.com](http://dunod.com)



Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage.

Le Code de la propriété intellectuelle du 1<sup>er</sup> juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements



d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée. Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du Centre français d'exploitation du droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).

© Dunod, Paris, 2009  
ISBN 978-2-10-053932-1

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2<sup>e</sup> et 3<sup>e</sup> al), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

# Avant-propos

L'organisation en crédits d'enseignement entraîne des variations entre les Universités.

Les deux premières années de licence (L1 et L2) ont cependant suffisamment de points communs pour proposer des livres utiles à tous.

Avec la collection Express, vous allez vite à l'essentiel.

Pour aller vite, il faut la taille mince et le prix léger.

Il faut aussi une organisation en fiches courtes et nombreuses pour vous permettre de ne retenir que les sujets du moment, semestre après semestre.

Il faut avoir fait des choix cohérents et organisés de ce qui est le plus couramment enseigné lors des deux premières années des licences de mathématiques, informatique, mais aussi de sciences physiques, et dans les cycles préparatoires intégrés.

Il faut un index détaillé pour effacer rapidement un malencontreux trou de mémoire.

Dans la collection Express, il y a donc l'essentiel, sauf votre propre travail. Bon courage !

Toutes vos remarques, vos commentaires, vos critiques, et même vos encouragements, seront accueillis avec plaisir.

daniel.fredon@laposte.net  
mmaumy@math.u-strasbg.fr  
fbertran@math.u-strasbg.fr

# Table des matières

## Partie 1 : Raisonnement et algèbre générale

|          |                                      |    |
|----------|--------------------------------------|----|
| Fiche 1  | Logique et raisonnement              | 6  |
| Fiche 2  | Langage des ensembles                | 12 |
| Fiche 3  | Applications                         | 16 |
| Fiche 4  | Relations binaires                   | 20 |
| Fiche 5  | Entiers naturels                     | 24 |
| Fiche 6  | Groupes                              | 26 |
| Fiche 7  | Anneaux et corps                     | 32 |
| Fiche 8  | Arithmétique dans $\mathbb{Z}$       | 36 |
| Fiche 9  | Nombres complexes                    | 42 |
| Fiche 10 | Nombres complexes et géométrie plane | 48 |
| Fiche 11 | Polynômes                            | 52 |
| Fiche 12 | Fractions rationnelles               | 58 |

## Partie 2 : Algèbre linéaire

|          |                                       |     |
|----------|---------------------------------------|-----|
| Fiche 13 | Systèmes linéaires                    | 62  |
| Fiche 14 | Espaces vectoriels                    | 66  |
| Fiche 15 | Espaces vectoriels de dimension finie | 72  |
| Fiche 16 | Applications linéaires                | 78  |
| Fiche 17 | Applications linéaires particulières  | 86  |
| Fiche 18 | Calcul matriciel                      | 90  |
| Fiche 19 | Matrices et applications linéaires    | 96  |
| Fiche 20 | Déterminants                          | 102 |
| Fiche 21 | Diagonalisation des endomorphismes    | 108 |

|                 |                              |     |
|-----------------|------------------------------|-----|
| <b>Fiche 22</b> | Espaces préhilbertiens       | 114 |
| <b>Fiche 23</b> | Orthogonalité                | 120 |
| <b>Fiche 24</b> | Groupe orthogonal            | 126 |
| <b>Fiche 25</b> | Matrices symétriques réelles | 132 |

## Partie 3 : Géométrie

|                 |                                 |     |
|-----------------|---------------------------------|-----|
| <b>Fiche 26</b> | Calcul vectoriel et distances   | 134 |
| <b>Fiche 27</b> | Coniques                        | 138 |
| <b>Fiche 28</b> | Courbes paramétrées             | 144 |
| <b>Fiche 29</b> | Courbes en coordonnées polaires | 150 |
| <b>Fiche 30</b> | Longueur des arcs, courbure     | 154 |
| <b>Index</b>    |                                 | 159 |

# Logique et raisonnement

## I Logique binaire

### • Proposition logique

C'est un assemblage de lettres et de signes qui a une syntaxe correcte (le lecteur sait le lire), une sémantique correcte (le lecteur comprend ce qu'il lit) et qui a une seule valeur de vérité : vrai (V) ou faux (F).

Deux propositions seront considérées comme égales si elles ont toujours la même valeur de vérité.

### • Connecteurs logiques

À partir de propositions  $p, q, \dots$  on peut former de nouvelles propositions définies par des tableaux de vérité.

– Négation : non  $p$  (noté aussi  $\neg p$ )

| $p$ | non $p$ |
|-----|---------|
| V   | F       |
| F   | V       |

– Conjonction :  $p$  et  $q$  (noté aussi  $p \wedge q$ )

– Disjonction :  $p$  ou  $q$  (noté aussi  $p \vee q$ )

– Implication :  $p \implies q$

– Équivalence :  $p \iff q$

| $p$ | $q$ | $p$ et $q$ | $p$ ou $q$ | $p \implies q$ | $p \iff q$ |
|-----|-----|------------|------------|----------------|------------|
| V   | V   | V          | V          | V              | V          |
| V   | F   | F          | V          | F              | F          |
| F   | V   | F          | V          | V              | F          |
| F   | F   | F          | F          | V              | V          |

Le « ou » a un sens inclusif, à ne pas confondre avec le sens exclusif qui figure dans « fromage ou dessert », c'est-à-dire du fromage ou bien du dessert mais pas les deux.

- **Propriétés des connecteurs**

$$\text{non}(\text{non } p) = p$$

$$\text{non}(p \text{ ou } q) = (\text{non } p) \text{ et } (\text{non } q)$$

$$\text{non}(p \text{ et } q) = (\text{non } p) \text{ ou } (\text{non } q)$$

$$(p \implies q) = [(\text{non } p) \text{ ou } q]$$

$$\text{non}(p \implies q) = [p \text{ et } (\text{non } q)]$$

La négation d'une implication n'est donc pas une implication.

$$(p \implies q) = [(\text{non } q) \implies (\text{non } p)]$$

Cette seconde implication est la contraposée de la première. Faites attention à l'ordre des propositions.

$$(p \iff q) = [(p \implies q) \text{ et } (q \implies p)]$$

Pour démontrer une équivalence, on démontre souvent une implication et sa réciproque.

## II Quantificateurs

- **Notation**

Les quantificateurs servent à indiquer la quantité d'éléments qui interviennent dans une proposition. On utilise :

– le quantificateur universel  $\forall$

$\forall x$  signifie : pour tout  $x$  ;

– le quantificateur existentiel  $\exists$

$\exists x$  signifie : il existe au moins un  $x$ .

- **Ordre**

Si l'on utilise deux fois le même quantificateur, l'ordre n'a pas d'importance.

On peut permuter les quantificateurs dans des écritures du type :

$$\forall x \in E \quad \forall y \in E \quad p(x, y)$$

$$\exists x \in E \quad \exists y \in E \quad p(x, y)$$

Mais si les quantificateurs sont différents, leur ordre est important.

Dans l'écriture  $\forall x \in E \quad \exists y \in E \quad p(x, y)$   $y$  dépend de  $x$ .

Dans l'écriture  $\exists y \in E \quad \forall x \in E \quad p(x, y)$   $y$  est indépendant de  $x$ .

- **Négation**

La négation de «  $\forall x \in E, x \text{ vérifie } p$  » est «  $\exists x \in E$  tel que  $x$  ne vérifie pas  $p$  ».

La négation de «  $\exists x \in E, x \text{ vérifie } p$  » est «  $\forall x \in E, x \text{ ne vérifie pas } p$  ».

### III Quelques méthodes de démonstration

- **Dédution**

Si  $p$  est vraie et si l'on démontre  $(p \implies q)$ , alors on peut conclure que  $q$  est vraie.

Si la démonstration d'une implication vous résiste, pensez à examiner la contraposée. Elle a le même sens, mais il est possible que sa démonstration soit plus facile.

- **Raisonnement par l'absurde**

Pour démontrer que  $p$  est vraie, on peut supposer que  $p$  est fausse et en déduire une contradiction.

Comme vous partez de « non  $p$  », ne vous trompez pas dans la négation, en particulier en ce qui concerne les quantificateurs.

- **Disjonction des cas**

Elle est basée sur le fait que :

$$[(p \implies q) \text{ et } (\text{non } p \implies q)] \implies q.$$

- **Exemples et contre-exemples**

Beaucoup de propositions mathématiques sont de type universel. Dans ce cas,

- un exemple est une illustration, mais ne démontre rien,
- un contre-exemple démontre que la proposition est fausse.

- **Raisonnement par récurrence**

Voir la fiche 5.

## Application

Les questions qui suivent sont indépendantes. Elles ont pour but de faire fonctionner diverses méthodes de raisonnement.

1. Démontrez que, si  $x$  est un réel positif, alors  $\frac{x+1}{x+2} < \frac{x+3}{x+4}$ .

2. Démontrez que la somme d'un rationnel et d'un irrationnel est irrationnelle.

3. Soit  $n \in \mathbb{N}$ . Démontrez que :

$$n \text{ pair} \iff n^2 \text{ pair.}$$

4. Démontrez que, pour tout réel  $x$ , si  $x^2 - 9 > 0$ , alors  $x^2 - x - 2 > 0$ .

5. Écrivez la négation de la proposition :

*Il existe une ville de France dans laquelle toute place comporte au moins une agence bancaire.*

6. Rétablissez la forme affirmative d'une ancienne publicité :

*Si vous n'êtes pas moderne, alors vous n'êtes pas client de la Société Générale.*

## Solution

### 1. Équivalences logiques successives

Les propositions suivantes sont toutes équivalentes :

$$\frac{x+1}{x+2} < \frac{x+3}{x+4}$$

$$\iff (x+1)(x+4) < (x+2)(x+3) \quad \text{car } (x+2)(x+4) > 0$$

$$\iff x^2 + 5x + 4 < x^2 + 5x + 6$$

$$\iff 4 < 6.$$

La dernière proposition étant vraie, toutes les propositions précédentes sont vraies, et l'inégalité de l'énoncé est démontrée.

### 2. Raisonnement par l'absurde

Considérons deux réels  $x$  et  $y$  tels que  $x \in \mathbb{Q}$  et  $y \notin \mathbb{Q}$ .

Supposons que  $x + y$  soit rationnel. Dans ce cas,  $(x + y) - x = y$  serait rationnel, alors qu'on sait que  $y \notin \mathbb{Q}$ .

On obtient ainsi une contradiction, et on doit rejeter l'hypothèse qui vient d'être formulée, c'est-à-dire conclure que  $x + y$  est irrationnel.

### 3. Implication et contraposée

- Montrons que :  $n$  pair  $\implies n^2$  pair.

Si  $n$  est pair, il existe  $k \in \mathbb{N}$  tel que  $n = 2k$ . On a alors  $n^2 = 4k^2 = 2(2k^2)$  avec  $2k^2 \in \mathbb{N}$ .  $n^2$  est donc pair.

- Montrons que  $n^2$  pair  $\implies n$  pair en utilisant la contraposée, c'est-à-dire en démontrant que :  $n$  impair  $\implies n^2$  impair.

Si  $n$  est impair, il existe  $k \in \mathbb{N}$  tel que  $n = 2k + 1$ .

On a alors  $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$  avec  $2k^2 + 2k \in \mathbb{N}$ .

$n^2$  est donc impair.

### 4. Raisonnement par disjonction de cas

L'hypothèse  $x^2 - 9 > 0$  se décompose en deux cas.

- Si  $x > 3$ , alors  $x^2 - x - 2 = (x - 2)(x + 1)$  est le produit de deux facteurs strictement positifs, donc  $x^2 - x - 2 > 0$ .
- Si  $x < -3$ , alors  $x^2 - x - 2 = (x - 2)(x + 1)$  est le produit de deux facteurs strictement négatifs, donc  $x^2 - x - 2 > 0$ .

### 5. Négation de quantificateurs

Dans toute ville de France, il existe au moins une place qui ne comporte pas d'agence bancaire.

### 6. Publicité et contraposée

En terme de logique, la publicité citée est l'implication :

$$\text{non moderne} \implies \text{non client.}$$

Elle a le même sens que sa contraposée :

$$\text{client} \implies \text{moderne}$$

c'est-à-dire que tous les clients de la Société Générale sont modernes (qualicatif censé être à valeur positive).

Si un lecteur se trompe et pense que les clients des autres banques ne sont pas modernes, le message est plus fort et diffamatoire, mais ce n'est pas ce qui a été dit !

Et des psychologues disent qu'avoir à rétablir une forme affirmative conduit à mieux adhérer au message !

De bonnes bases de logique sont donc utiles pour ne pas se faire manipuler.

## Application

Extrait d'un concours ESIEE ; réponse par QCM, le nombre de réponses exactes n'est pas fixé.

Soit un ensemble de 50 animaux qui sont soit mâle soit femelle, soit carnivore soit herbivore.

On considère les énoncés suivants :

$P$  : tout mâle est carnivore ;

$Q$  : il existe un mâle carnivore et il existe une femelle carnivore ;

alors dans l'ensemble des 50 animaux :

1. pour prouver que  $P$  est vrai, il suffit de vérifier que tous les herbivores sont des femelles ;
2. pour prouver que  $P$  est faux, il est nécessaire de vérifier que tous les mâles sont herbivores ;
3. pour prouver que  $Q$  est vrai, il suffit de trouver une femelle carnivore ;
4. pour prouver que  $Q$  est vrai, il est nécessaire de trouver une femelle carnivore ;
5. pour prouver que  $Q$  est faux, il est nécessaire de vérifier que les 50 animaux sont herbivores.

## Solution

Réponses vraies : **1. 4.**

1. est vraie car la contraposée de  $P$  est « tout herbivore est une femelle ».

Pour prouver que  $P$  est faux, il suffit de trouver un mâle herbivore, ce qui montre que

2. est fausse.

Parmi les 50 animaux, il peut y avoir 49 mâles herbivores et une femelle carnivore.

Dans ce cas,  $Q$  est faux, ce qui montre que les affirmations **3.** et **5.** sont fausses.

## I Ensembles

## • Notion d'ensemble

La notion d'ensemble est considérée comme primitive. Retenons que la caractérisation d'un ensemble  $E$  doit être nette, c'est-à-dire que, pour tout élément  $x$ , on doit pouvoir affirmer : ou bien qu'il est dans  $E$  ( $x \in E$ ), ou bien qu'il n'y est pas ( $x \notin E$ ).

On note  $\emptyset$  l'ensemble vide, c'est-à-dire l'ensemble qui ne contient aucun élément.  $E$  et  $F$  étant des ensembles, on dit que  $E$  est inclus dans  $F$  si, et seulement si, tous les éléments de  $E$  appartiennent aussi à  $F$ . On note  $E \subset F$ .

On dit aussi que  $E$  est une partie de  $F$ , ou que  $F$  contient  $E$ .

L'ensemble des parties de  $E$  se note  $\mathcal{P}(E)$ . Dire que  $A \in \mathcal{P}(E)$  signifie que  $A \subset E$ .

• Opérations dans  $\mathcal{P}(E)$ 

Soit  $E$  un ensemble.  $A$  et  $B$  étant des parties de  $E$ , on définit :

– le complémentaire de  $A$  dans  $E$  :  $\bar{A} = \{x \in E ; x \notin A\}$  ;

– l'intersection de  $A$  et de  $B$  :  $A \cap B = \{x \in E ; x \in A \text{ et } x \in B\}$  ;

Si  $A \cap B = \text{card } \emptyset$ , c'est-à-dire s'il n'existe aucun élément commun à  $A$  et  $B$ , on dit que les parties  $A$  et  $B$  sont disjointes ;

– la réunion de  $A$  et de  $B$  :  $A \cup B = \{x \in E ; x \in A \text{ ou } x \in B\}$ .

Ce « ou » a un sens inclusif c'est-à-dire que  $A \cup B$  est l'ensemble des éléments  $x$  de  $E$  qui appartiennent à l'une au moins des parties  $A$  et  $B$ .

– la différence :  $A \setminus B = \{x \in E ; x \in A \text{ et } x \notin B\} = A \cap \bar{B}$  ;

– la différence symétrique :

$$A \Delta B = (A \cup B) \setminus (A \cap B) = (A \cap \bar{B}) \cup (\bar{A} \cap B).$$

$A \Delta B$  est l'ensemble des éléments qui appartiennent à une, et une seule, des parties  $A$  et  $B$ .

## • Recouvrement, partition

Un recouvrement d'une partie  $A$  de  $E$  est une famille de parties de  $E$  dont la réunion contient  $A$ .

Une partition d'un ensemble  $E$  est une famille de parties non vides de  $E$ , deux à deux disjointes, et dont la réunion est  $E$ .

## II Propriétés des opérations dans $\mathcal{P}(E)$

Pour toutes parties  $A$ ,  $B$  et  $C$  de  $E$ , on a les propriétés qui suivent.

- **Complémentaire**

$$\overline{E} = \text{card } \emptyset \quad ; \quad \overline{\text{card } \emptyset} = E \quad ; \quad \overline{\overline{A}} = A \quad ; \quad \text{si } A \subset B \text{ alors } \overline{B} \subset \overline{A}.$$

- **Lois de de Morgan**

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \quad ; \quad \overline{A \cup B} = \overline{A} \cap \overline{B}.$$

- **Réunion**

$$A \cup B = B \cup A \quad ; \quad A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \cup A = A \quad ; \quad A \cup \text{card } \emptyset = A \quad ; \quad A \cup E = E.$$

- **Intersection**

$$A \cap B = B \cap A \quad ; \quad A \cap (B \cap C) = (A \cap B) \cap C ;$$

$$A \cap A = A \quad ; \quad A \cap \text{card } \emptyset = \text{card } \emptyset \quad ; \quad A \cap E = A.$$

- **Réunion et intersection**

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) ;$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

## III Produit cartésien

Le produit des ensembles  $A$  et  $B$  est l'ensemble, noté  $A \times B$ , des couples  $(a, b)$  où  $a \in A$  et  $b \in B$ .

Attention, le couple  $(b, a)$  est différent du couple  $(a, b)$ , sauf si  $a = b$ .

Plus généralement, le produit cartésien de  $n$  ensembles  $E_i$  est :

$$E_1 \times \cdots \times E_n = \{(x_1, \dots, x_n) \mid x_1 \in E_1, \dots, x_n \in E_n\}.$$

Si  $E_1 = \cdots = E_n = E$ , on le note  $E^n$ .

## Application

Soit  $E$  un ensemble. Caractérisez les parties  $A, B, C$  de  $E$  telles que :

$$A \cup (B \cap C) = (A \cup B) \cap C.$$

## Solution

On cherche une condition nécessaire et suffisante sur  $(A, B, C)$  élément de  $(\mathcal{P}(E))^3$  pour que :

$$A \cup (B \cap C) = (A \cup B) \cap C \quad (1).$$

Supposons la condition (1). On a alors  $A \subset A \cup (B \cap C) \subset C$ . Par conséquent,  $A \subset C$  est une condition nécessaire pour que l'on ait (1).

Réciproquement, supposons que  $A \subset C$ . On a alors :

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C) = A \cup (B \cap C),$$

ce qui est la condition (1).

Une condition nécessaire et suffisante pour que l'on ait (1) est donc  $A \subset C$ .

## Application

Soit  $E$  un ensemble, et  $A, B, C$  trois parties de  $E$  telles que :

$$A \cup B \subset A \cup C \quad \text{et} \quad A \cap B \subset A \cap C.$$

Comparez  $B$  et  $C$ .

## Solution

Supposons que

$$\begin{cases} A \cup B \subset A \cup C & (1) \\ A \cap B \subset A \cap C & (2). \end{cases}$$

Quelques essais vous permettront d'imaginer que  $B \subset C$  ; mais il faut le démontrer.

Soit  $x \in B$  ; montrons que  $x \in C$ .

Si  $x \in A$ , alors  $x \in A \cap B$ . De l'inclusion (2), on déduit que  $x \in A \cap C$ , donc  $x \in C$ .

Si  $x \notin A$ , comme  $x$  appartient à  $A \cup B$ , donc à  $A \cup C$  d'après (1), on obtient encore  $x \in C$ .

## Application

Extrait d'un concours ESIEE ; réponse par QCM, le nombre de réponses exactes n'est pas fixé.

Soit  $\mathcal{E} = \{1, 2, 3, 4\}$ . Si  $X$  est un sous-ensemble de  $\mathcal{E}$ , on note  $\overline{X}$  le complémentaire de  $X$  dans  $\mathcal{E}$ .

Pour tous sous-ensembles  $X, Y, Z$  de  $\mathcal{E}$ , différents du vide et de  $\mathcal{E}$ , on a :

1. si  $X \cap Y \neq \emptyset$  et  $Y \cap \overline{Z} = \emptyset$  alors  $X \cap Z \neq \emptyset$  ;
2. si  $X \subset Y$  et  $\overline{Y} \cap Z = \emptyset$  alors  $\overline{X} \cap Z = \emptyset$  ;
3. si  $\overline{X} \cap \overline{Y} \neq \emptyset$  et  $\overline{Z} \subset \overline{Y}$  alors  $\overline{X} \cap \overline{Z} \neq \emptyset$  ;
4. si  $\overline{X} \cap Y = \emptyset$  et  $Y \cap Z \neq \emptyset$  alors  $X \cap Z \neq \emptyset$  ;
5. si  $\overline{X} \subset Y$  et  $Y \cap Z \neq \emptyset$  alors  $\overline{X} \subset Z$ .

## Solution

Réponses vraies : **1. 4.**

Si  $Y \cap \overline{Z} = \emptyset$ , on a  $Y \subset Z$ , donc  $X \cap Y \subset X \cap Z$ . Si  $X \cap Y \neq \emptyset$ , on a donc  $X \cap Z \neq \emptyset$ , donc **1.** est vraie.

Le contre-exemple  $X = \{1\}$ ,  $Y = \{1, 2, 3\}$ ,  $Z = \{1, 2\}$  montre que **2.** est fausse.

Le contre-exemple  $X = \{1, 2\}$ ,  $Y = \{1, 3\}$ ,  $Z = \{1, 3, 4\}$  montre que **3.** est fausse.

Si  $\overline{X} \cap Y = \emptyset$ , on a  $Y \subset X$ , donc  $Y \cap Z \subset X \cap Z$ . Si  $Y \cap Z \neq \emptyset$ , on a donc  $X \cap Z \neq \emptyset$ , donc **4.** est vraie.

Le contre-exemple  $X = \{1, 2\}$ ,  $Y = \{1, 3, 4\}$ ,  $Z = \{4\}$  montre que **5.** est fausse.

## I Généralités

### • Définitions

Une application  $f$  est définie par son ensemble de départ  $E$ , son ensemble d'arrivée  $F$ , et une relation qui permet d'associer à tout  $x \in E$  un élément unique  $y$  dans  $F$ . On le note  $f(x)$ .

Les applications de  $E$  dans  $F$  forment un ensemble noté  $\mathcal{F}(E, F)$ .

L'application identité de  $E$  est l'application de  $E$  dans  $E$  définie par  $x \mapsto x$ . On la note  $Id_E$ .

### • Restriction, prolongement

Soit  $f$  une application de  $A$  dans  $F$ , et  $g$  une application de  $B$  dans  $F$ .

Si  $A \subset B$  et si, pour tout  $x$  de  $A$ , on a  $f(x) = g(x)$ , on dit que  $f$  est une restriction de  $g$ , ou que  $g$  est un prolongement de  $f$ .

### • Composition des applications

Soit  $E, F, G$  trois ensembles,  $f$  une application de  $E$  dans  $F$ ,  $g$  une application de  $F$  dans  $G$ .

La composée de  $f$  et de  $g$  est l'application de  $E$  dans  $G$  définie par :

$$x \mapsto g(f(x)) = (g \circ f)(x).$$

## II Injections, surjections, bijections

### • Application injective

Une application  $f$  de  $E$  dans  $F$  est dite injective (ou est une injection) si elle vérifie l'une des deux propriétés équivalentes :

$$\forall x \in E \quad \forall x' \in E \quad x \neq x' \implies f(x) \neq f(x')$$

$$\forall x \in E \quad \forall x' \in E \quad f(x) = f(x') \implies x = x'.$$

Ne confondez pas avec la définition d'une application qui s'écrit :

$$\forall x \in E \quad \forall x' \in E \quad x = x' \implies f(x) = f(x')$$

$$\forall x \in E \quad \forall x' \in E \quad f(x) \neq f(x') \implies x \neq x'$$

- **Application surjective**

Une application  $f$  de  $E$  dans  $F$  est dite surjective (ou est une surjection) si tout élément  $y$  de  $F$  est l'image d'au moins un élément  $x$  de  $E$ , soit :

$$\forall y \in F \quad \exists x \in E \quad y = f(x).$$

- **Application bijective**

Une application  $f$  de  $E$  dans  $F$  est dite bijective (ou est une bijection) si elle est à la fois injective et surjective. Dans ce cas, tout élément  $y$  de  $F$  est l'image d'un, et un seul, élément  $x$  de  $E$ .

À tout  $y$  de  $F$ , on associe ainsi un  $x$  unique dans  $E$  noté  $f^{-1}(y)$ .

$f^{-1}$  est la bijection réciproque de  $f$ . On a donc :

$$x = f^{-1}(y) \iff y = f(x),$$

ce qui entraîne  $f \circ f^{-1} = Id_F$  et  $f^{-1} \circ f = Id_E$ .

- **Théorème**

Soit  $f$  une application de  $E$  dans  $F$ , et  $g$  une application de  $F$  dans  $G$ . On a les implications qui suivent.

- Si  $f$  et  $g$  sont injectives, alors  $g \circ f$  est injective.
- Si  $g \circ f$  est injective, alors  $f$  est injective.
- Si  $f$  et  $g$  sont surjectives, alors  $g \circ f$  est surjective.
- Si  $g \circ f$  est surjective, alors  $g$  est surjective.
- Si  $f$  et  $g$  sont bijectives, alors  $g \circ f$  est bijective, et  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ .

### III Image directe et image réciproque

- **Définitions**

Soit  $f$  une application de  $E$  dans  $F$ .

Si  $A \subset E$ , on appelle image de  $A$  par  $f$ , la partie de  $F$  constituée par les images des éléments de  $A$  :

$$f(A) = \{f(x) ; x \in A\}.$$

Si  $B \subset F$ , on appelle image réciproque de  $B$ , la partie de  $E$  constituée par les  $x$  dont l'image est dans  $B$  :

$$f^{-1}(B) = \{x \in E ; f(x) \in B\}.$$

- **Théorème**

$$\begin{aligned} A_1 \subset A_2 &\implies f(A_1) \subset f(A_2) ; B_1 \subset B_2 \implies f^{-1}(B_1) \subset f^{-1}(B_2) \\ f(A_1 \cup A_2) &= f(A_1) \cup f(A_2) ; f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2) ; \\ f^{-1}(B_1 \cup B_2) &= f^{-1}(B_1) \cup f^{-1}(B_2) ; f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2). \end{aligned}$$

## Application

$f, g, h$  sont trois applications de l'ensemble  $E$  dans lui-même. Montrez que :

$$g \circ f \text{ et } h \circ g \text{ bijectives} \implies f, g, h \text{ bijectives.}$$

## Solution

Supposons  $g \circ f$  et  $h \circ g$  bijectives.

De  $g \circ f$  surjective, on déduit  $g$  surjective. De  $h \circ g$  injective, on déduit  $g$  injective.

Donc  $g$  est bijective.

$g^{-1} \circ (g \circ f) = f$  est donc bijective, ainsi que  $h = (h \circ g) \circ g^{-1}$  comme composées de bijections.

## Application

Soit  $f$  l'application de  $\mathbb{R}^2$  dans  $\mathbb{R}^2$  définie par  $f(x, y) = (X, Y)$  avec :

$$\begin{cases} X &= x + y \\ Y &= 2x + y^3. \end{cases}$$

1.  $f$  est-elle surjective?

2.  $f$  est-elle injective?

## Solution

1.  $f$  est surjective si, pour tout élément  $(X, Y)$  de  $\mathbb{R}^2$ , il existe toujours  $(x, y) \in \mathbb{R}^2$  tel que  $f(x, y) = (X, Y)$ .

On a nécessairement  $x = X - y$ , puis, en reportant :

$$Y = 2(X - y) + y^3, \quad \text{soit} \quad y^3 - 2y + 2X - Y = 0.$$

La fonction  $\varphi$  définie par  $\varphi(y) = y^3 - 2y + 2X - Y$  est continue, négative lorsque  $y$  tend vers  $-\infty$ , positive lorsque  $y$  tend vers  $+\infty$ .

Il existe donc au moins un réel  $y$  tel que  $\varphi(y) = 0$ .

Comme il existe toujours  $y$  et  $x$ ,  $f$  est surjective.

2. On a  $f(1, 0) = (1, 2)$ . Existe-t-il un autre couple  $(x, y) \in \mathbb{R}^2$  tel que  $f(x, y) = (1, 2)$  ? Ceci est équivalent à :

$$x = 1 - y \quad \text{et} \quad y^3 - 2y = 0.$$

Pour obtenir un nouvel élément, il suffit de prendre  $y = \sqrt{2}$  et  $x = 1 - \sqrt{2}$ .

On obtient donc  $f(1 - \sqrt{2}, \sqrt{2}) = f(1, 0)$ .

Un exemple de deux éléments distincts ayant la même image démontre que  $f$  n'est pas injective.

## Application

Soit  $f$  une application de  $E$  dans  $E$ . Montrez que :

$$f \text{ injective} \iff \left[ \forall (X, Y) \in (\mathcal{P}(E))^2 \quad f(X \cap Y) = f(X) \cap f(Y) \right].$$

## Solution

On sait que l'on a toujours :

$$f(X \cap Y) \subset f(X) \cap f(Y).$$

Mais y a-t-il égalité ? Considérons, par exemple, la fonction  $f$ , de  $\mathbb{R}$  dans  $\mathbb{R}$ , définie par  $f(x) = x^2$ .

$$\text{On a } f([0, 1] \cap [-1, 0]) = f(\{0\}) = \{f(0)\} = \{0\}.$$

Mais  $f([0, 1]) \cap f([-1, 0]) = [0, 1]$ , ce qui montre un cas où l'inclusion est stricte.

• Supposons  $f$  injective et  $(X, Y) \in (\mathcal{P}(E))^2$ .

Soit  $z \in f(X) \cap f(Y)$ . Il existe donc  $x \in X$  tel que  $z = f(x)$ , et  $y \in Y$  tel que  $z = f(y)$ .

Comme  $f$  est injective, de  $f(x) = f(y)$ , on déduit  $x = y$ .

Cet élément appartient à la fois à  $X$  et à  $Y$ , donc à  $X \cap Y$ .

On a  $z \in f(X \cap Y)$ , ce qui prouve que  $f(X) \cap f(Y) \subset f(X \cap Y)$ , et donc  $f(X \cap Y) = f(X) \cap f(Y)$ .

• Réciproquement, supposons que :

$$\forall (X, Y) \in (\mathcal{P}(E))^2 \quad f(X \cap Y) = f(X) \cap f(Y),$$

et montrons que  $f$  est injective.

Pour ceci, considérons des éléments  $x$  et  $y$  de  $E$  tels que  $f(x) = f(y)$ , et montrons que  $x = y$ .

Soit  $X = \{x\}$  et  $Y = \{y\}$ . On a  $f(X) = \{f(x)\}$  et  $f(Y) = \{f(y)\}$ .

D'où  $f(X) \cap f(Y) = \{f(x)\} = f(X \cap Y)$  d'après l'hypothèse.

Il vient  $X \cap Y = \{x\} \cap \{y\} \neq \emptyset$ , soit  $x = y$ .  $f$  est donc injective.

## I Généralités

### • Définition

Choisir une partie  $\Gamma$  de  $E \times E$ , c'est définir une relation binaire  $\mathcal{R}$  sur  $E$ . Si  $(x, y) \in \Gamma$ , on dit que  $x$  et  $y$  sont en relation, et on note  $x\mathcal{R}y$ .

### • Propriétés

Une relation binaire  $\mathcal{R}$ , définie sur un ensemble  $E$ , est :

- réflexive si elle vérifie :  $\forall x \in E \quad x\mathcal{R}x$  ;
- symétrique si :  $\forall x \in E \quad \forall y \in E \quad x\mathcal{R}y \implies y\mathcal{R}x$  ;
- antisymétrique si elle vérifie l'une des deux propriétés équivalentes :

$$\forall x \in E \quad \forall y \in E \quad (x\mathcal{R}y \text{ et } y\mathcal{R}x) \implies x = y,$$

$$\forall x \in E \quad \forall y \in E \quad (x\mathcal{R}y \text{ et } x \neq y) \implies \text{non } (y\mathcal{R}x).$$

- transitive si elle vérifie :

$$\forall x \in E \quad \forall y \in E \quad \forall z \in E \quad (x\mathcal{R}y \text{ et } y\mathcal{R}z) \implies x\mathcal{R}z.$$

## II Relations d'équivalence

### • Définition

Une relation binaire  $\mathcal{R}$ , définie sur un ensemble  $E$ , est une relation d'équivalence si elle est, à la fois, réflexive, symétrique et transitive.

Si  $x \in E$ , on appelle classe d'équivalence de  $x$ , modulo  $\mathcal{R}$ , l'ensemble des  $y$  de  $E$  tels que  $x\mathcal{R}y$ .

### • Classes d'équivalence et partition

L'ensemble des classes d'équivalence de  $\mathcal{R}$  constitue une partition de  $E$ .

Réciproquement, si on se donne une partition de  $E$ , la relation «  $x$  et  $y$  appartiennent au même élément de la partition » est une relation d'équivalence sur  $E$ .

Si  $f$  est une application de  $E$  dans  $F$ , la relation binaire  $x\mathcal{R}x'$  définie par  $f(x) = f(x')$  est une relation d'équivalence dans  $E$ . Les classes d'équivalence sont

les images réciproques  $f^{-1}(\{y\})$  des parties à un élément de  $F$ .

# III Relations d'ordre

## • Définitions

Une relation binaire  $\mathcal{R}$ , définie dans un ensemble  $E$ , est une relation d'ordre si elle est, à la fois, réflexive, antisymétrique et transitive.

On la note  $<$ .

Une relation d'ordre  $<$  dans  $E$  est dite relation d'ordre total si deux éléments quelconques  $x$  et  $y$  de  $E$  sont toujours comparables, c'est-à-dire si l'on a  $x < y$  ou  $y < x$ .

Dans le cas contraire, l'ordre est partiel.

## Exemples

$\leq$  est un ordre total dans  $\mathbb{R}$ .  $\subset$  est un ordre partiel dans  $\mathcal{P}(E)$ .

## • Éléments particuliers

Soit  $A$  une partie d'un ensemble ordonné  $E$ .

– S'il existe un élément  $a$  de  $E$  tel que, pour tout  $x \in A$ , on ait  $x < a$ , on dit que  $a$  est un majorant de  $A$ , que  $A$  est une partie majorée de  $E$ .

De même, un élément  $b$  de  $E$  est un minorant de  $A$  si  $b < x$  pour tout  $x \in A$ . On dit alors que  $A$  est une partie minorée de  $E$ .

Une partie bornée de  $E$  est une partie qui est à la fois majorée et minorée.

– Un élément  $a$  de  $E$  est appelé plus grand élément de  $A$  si  $a \in A$  et si  $a$  est un majorant de  $A$ . Si un tel élément existe, il est unique.

De même, un élément  $b$  de  $E$  est le plus petit élément de  $A$  si  $b \in A$  et si  $b$  est un minorant de  $A$ .

– On appelle borne supérieure d'une partie majorée  $A$ , le plus petit des majorants de  $A$ , et borne inférieure d'une partie minorée  $A$  le plus grand des minorants de  $A$ .

Si ces bornes existent, elles sont uniques.

– Dans  $(\mathbb{R}, \leq)$ , pour démontrer que  $a$  est la borne supérieure de  $A$ , on démontre souvent :

- que c'est un majorant, soit  $x \leq a$  pour tout  $x \in A$  ;
- que, pour tout  $\varepsilon > 0$ ,  $a - \varepsilon$  n'est pas un majorant, c'est-à-dire qu'il existe  $x \in A$  tel que  $a - \varepsilon < x$ .

## Application

Dans  $]0, +\infty[$ , montrez que la relation  $\mathcal{R}$  définie par :

$$x \mathcal{R} y \iff x \ln y = y \ln x,$$

est une relation d'équivalence.

Pour chaque  $x$ , précisez le nombre d'éléments de sa classe d'équivalence.

## Solution

Dans  $]0, +\infty[$ , on peut écrire :

$$x \mathcal{R} y \iff \frac{\ln x}{x} = \frac{\ln y}{y} \iff f(x) = f(y),$$

où  $f$  est la fonction de  $]0, +\infty[$  dans  $\mathbb{R}$  définie par  $f(x) = \frac{\ln x}{x}$  et de classe  $\mathcal{C}^1$  sur son intervalle de définition.

$\mathcal{R}$  est donc la relation d'équivalence associée à  $f$ .

Pour préciser les classes d'équivalence, étudions les variations de  $f$ . On a :

$$\forall x \in ]0, +\infty[ \quad f'(x) = \frac{1 - \ln x}{x^2}$$

On en déduit le tableau de variation de la fonction  $f$  :

| $x$  | 0         | 1      | e                           | $+\infty$       |
|------|-----------|--------|-----------------------------|-----------------|
| $f'$ |           | +      | 0                           | —               |
| $f$  | $-\infty$ | ↗<br>0 | $\nearrow$<br>$\frac{1}{e}$ | $\searrow$<br>0 |

La lecture de ce tableau, et le théorème des valeurs intermédiaires des fonctions continues, nous permet de répondre à la question posée.

- Si  $x \in ]0, 1[$  ou si  $x = e$ , la classe d'équivalence de  $x$  est réduite à  $x$ .
- Si  $x \in ]1, e[ \cup ]e, +\infty[$ , la classe d'équivalence de  $x$  comporte deux éléments.

## Application

Dans  $\mathbb{N} \times \mathbb{N}$ , on définit la relation  $<$  par :

$$\forall (a,b) \in \mathbb{N}^2 \quad \forall (a',b') \in \mathbb{N}^2 \quad (a,b) < (a',b') \iff a \leq a' \text{ et } b \leq b'.$$

**1.** Montrez qu'il s'agit d'une relation d'ordre. Cet ordre est-il total ?

**2.** Soit  $A = \{(1,2), (2,3), (3,1), (3,2), (3,4), (4,3), (4,4), (5,5)\}$ .

Déterminez des minorants de  $A$ , des majorants de  $A$ .

$A$  admet-elle un plus grand élément ? un plus petit élément ? une borne supérieure ? une borne inférieure ?

## Solution

**1.** Pour tout  $(a,b) \in \mathbb{N}^2$ , on a  $a \leq a$  et  $b \leq b$ , soit  $(a,b) < (a,b)$ .

La relation  $<$  est donc réflexive.

Pour tout  $(a,b) \in \mathbb{N}^2$  et  $(a',b') \in \mathbb{N}^2$ , si  $(a,b) < (a',b')$  et  $(a',b') < (a,b)$ , alors  $(a,b) = (a',b')$ .

La relation  $<$  est donc antisymétrique.

Pour tout  $(a,b) \in \mathbb{N}^2$ ,  $(a',b') \in \mathbb{N}^2$ ,  $(a'',b'') \in \mathbb{N}^2$ , si  $(a,b) < (a',b')$  et  $(a',b') < (a'',b'')$ , de  $a \leq a'$  et  $a' \leq a''$ , on déduit  $a \leq a''$ , puis de même  $b \leq b''$ . On obtient ainsi  $(a,b) < (a'',b'')$ .

La relation  $<$  est donc transitive.

Par conséquent,  $<$  est une relation d'ordre.

Cet ordre n'est pas total car, par exemple,  $(1,2)$  et  $(2,1)$  ne sont pas comparables pour  $<$ .

**2.** Tous les éléments  $(a,b)$  de  $A$  vérifient  $(a,b) < (5,5)$ , et  $(5,5)$  est un élément de  $A$ . C'est donc le plus grand élément de  $A$ . C'est aussi la borne supérieure de  $A$ .

Si  $(a,b)$  est un minorant de  $A$ , de  $(a,b) < (1,2)$ , on déduit  $a \leq 1$  ; de  $(a,b) < (3,1)$ , on déduit  $b \leq 1$  ; d'où  $(a,b) < (1,1)$ .

Réciproquement, tout couple  $(a,b)$  tel que  $(a,b) < (1,1)$  est un minorant de  $A$ . L'ensemble des minorants de  $A$  est donc :

$$M = \{(a,b) \in \mathbb{N}^2 ; a \leq 1 \text{ et } b \leq 1\}.$$

Comme aucun élément de  $A$  n'appartient à cet ensemble,  $A$  n'admet pas de plus petit élément.

Comme  $(1,1)$  majore  $M$ , c'est la borne inférieure de  $A$ .

## I Nombres entiers naturels

- **Propriétés fondamentales de  $\mathbb{N}$**

L'ensemble  $\mathbb{N}$  des entiers naturels est totalement ordonné et vérifie les trois propriétés suivantes :

toute partie non vide de  $\mathbb{N}$  a un plus petit élément ;

toute partie non vide majorée de  $\mathbb{N}$  a un plus grand élément ;

$\mathbb{N}$  n'a pas de plus grand élément.

- **Raisonnement par récurrence**

Soit  $E(n)$  un énoncé qui dépend d'un entier naturel  $n$ .

Si  $E(0)$  est vrai, et si, quel que soit  $k \geq 0$ , l'implication  $E(k) \implies E(k+1)$  est vraie, alors l'énoncé  $E(n)$  est vrai pour tout entier  $n$ .

## II Ensembles finis

- **Définition**

Un ensemble  $E$  est fini s'il existe une bijection d'un intervalle  $\{1, \dots, n\}$  de  $\mathbb{N}$  sur  $E$ . Le nombre  $n$  est le cardinal (ou nombre d'éléments) de  $E$ . On le note  $n = \text{card } E$ . On convient que l'ensemble vide est fini, et que  $\text{card } \emptyset = 0$ .

- **Inclusion**

Soit  $E$  un ensemble fini. Toute partie  $A$  de  $E$  est finie, et on a :

$$\text{card } A \leq \text{card } E$$

l'égalité des cardinaux ayant lieu si, et seulement si,  $A = E$ .

- **Applications**

Soit  $E$  et  $F$  deux ensembles finis de même cardinal, et  $f$  une application de  $E$  dans  $F$ . On a l'équivalence des trois propriétés :

$$f \text{ bijective} \iff f \text{ injective} \iff f \text{ surjective.}$$

Dans ce cas, pour démontrer que  $f$  est bijective, il suffit de démontrer, soit que  $f$  est injective, soit que  $f$  est surjective.

## Application

Montrez que, pour tout  $n \in \mathbb{N}^*$ ,  $3 \times 5^{2n-1} + 2^{3n-2}$  est divisible par 17.

## Solution

Démontrons par récurrence, pour  $n \in \mathbb{N}^*$ , la propriété  $P(n)$  :

$$\alpha_n = 3 \times 5^{2n-1} + 2^{3n-2} \text{ est divisible par 17.}$$

Comme  $\alpha_1 = 17$ , la propriété  $P(1)$  est vraie.

Supposons que  $P(k)$  soit vraie, et montrons que cela entraîne  $P(k+1)$ .

$$\begin{aligned} \alpha_{k+1} &= 3 \times 5^{2k+1} + 2^{3k+1} = 3 \times 25 \times 5^{2k-1} + 8 \times 2^{3k-2} \\ &= 8(3 \times 5^{2k-1} + 2^{3k-2}) + 17 \times 3 \times 5^{2k-1} \\ &= 8\alpha_k + 17 \times 3 \times 5^{2k-1}. \end{aligned}$$

$\alpha_k$  étant divisible par 17, on en déduit que  $\alpha_{k+1}$  est divisible par 17.

## Application

Démontrez par récurrence que :  $\sum_{i=1}^n (2i-1)^2 = \frac{1}{3} n (4n^2 - 1)$ .

## Solution

Notons  $P(n)$  la propriété à démontrer.

Elle est vraie pour  $n = 1$  car  $1^2 = \frac{1}{3}(4 - 1)$ .

Supposons que  $P(k)$  soit vraie, et montrons que cela entraîne  $P(k+1)$ .

$$\begin{aligned} \sum_{i=1}^{k+1} (2i-1)^2 &= \frac{1}{3} k (4k^2 - 1) + (2k+1)^2 = \frac{1}{3} (2k+1) [4k^2 + 5k + 3] \\ &= \frac{1}{3} (k+1)(2k+1)(2k+3) = \frac{1}{3} (k+1) [4(k+1)^2 - 1]. \end{aligned}$$

La propriété est donc démontrée pour tout  $n \in \mathbb{N}^*$ .

## I Lois de composition interne

### • Définition

Une loi de composition interne sur un ensemble  $E$  est une application de  $E \times E$  dans  $E$ . À un couple  $(x, y)$ , on associe donc un élément, noté  $x * y$ , ou  $x + y$ , ou  $xy$ , ..., appelé composé de  $x$  et de  $y$ .

### • Propriétés

– Une loi de composition interne  $*$  sur  $E$  est :

• associative si :

$$\forall x \in E \quad \forall y \in E \quad \forall z \in E \quad (x * y) * z = x * (y * z) ;$$

• commutative si :

$$\forall x \in E \quad \forall y \in E \quad x * y = y * x$$

• Elle admet un élément neutre  $e$  si :

$$\exists e \in E \quad \forall x \in E \quad x * e = e * x = x.$$

Si l'élément neutre existe, il est unique.

– Un élément  $x$  est inversible (ou symétrisable) dans  $E$ , s'il existe  $x' \in E$  (dit inverse, ou symétrique, de  $x$ ) tel que :

$$x * x' = x' * x = e.$$

– Si  $*$  et  $\top$  sont deux lois de composition interne de  $E$ , on dit que  $*$  est distributive par rapport à  $\top$ , si l'on a toujours :

$$x * (y \top z) = (x * y) \top (x * z) \quad \text{et} \quad (y \top z) * x = (y * x) \top (z * x).$$

## II Groupes

### • Définitions

Un ensemble non vide  $G$ , muni d'une loi  $*$ , est un groupe si :

– la loi est associative ;

– il existe un élément neutre  $e$  ;

– tout élément de  $G$  possède un symétrique dans  $G$ .

Si, de plus, la loi est commutative, le groupe est dit commutatif, ou abélien.

Dans un groupe, tout élément est régulier (ou simplifiable), c'est-à-dire que l'on a toujours :

$$x * y = x * z \implies y = z \quad ; \quad y * x = z * x \implies y = z.$$

Généralement, un groupe est noté additivement ou multiplicativement. Le symétrique  $x'$  de  $x$  est alors noté  $-x$  dans le premier cas,  $x^{-1}$  dans le second.

## • Sous-groupes

### Définition

Une partie stable  $H$  d'un groupe  $G$  est un sous-groupe de  $G$  si la restriction à  $H$  de la loi de  $G$  définit dans  $H$  une structure de groupe.

### Propriété caractéristique

Pour qu'une partie non vide  $H$  d'un groupe  $G$  soit un sous-groupe de  $G$ , il faut et il suffit que :

$$\forall x \in H \quad \forall y \in H \quad xy \in H \quad \text{et} \quad x^{-1} \in H$$

ou encore :

$$\forall x \in H \quad \forall y \in H \quad xy^{-1} \in H.$$

### Propriété

L'intersection d'une famille de sous-groupes est un sous-groupe de  $G$ .

## • Morphismes de groupes

### Définitions



Soit  $G$  et  $G'$  deux groupes notés multiplicativement. Une application  $f$ , de  $G$  dans  $G'$ , est un morphisme de groupes si, et seulement si,

$$\forall x \in G \quad \forall y \in G \quad f(xy) = f(x)f(y).$$

Si, de plus,  $f$  est bijective, on dit que  $f$  est un isomorphisme de groupes. Les deux groupes sont alors isomorphes.

### Composition

Le composé de deux morphismes (resp. isomorphismes) de groupes est un morphisme (resp. isomorphisme) de groupes.

### Noyau et image

Soit  $G$  et  $G'$  deux groupes notés multiplicativement, d'éléments neutres respectifs  $e$  et  $e'$ , et  $f$  un morphisme de  $G$  dans  $G'$ . On a :

$$e' = f(e) \quad ; \quad f(x^{-1}) = [f(x)]^{-1}.$$

$f(G)$  sous-groupe de  $G'$  appelé image de  $f$  et noté  $\text{Im } f$ .

$N = f^{-1}(\{e'\}) = \{x ; x \in G, f(x) = e'\}$  est un sous-groupe de  $G$  que l'on appelle le noyau du morphisme  $f$ . On le note  $\text{Ker } f$ .

$f$  est injectif si, et seulement si,  $\text{Ker } f = \{e\}$ .

# III Groupe symétrique

- **Définition**

L'ensemble  $S(E)$  des bijections d'un ensemble fini  $E$  à  $n$  éléments, muni de la loi de composition des applications, est un groupe appelé groupe des permutations (ou substitutions) de  $E$ .

Il est isomorphe à  $S_n$ , groupe des permutations de l'intervalle  $\{1, \dots, n\}$  de  $\mathbb{N}$ , appelé groupe symétrique d'ordre  $n$ .

- **Décomposition d'une permutation en produit de cycles**

*Définition*

Un cycle (ou permutation circulaire) d'ordre  $p$  est une permutation  $\sigma$  de  $E$  qui laisse invariants  $n - p$  éléments de  $E$ , et telle que l'on puisse ranger les  $p$  éléments restants  $(a_1, \dots, a_p)$  de manière que :

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_{p-1}) = a_p, \sigma(a_p) = a_1.$$

On note  $\sigma = (a_1, \dots, a_p)$ .

*Théorème*

Toute permutation de  $E$  est décomposable en produit de cycles disjoints, deux cycles quelconques étant permutables.

- **Signature d'une permutation**

*Transposition*

On appelle transposition de  $E$  une permutation de  $E$  qui échange deux éléments de  $E$ , et qui laisse invariants tous les autres. C'est donc un cycle d'ordre 2.

*Parité d'une permutation*

Toute permutation de  $E$  est décomposable en un produit de transpositions. Cette décomposition n'est pas unique, mais, pour une permutation donnée, la parité du nombre de transpositions est fixe.

Si ce nombre est pair, on dit que la permutation est paire.

Si ce nombre est impair, on dit que la permutation est impaire.

*Signature d'une permutation*

La signature d'une permutation  $\sigma$  est le nombre, noté  $\varepsilon(\sigma)$ , égal à 1 si la permutation  $\sigma$  est paire, à  $-1$  si  $\sigma$  est impaire.

Pour déterminer  $\varepsilon(\sigma)$ , la méthode la plus rapide consiste à décomposer d'abord  $\sigma$  en produit de cycles, puis à savoir qu'un cycle d'ordre  $p$  peut se décomposer en  $p - 1$  transpositions.

## Application

Sur  $\mathbb{R}$  déjà muni de la multiplication et de l'addition, on définit la loi  $*$  par :

$$a * b = a + b + ab.$$

1. Montrez que  $*$  est associative et commutative ; qu'elle possède un élément neutre. Quels sont les éléments symétrisables ?
2. La loi  $*$  est-elle distributive par rapport à la multiplication ? Est-elle distributive par rapport à l'addition ?

## Solution

1. On a toujours :

$$a * b = a + b + ab = b + a + ba = b * a.$$

La loi  $*$  est donc commutative.

Quels que soient les réels  $a, b, c$ , on a :

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) = a + b + c + bc + a(b + c + bc) \\ &= a + b + c + ab + bc + ca + abc. \end{aligned}$$

Comme cette expression est invariante par permutation circulaire sur  $a, b, c$ , on obtiendra le même résultat en partant de  $(a * b) * c$ .

La loi  $*$  est donc associative.

0 est élément neutre de  $*$  car :

$$\forall a \in \mathbb{R} \quad a * 0 = 0 * a = a + 0 + a \times 0 = a.$$

$a$  sera symétrisable s'il existe  $b$  tel que :

$$0 = a * b = a + b + ab = a + (a + 1)b,$$

c'est-à-dire si  $a \neq -1$ . Le symétrique de  $a$  est alors  $\frac{-a}{a+1}$ .

2. On a :  $a * (bc) = a + bc + abc$  et  $(a * b)(a * c) = (a + b + ab)(a + c + ac)$ . Ces deux résultats ne semblent pas être toujours égaux.

Le contre-exemple :

$$1 * (1 \times 1) = 3 \quad ; \quad (1 * 1) \times (1 * 1) = 9,$$

prouve que  $*$  n'est pas distributive par rapport à la multiplication.

On a :  $a * (b+c) = a + b + c + a(b+c)$  et  $(a * b) + (a * c) = a + b + ab + a + c + ac$ .

Ces deux expressions sont égales si, et seulement si,  $a = 0$ . Comme elles ne sont pas toujours égales, la loi  $*$  n'est pas distributive par rapport à l'addition.

## Application

Démontrez que la réunion de deux sous-groupes est un sous-groupe si, et seulement si, l'un est inclus dans l'autre.

## Solution

Soit  $(G, +)$  un groupe,  $H_1$  et  $H_2$  deux sous-groupes.

Si  $H_1 \subset H_2$ , ou  $H_2 \subset H_1$ , alors  $H_1 \cup H_2$  est un sous-groupe de  $G$ , puisqu'il est égal à  $H_1$  ou à  $H_2$ . Cette condition est donc suffisante.

Pour la réciproque, démontrons la contraposée, c'est-à-dire que, si  $H_1 \not\subset H_2$  et si  $H_2 \not\subset H_1$ , alors  $H_1 \cup H_2$  n'est pas un sous-groupe de  $G$ .

Par hypothèse, il existe un élément  $h_1$  de  $H_1$  qui n'appartient pas à  $H_2$ , et un élément  $h_2$  de  $H_2$  qui n'appartient pas à  $H_1$ . Montrons que  $h_1 + h_2$  n'appartient pas à  $H_1 \cup H_2$ . Si l'on avait  $h_1 + h_2 \in H_1$ , alors  $(h_1 + h_2) - h_1 = h_2$  appartiendrait au sous-groupe  $H_1$ , ce qui est contraire à l'hypothèse. On montre de même que  $h_1 + h_2$  n'appartient pas à  $H_2$ .

On a donc  $h_1 \in H_1 \cup H_2$ ,  $h_2 \in H_1 \cup H_2$  et  $h_1 + h_2 \notin H_1 \cup H_2$ .

Comme  $H_1 \cup H_2$  n'est pas stable pour  $+$ , ce n'est pas un sous-groupe.

## Application

Montrez que  $\mathbb{R}$  muni de la loi  $*$  définie par :

$$x * y = \sqrt[2009]{x^{2009} + y^{2009}}$$

est isomorphe à  $\mathbb{R}$  muni de l'addition.

## Solution

L'application  $f$ , de  $\mathbb{R}$  dans  $\mathbb{R}$ , définie par  $f(x) = x^{2009}$  est une bijection puisqu'elle est continue, strictement croissante, avec  $f(\mathbb{R}) = \mathbb{R}$ .

De plus, on observe que, pour tous réels  $x$  et  $y$ , on a :

$$f(x * y) = f(x) + f(y).$$

$f$  transporte donc la structure de groupe commutatif de  $(\mathbb{R}, +)$ , et les groupes  $(\mathbb{R}, +)$  et  $(\mathbb{R}, *)$  sont isomorphes.

## Application

Soit  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 11 & 4 & 10 & 12 & 9 & 2 & 5 & 8 & 3 & 7 & 1 & 6 \end{pmatrix}$ .

Décomposez  $\sigma$  en un produit de cycles disjoints, puis en un produit de transpositions.

Déduisez-en  $\varepsilon(\sigma)$ , et déterminez  $\sigma^{2009}$ .

## Solution

Soit  $\sigma_1 = \begin{pmatrix} 1 & 11 \\ 11 & 1 \end{pmatrix} = (1 \ 11),$

$\sigma_2 = \begin{pmatrix} 2 & 4 & 12 & 6 \\ 4 & 12 & 6 & 2 \end{pmatrix} = (2 \ 4 \ 12 \ 6),$

$\sigma_3 = \begin{pmatrix} 3 & 10 & 7 & 5 & 9 \\ 10 & 7 & 5 & 9 & 3 \end{pmatrix} = (3 \ 10 \ 7 \ 5 \ 9).$

On vérifie que  $\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3$ .

On en déduit qu'on peut décomposer  $\sigma$  en  $1 + 3 + 4 = 8$  transpositions :

$$\begin{aligned} \sigma &= \sigma_1 \circ \sigma_2 \circ \sigma_3 \\ &= (1 \ 11) \circ (2 \ 4) \circ (4 \ 12) \circ (12 \ 6) \circ (3 \ 10) \circ (10 \ 7) \circ (7 \ 5) \circ (5 \ 9). \end{aligned}$$

C'est une permutation paire ; donc  $\varepsilon(\sigma) = (-1)^8 = 1$ .

Les cycles  $\sigma_1$ ,  $\sigma_2$  et  $\sigma_3$  étant disjoints, on a :

$$\sigma^{2009} = \sigma_1^{2009} \circ \sigma_2^{2009} \circ \sigma_3^{2009}.$$

Comme on a  $\sigma_1^2 = \sigma_2^4 = \sigma_3^5 = \text{Id}$ , on en déduit :

$$\sigma^{2009} = \sigma_1^{2 \times 1004 + 1} \circ \sigma_2^{4 \times 502 + 1} \circ \sigma_3^{5 \times 401 + 4} = \sigma_1 \circ \sigma_2 \circ \sigma_3^4.$$

Donc :

$$\sigma^{2009} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 11 & 4 & 9 & 12 & 7 & 2 & 10 & 8 & 5 & 3 & 1 & 6 \end{pmatrix}.$$

## I Anneaux

### • Structure d'anneau

Un ensemble  $A$ , muni d'une loi notée  $+$  (dite addition) et d'une loi notée  $\times$  (dite multiplication), possède une structure d'anneau si :

- $A$  possède une structure de groupe commutatif pour l'addition ;
- la multiplication est associative et possède un élément neutre ;
- la multiplication est distributive par rapport à l'addition.

Si la multiplication est commutative, l'anneau est dit commutatif.

### • Règles de calcul

$$x \left( \sum_{i=1}^n y_i \right) = \sum_{i=1}^n x y_i \quad ; \quad \left( \sum_{i=1}^n y_i \right) x = \sum_{i=1}^n y_i x .$$

Dans un anneau commutatif, pour tout  $n \in \mathbb{N}$ , on a :

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k} \quad (\text{formule du binôme}) \quad \text{où} \quad \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

$$x^n - y^n = (x - y) \sum_{k=0}^{n-1} x^{n-k-1} y^k .$$

Si l'anneau n'est pas commutatif, ces formules restent vraies pour des éléments permutable, c'est-à-dire tels que  $xy = yx$ .

### • Sous-anneau

On dit qu'une partie  $B$  d'un anneau  $A$ , stable pour  $+$  et  $\times$ , est un sous-anneau de  $A$ , si la restriction à  $B$  des deux lois de  $A$  définit dans  $B$  une structure d'anneau, avec le même élément neutre pour  $\times$  que dans  $A$ .

Pour qu'une partie  $B$  d'un anneau  $A$  soit un sous-anneau de  $A$ , il faut et il suffit que  $1_A \in B$  et :

$$\forall x \in B \quad \forall y \in B \quad x - y \in B \quad \text{et} \quad xy \in B .$$

- **Morphismes d'anneaux**

$A$  et  $B$  étant deux anneaux, une application  $f$ , de  $A$  dans  $B$ , est un morphisme d'anneaux si l'on a toujours :

$$f(x + y) = f(x) + f(y) ; f(xy) = f(x) f(y) ; f(1_A) = 1_B.$$

- **Anneau intègre**

Lorsqu'il existe, dans un anneau, des éléments  $a$  et  $b$  tels que

$$a \neq 0 \quad \text{et} \quad b \neq 0 \quad \text{et} \quad ab = 0,$$

on dit que  $a$  et  $b$  sont des diviseurs de zéro.

Un anneau intègre est un anneau commutatif, non réduit à  $\{0\}$ , et sans diviseur de zéro.

Pour qu'un anneau commutatif, non réduit à  $\{0\}$ , soit intègre, il faut et il suffit que tout élément non nul soit simplifiable pour la multiplication.

## II Corps

- **Structure de corps**

Un corps est un anneau non réduit à  $\{0\}$  dont tous les éléments, sauf 0, sont inversibles. Il est dit commutatif si l'anneau est commutatif.

Dans cet ouvrage, tous les corps seront supposés commutatifs, sans avoir besoin de le préciser à chaque fois.

- **Sous-corps**

On dit qu'une partie  $L$  d'un corps  $K$ , stable pour  $+$  et  $\times$ , est un sous-corps de  $K$ , si la restriction à  $L$  des deux lois de  $K$  définit dans  $L$  une structure de corps, c'est-à-dire si c'est un sous-anneau, et si l'inverse d'un élément non nul de  $L$  reste dans  $L$ .

Pour qu'une partie non vide  $L$  d'un corps  $K$  soit un sous-corps de  $K$ , il faut et il suffit que  $1 \in L$  et que :

$$\begin{cases} \forall x \in L \quad \forall y \in L & x - y \in L \quad \text{et} \quad xy \in L \\ \forall x \in L^* & x^{-1} \in L^* \end{cases} \quad \text{où } L^* = L \setminus \{0\}.$$

## Application

Soit  $x$  un élément d'un anneau intègre  $A$ .

Démontrez que si  $x$  est inversible à droite, alors  $x$  est inversible à gauche.

## Solution

Comme  $x$  admet un symétrique à droite, il existe  $x' \in A$  tel que  $xx' = 1$ . On a :

$$(x'x - 1)x' = x'xx' - x' = x' - x' = 0.$$

Puisque  $xx' = 1$ , on a  $x' \neq 0$  car sinon on aurait  $0 = 1$  et l'anneau  $A$  serait réduit à  $\{0\}$ .

Comme  $(x'x - 1)x' = 0$  et  $x' \neq 0$  dans un anneau intègre, on obtient  $x'x - 1 = 0$ , soit  $x'x = 1$ .

$x$  admet donc aussi un symétrique à gauche.

## Application

Soit  $A$  un anneau commutatif. On dit qu'un élément  $x$  est nilpotent s'il existe  $n \in \mathbb{N}$  tel que  $x^n = 0$ .

1. Montrez que, si  $x$  est nilpotent, alors  $1 - x$  est inversible.

2. Montrez que, si  $x$  et  $y$  sont nilpotents, alors  $xy$  et  $x + y$  le sont aussi.

## Solution

1. Supposons qu'il existe un entier  $n$  tel que  $x^n = 0$ .

$y = 1 + x + \dots + x^{n-1}$  est un élément de  $A$ .

En développant grâce aux propriétés d'un anneau, on obtient :

$$(1 - x)y = (1 - x)(1 + x + \dots + x^{n-1}) = 1 - x^n = 1.$$

L'élément  $1 - x$  est donc inversible, et a pour inverse  $y$ .

2.  $x$  et  $y$  étant supposés nilpotents, il existe  $p \in \mathbb{N}$  tel que  $x^p = 0$ , et  $q \in \mathbb{N}$  tel que  $y^q = 0$ .

L'anneau étant commutatif, on a  $(xy)^p = x^p y^p$ .

Comme  $x^p = 0$ , on en déduit que  $(xy)^p = 0$ , ce qui prouve que  $xy$  est nilpotent.

Considérons  $(x + y)^n$  avec  $n = p + q$ . On peut le développer en utilisant la formule du binôme car l'anneau est commutatif :

$$(x + y)^{p+q} = \sum_{k=0}^{p+q} \binom{p+q}{k} x^k y^{p+q-k}.$$

Pour  $0 \leq k \leq p$ , on a  $p + q - k \geq q$ , qui entraîne  $y^{p+q-k} = y^q y^{p-k} = 0$ , puis

$$\binom{p+q}{k} x^k y^{p+q-k} = 0.$$



Pour  $p \leq k \leq p + q$ , on a  $x^k = x^p x^{k-p} = 0$ , et  $y^{p+q-k}$  existe puisque  $p + q - k \geq 0$ .

Le terme correspondant est donc nul lui aussi.

Tous les termes de la somme sont donc nuls.

On a donc montré qu'il existe  $n = p + q$  tel que  $(x + y)^n = 0$ , c'est-à-dire que  $x + y$  est nilpotent.

## Application

Montrez que le corps des rationnels  $\mathbb{Q}$  n'admet pas d'autre sous-corps que lui-même.

## Solution

Soit  $\mathbb{K}$  un sous-corps de  $\mathbb{Q}$ .

Il contient les éléments neutres 0 et 1 de l'addition et de la multiplication.

Comme il est stable par addition, tout entier naturel non nul  $n = 1 + \dots + 1$  appartient aussi à  $\mathbb{K}$ . Donc  $\mathbb{N} \subset \mathbb{K}$ .

Comme  $\mathbb{K}$  est un groupe pour l'addition, pour tout entier naturel  $n$ , on a aussi  $-n \in \mathbb{K}$ . Donc  $\mathbb{Z} \subset \mathbb{K}$ .

Considérons un rationnel  $r = \frac{p}{q}$  avec  $q \neq 0$ . Comme  $p$  et  $q$  appartiennent au corps

$\mathbb{K}$ , alors  $r = p \times q^{-1} \in \mathbb{K}$ . Donc  $\mathbb{Q} \subset \mathbb{K}$ .

On est parti de  $\mathbb{K} \subset \mathbb{Q}$ . On conclut donc que  $\mathbb{K} = \mathbb{Q}$ .

## I Divisibilité dans $\mathbb{Z}$

- **Division euclidienne**

Pour tout  $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ , il existe un élément unique  $(q, r) \in \mathbb{Z} \times \mathbb{N}$  tel que :

$$a = bq + r \text{ avec } 0 \leq r < b.$$

$q$  est le quotient et  $r$  le reste de la division euclidienne de  $a$  par  $b$ .

- **Divisibilité**

Si  $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ , on dit que  $b$  divise  $a$  si, et seulement si, il existe  $q \in \mathbb{Z}$  tel que  $a = bq$ .

On dit alors que  $a$  est un multiple de  $b$ , ou que  $b$  est un diviseur de  $a$ .

La relation de divisibilité est une relation d'ordre partiel dans  $\mathbb{N}$ .

- **Nombres premiers**

*Définition*

Un entier  $p$  est premier si  $p \geq 2$ , et si ses seuls diviseurs sont 1 et  $p$ .

*Propriétés*

Il y a une infinité de nombres premiers.

Si  $n$  n'est divisible par aucun nombre premier inférieur ou égal à  $\sqrt{n}$ , alors il est premier.

Tout entier  $n$ , avec  $n \geq 2$ , s'écrit de façon unique comme produit de nombres premiers.

## II pgcd et ppcm

- **pgcd**

*Définition*

Soit  $a$  et  $b$  deux entiers relatifs non nuls. L'ensemble des nombres de  $\mathbb{N}^*$  qui divisent à la fois  $a$  et  $b$ , admet un plus grand élément  $d$ , pour la relation d'ordre de divisibilité.

C'est le plus grand commun diviseur de  $a$  et de  $b$ . On le note  $\text{PGCD}(a, b)$ , ou  $a \vee b$ .

### Algorithme d'Euclide

Si  $q_1$  et  $r_1$  sont respectivement le quotient et le reste de la division euclidienne de  $a$  par  $b$ , on a :

$$a \vee b = b \vee r_1.$$

On recommence avec  $b$  et  $r_1$ . Le dernier reste non nul de ce processus est le PGCD de  $a$  et de  $b$ .

### Nombres premiers entre eux

Si  $\text{PGCD}(a, b) = 1$ , on dit que  $a$  et  $b$  sont premiers entre eux.

Soit  $r = \frac{a}{b}$  (avec  $b \neq 0$ ) un nombre rationnel. Si  $d$  désigne le PGCD de  $a$  et de  $b$ , on a  $a = da'$  et  $b = db'$ , avec  $a'$  et  $b'$  premiers entre eux. On peut alors écrire  $r = \frac{a'}{b'}$  (avec  $b' \neq 0$ ). C'est la forme irréductible de  $r$ .

- **ppcm**

#### Définition

Soit  $a$  et  $b$  deux entiers relatifs non nuls. L'ensemble des nombres de  $\mathbb{N}^*$  qui sont multiples à la fois de  $a$  et de  $b$ , admet un plus petit élément  $m$ , pour la relation d'ordre de divisibilité.

C'est le plus petit commun multiple de  $a$  et de  $b$ . On le note  $\text{PPCM}(a, b)$ , ou  $a \wedge b$ .

#### Théorème

$$\text{PGCD}(a, b) \times \text{PPCM}(a, b) = |a b|.$$

- **Théorème de Bézout**

Pour que deux entiers relatifs non nuls  $a$  et  $b$  soient premiers entre eux, il faut, et il suffit, qu'il existe  $u$  et  $v$  dans  $\mathbb{Z}$  tels que :

$$au + bv = 1.$$

On obtient  $u$  et  $v$  avec l'algorithme d'Euclide.

- **Théorème de Gauss**

Soit  $a, b, c$  trois entiers relatifs tels que  $a$  divise  $bc$ , et  $a$  premier avec  $b$ . Alors  $a$  divise  $c$ .

### III Anneau $\mathbb{Z}/n\mathbb{Z}$

- **Congruences dans  $\mathbb{Z}$**

Soit  $n \in \mathbb{N}^*$ . La relation binaire dans  $\mathbb{Z}$  :

$$a \text{ et } b \text{ ont le même reste dans la division par } n \iff n/(a - b)$$

se note  $a \equiv b \pmod{n}$  ; lire :  $a$  congru à  $b$  modulo  $n$ .

On écrit  $\mathbb{Z}/n\mathbb{Z}$  pour désigner l'ensemble des classes ainsi formées par regroupement :

$$\bar{a} = \{b \in \mathbb{Z} ; a \equiv b \pmod{n}\}.$$

- **Propriétés algébriques de  $\mathbb{Z}/n\mathbb{Z}$**

#### *Structure*

Pour  $n \geq 2$ , l'ensemble  $\mathbb{Z}/n\mathbb{Z}$  muni des deux lois :

$$\bar{a} + \bar{b} = \overline{a + b} ; \bar{a} \times \bar{b} = \overline{a \times b}$$

est un anneau commutatif.

#### *Éléments inversibles*

Un élément  $\bar{a}$  de  $\mathbb{Z}/n\mathbb{Z}$  est inversible si, et seulement si,  $a$  et  $n$  sont premiers entre eux.

#### *Cas particulier*

$\mathbb{Z}/n\mathbb{Z}$  est un corps si, et seulement si,  $n$  est premier.

## Application

1. Démontrez que 143 et 100 sont premiers entre eux.
2. Déterminez tous les couples  $(u, v)$  d'entiers relatifs tels que :

$$143u + 100v = 1.$$

## Solution

1. La décomposition en facteurs premiers des deux nombres s'écrit :

$$143 = 11 \times 13 \quad ; \quad 100 = 2^2 \times 5^2.$$

Comme il n'y a aucun facteur premier commun à ces deux décompositions, les nombres 100 et 143 sont premiers entre eux.

L'algorithme d'Euclide conduit à une deuxième démonstration de ce résultat. Il prouve l'existence de nombres  $u$  et  $v$  du théorème de Bézout, en fournissant explicitement une solution particulière.

Il s'agit de réaliser une suite de divisions euclidiennes : de 143 par 100, puis de 100 par le reste  $r_1$  obtenu, puis de  $r_1$  par  $r_2$ ... On obtient :

$$143 = 100 \times 1 + 43$$

$$100 = 43 \times 2 + 14$$

$$43 = 14 \times 3 + 1$$

Comme cet algorithme se termine par 1, c'est une nouvelle preuve que 143 et 100 sont premiers entre eux.

On va en déduire un exemple de nombres  $u$  et  $v$  tels que :

$$143u + 100v = 1,$$

par des substitutions successives des restes en partant de la dernière égalité où figure déjà le 1 du second membre.

$$1 = 43 - 14 \times 3$$

$$= 43 - (100 - 43 \times 2) \times 3 = (-3) \times 100 + 7 \times 43$$

$$= (-3) \times 100 + 7 \times (143 - 100) = 7 \times 143 + (-10) \times 100.$$

Les nombres  $u_0 = 7$  et  $v_0 = -10$  vérifient donc  $143u_0 + 100v_0 = 1$ .

2. Considérons des entiers relatifs  $u$  et  $v$  tels que  $143u + 100v = 1$ .

En retranchant l'égalité précédente, on obtient :

$$143(u - u_0) = 100(v_0 - v).$$

143 divise donc  $100(v_0 - v)$ . Comme 143 est premier avec 100, on en déduit, d'après le théorème de Gauss, que 143 divise  $(v_0 - v)$ , c'est-à-dire qu'il existe  $k \in \mathbb{Z}$  tel que :  $v_0 - v = 143k$ .

En reportant, on obtient aussi :  $u - u_0 = 100k$ .

Réciproquement, tous les nombres  $u$  et  $v$  ainsi obtenus conviennent.  
L'ensemble  $\mathcal{S}$  des solutions  $(u, v) \in \mathbb{Z}^2$  de l'équation  $143u + 100v = 1$  est donc :

$$\mathcal{S} = \{(7 + 100k, -10 - 143k) ; k \in \mathbb{Z}\}.$$

## Application

$a$  et  $b$  étant deux entiers naturels non nuls, on note  $d$  leur PGCD et  $m$  leur PPCM.  
Déterminez tous les couples  $(a, b)$  vérifiant le système :

$$\begin{cases} m &= d^2 \\ m + d &= 156 \\ a &\geq b. \end{cases}$$

## Solution

En reportant la première égalité dans la deuxième, on obtient :

$$m + d = d^2 + d = d(d + 1) = 156.$$

$d$  et  $d + 1$  sont donc des diviseurs de 156.

Dans  $\mathbb{N}$ , les diviseurs de  $156 = 2^2 \times 3 \times 13$  sont :

$$\{1, 2, 3, 4, 6, 12, 13, 26, 39, 52, 78, 156\}.$$

On a donc  $d = 12$  et  $m = 144$ .

On sait que  $md = |ab|$ . Introduisons les nombres  $a'$  et  $b'$ , premiers entre eux avec  $a' \geq b'$ , tels que  $a = 12a'$  et  $b = 12b'$ .

En reportant dans la dernière égalité, on obtient :

$$a'b' = 12.$$

Deux possibilités sont à envisager car  $a \geq b$  :

- $a' = 12$  et  $b' = 1$ , qui conduit à la solution  $a = 144$  et  $b = 12$  ;
- $a' = 4$  et  $b' = 3$ , qui conduit à la solution  $a = 48$  et  $b = 36$ .

## Application

Dans  $\mathbb{Z}/60\mathbb{Z}$ , montrez que  $\overline{11}$  et  $\overline{7}$  sont inversibles et déterminez leurs inverses.

## Solution

- Comme 11 et 7 sont premiers avec 60, les deux éléments  $\overline{11}$  et  $\overline{7}$  sont inversibles dans  $\mathbb{Z}/60\mathbb{Z}$ .
- On a  $\overline{11} \times \overline{11} = \overline{121} = \overline{1}$ . L'inverse de  $\overline{11}$  dans  $\mathbb{Z}/60\mathbb{Z}$  est donc  $\overline{11}$ .
- Déterminons des entiers  $u$  et  $v$  tels que  $7u + 60v = 1$  avec l'algorithme d'Euclide :

$$60 = 7 \times 8 + 4$$

$$7 = 4 \times 1 + 3$$

$$4 = 3 \times 1 + 1$$

d'où l'on déduit :

$$1 = 4 - 3$$

$$= 4 - (7 - 4) = 4 \times 2 - 7$$

$$= (60 - 7 \times 8) \times 2 - 7$$

$$= 60 \times 2 - 17 \times 7.$$

On a donc dans  $\mathbb{Z}/60\mathbb{Z}$  :

$$\overline{1} = \overline{60 \times 2 - 17 \times 7} = \overline{-17} \times \overline{7} = \overline{43} \times \overline{7}.$$

L'inverse de  $\overline{7}$  dans  $\mathbb{Z}/60\mathbb{Z}$  est donc  $\overline{43}$ .

## I Forme algébrique

### • Définitions

Tout nombre complexe  $z$  s'écrit, de manière unique, sous la forme algébrique  $z = x + iy$  avec  $x$  et  $y$  réels,  $i$  étant un nombre complexe particulier tel que  $i^2 = -1$ .

Le réel  $x$  s'appelle la partie réelle de  $z$ , et se note  $\text{Re}(z)$ .

Le réel  $y$  s'appelle la partie imaginaire de  $z$ , et se note  $\text{Im}(z)$ .

### • Plan complexe

Soit  $(O, \vec{u}, \vec{v})$  un repère orthonormal du plan.

L'application qui, à tout nombre complexe  $z = x + iy$ , fait correspondre le point  $M$  de coordonnées  $(x, y)$  est une bijection.  $M$  est l'image de  $z$ , et  $z$  l'axe de  $M$ .

L'axe du vecteur  $\alpha \vec{u} + \beta \vec{v}$  est le nombre complexe  $z = \alpha + i\beta$ .

Si  $z_A$  et  $z_B$  sont les axes de  $A$  et  $B$ , le vecteur  $\overrightarrow{AB}$  a pour axe  $z_B - z_A$ .

La somme des nombres complexes correspond à l'addition des vecteurs.

### • Conjugué d'un nombre complexe

Le conjugué du nombre complexe  $z = x + iy$  (où  $x \in \mathbb{R}$  et  $y \in \mathbb{R}$ ) est le nombre complexe  $\bar{z} = x - iy$ .

Les images des nombres complexes  $z$  et  $\bar{z}$  sont symétriques par rapport à l'axe des abscisses.

On a les propriétés :

$$\bar{\bar{z}} = z \quad ; \quad \overline{z + z'} = \bar{z} + \bar{z'} \quad ; \quad \overline{zz'} = \bar{z}\bar{z'} \quad ; \quad \overline{\left(\frac{z}{z'}\right)} = \frac{\bar{z}}{\bar{z'}}.$$

## II Forme trigonométrique

### • Module d'un nombre complexe

Le module de  $z = x + iy$  (où  $x \in \mathbb{R}$  et  $y \in \mathbb{R}$ ) est le nombre réel positif

$\sqrt{z\bar{z}} = \sqrt{x^2 + y^2}$ . On le note  $|z|$ , ou  $\rho$ , ou  $r$ .

Si  $M$  est l'affixe de  $z$ ,  $|z|$  est la longueur  $OM$ .

Le module d'un nombre complexe a les mêmes propriétés que la valeur absolue d'un nombre réel.

- **Forme trigonométrique**

Tout nombre complexe non nul  $z$  s'écrit sous forme trigonométrique :

$$z = \rho (\cos \theta + i \sin \theta) \text{ avec } \rho > 0.$$

$\rho = |z|$  est le module de  $z$ .

$\theta$  est un argument de  $z$ . On le note  $\arg z$ . Il est défini, modulo  $2\pi$ , par :

$$\cos \theta = \frac{x}{\rho} \quad \text{et} \quad \sin \theta = \frac{y}{\rho}.$$

- **Propriétés de l'argument d'un nombre complexe non nul**

Les égalités suivantes ont lieu à  $2k\pi$  près (avec  $k \in \mathbb{Z}$ ) :

$$\arg(zz') = \arg z + \arg z' \quad ; \quad \arg(z^n) = n \arg z \text{ avec } n \in \mathbb{Z} ;$$

$$\arg\left(\frac{1}{z}\right) = -\arg z \quad ; \quad \arg\left(\frac{z}{z'}\right) = \arg z - \arg z'.$$

### III Exponentielle complexe

On convient de noter  $\cos \theta + i \sin \theta = e^{i\theta}$ .

- **Formule de Moivre**

$$\forall \theta \in \mathbb{R} \quad \forall n \in \mathbb{Z} \quad (\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta,$$

ce qui s'écrit avec la notation précédente :  $(e^{i\theta})^n = e^{in\theta}$ .

- **Formules d'Euler**

Pour tout réel  $x$  et tout entier  $n$ , on a :

$$\begin{aligned} \cos x &= \frac{e^{ix} + e^{-ix}}{2} \quad ; \quad \sin x = \frac{e^{ix} - e^{-ix}}{2i} ; \\ \cos nx &= \frac{e^{inx} + e^{-inx}}{2} \quad ; \quad \sin nx = \frac{e^{inx} - e^{-inx}}{2i}. \end{aligned}$$

- **Exponentielle complexe**

– Définition

On définit l'exponentielle du nombre complexe  $z = x + iy$  par :

$$e^z = e^x e^{iy} = e^x (\cos y + i \sin y).$$

– Propriétés

$$\begin{array}{lll} \forall z \in \mathbb{C} & \forall z' \in \mathbb{C} & e^z e^{z'} = e^{z+z'} ; \\ \forall z \in \mathbb{C} & \forall n \in \mathbb{Z} & (e^z)^n = e^{nz} . \end{array}$$

Si  $z$  est une constante complexe et  $t$  une variable réelle, on a :

$$\frac{d}{dt}(e^{zt}) = z e^{zt} .$$

## IV Racines $n$ -ièmes d'un nombre complexe

- **Racines  $n$ -ièmes de l'unité**

Soit  $U_n$  l'ensemble des racines  $n$ -ièmes de 1, c'est-à-dire l'ensemble des nombres complexes  $z$  tels que  $z^n = 1$ . On a :

$$U_n = \{u_0, u_1, \dots, u_{n-1}\} \text{ avec } u_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} = (u_1)^k$$

et la propriété :  $\sum_{k=0}^{n-1} u_k = 0$ .

- **Racines  $n$ -ièmes d'un nombre complexe non nul**

Tout nombre complexe non nul  $\rho (\cos \theta + i \sin \theta)$  possède  $n$  racines  $n$ -ièmes :

$$z_k = \sqrt[n]{\rho} \left( \cos \frac{\theta + 2k\pi}{n} + i \sin \frac{\theta + 2k\pi}{n} \right) \text{ avec } k \in \{0, \dots, n-1\}.$$

À partir de l'une d'entre elles, on peut les obtenir toutes en la multipliant par les éléments de  $U_n$ .

- **Cas particulier des racines carrées**

Pour déterminer les racines carrées de  $z = a + ib$ , il est plus commode de procéder par identification, c'est-à-dire de chercher les réels  $\alpha$  et  $\beta$  tels que  $(\alpha + i\beta)^2 = a + ib$ .

L'égalité des parties réelles et des parties imaginaires donne :

$$\alpha^2 - \beta^2 = a \quad \text{et} \quad 2\alpha\beta = b .$$

L'égalité des modules conduit à :

$$\alpha^2 + \beta^2 = \sqrt{a^2 + b^2} .$$

On en déduit  $\alpha^2$  et  $\beta^2$ , puis  $\alpha$  et  $\beta$  en utilisant le fait que  $\alpha\beta$  est du signe de  $b$ .

Ce calcul est utilisé lors de la résolution d'une équation du second degré à coefficients complexes.

## Application

Résolvez dans  $\mathbb{C}$  :  $z^8 = \bar{z}$ .

### Solution

L'égalité  $z^8 = \bar{z}$  entraîne  $|z^8| = |\bar{z}|$ , soit  $|z|^8 = |z|$ .

On a donc  $|z| = 0$  ou  $|z| = 1$ .

Si  $|z| = 0$ , alors  $z = 0$ .

Si  $|z| = 1$ , il reste à écrire l'égalité des arguments, à un multiple de  $2\pi$  près :

$$8 \arg z = -\arg z \iff 9 \arg z = 0,$$

soit  $\arg z = \frac{2k\pi}{9}$  avec  $k \in \{0, 1, \dots, 8\}$ .

Les racines de  $z^8 = \bar{z}$  sont donc 0 et les racines 9-ièmes de l'unité.

## Application

Calculez :  $\sum_{k=0}^n \binom{n}{k} \cos kx$ .

### Solution

$A = \sum_{k=0}^n \binom{n}{k} \cos kx$  est la partie réelle de :

$$\sum_{k=0}^n \binom{n}{k} \cos kx + i \sum_{k=0}^n \binom{n}{k} \sin kx = \sum_{k=0}^n \binom{n}{k} e^{ikx} = (1 + e^{ix})^n.$$

Pour élever  $1 + e^{ix}$  à la puissance  $n$ , on peut :

– soit utiliser des formules de trigonométrie :

$$\begin{aligned} 1 + e^{ix} &= 1 + \cos x + i \sin x = 2 \cos^2 \frac{x}{2} + 2i \sin \frac{x}{2} \cos \frac{x}{2} \\ &= 2 \cos \frac{x}{2} \left( \cos \frac{x}{2} + i \sin \frac{x}{2} \right). \end{aligned}$$

– soit utiliser une factorisation efficace :

$$1 + e^{ix} = e^{i\frac{x}{2}} \left( e^{i\frac{x}{2}} + e^{-i\frac{x}{2}} \right) = e^{i\frac{x}{2}} 2 \cos \frac{x}{2}.$$

On en déduit :

$$(1 + e^{ix})^n = \left( 2 \cos \frac{x}{2} \right)^n \left( \cos n \frac{x}{2} + i \sin n \frac{x}{2} \right),$$

$$\text{puis } A = 2^n \left( \cos \frac{x}{2} \right)^n \cos \left( n \frac{x}{2} \right).$$

## Application

Résolvez dans  $\mathbb{C}$  l'équation :

$$(1 + i)z^2 - (7 + 13i)z + 2 + 60i = 0 \quad (\mathbf{E}).$$

## Solution

On a :  $\Delta = (7 + 13i)^2 - 4(1 + i)(2 + 60i) = 112 - 66i \neq 0$ .

On cherche d'abord les racines carrées de  $\Delta$ , c'est-à-dire les réels  $\alpha$  et  $\beta$  tels que :

$$(\alpha + i\beta)^2 = 112 - 66i.$$

En écrivant l'égalité des parties réelles, des parties imaginaires et des modules, on obtient :

$$\begin{cases} \alpha^2 - \beta^2 = 112 \\ \alpha\beta = -33 \\ \alpha^2 + \beta^2 = 130 \end{cases} \iff \begin{cases} \alpha^2 = 121 \\ \alpha\beta < 0 \\ \beta^2 = 9 \end{cases}$$

Les racines de  $\Delta$  sont  $-11 + 3i$  et  $11 - 3i$ .

Les racines de  $(\mathbf{E})$  sont donc :

$$\frac{7 + 13i + (-11 + 3i)}{2(1 + i)} = 3 + 5i \quad \text{et} \quad \frac{7 + 13i + (11 - 3i)}{2(1 + i)} = 7 - 2i.$$

## Application

Soit  $a$  et  $b$  deux réels distincts et  $n \in \mathbb{N}^*$ . Résolvez l'équation (E) dans  $\mathbb{C}$  :

$$(z - a)^n - (z - b)^n = 0 \quad (\text{E}).$$

## Solution

Comme  $z = b$  n'est pas solution de (E) puisque  $a \neq b$ , l'équation est équivalente à :

$$\left( \frac{z - a}{z - b} \right)^n = 1 ;$$

d'où :  $\frac{z_k - a}{z_k - b} = e^{i \frac{2k\pi}{n}}$  avec  $k \in \{0, \dots, n-1\}$ .

Pour  $k = 0$ , on aurait  $a = b$ , ce qui est contraire à l'hypothèse.

Pour  $k \in \{1, \dots, n-1\}$ , on obtient :  $z_k = \frac{a - b e^{i \frac{2k\pi}{n}}}{1 - e^{i \frac{2k\pi}{n}}}.$

Résoudre (E), c'est chercher les racines d'un polynôme de degré  $n - 1$  (développez si nécessaire). Le théorème de d'Alembert (cf. fiche 11) nous dit qu'il y en a  $n - 1$  dans  $\mathbb{C}$ , ce qui permet de se contrôler.

En multipliant le numérateur et le dénominateur par  $e^{-i \frac{k\pi}{n}}$  on a :

$$\begin{aligned} z_k &= \frac{a e^{-i \frac{k\pi}{n}} - b e^{i \frac{k\pi}{n}}}{-2i \sin\left(\frac{k\pi}{n}\right)} = \frac{(a - b) \cos\left(\frac{k\pi}{n}\right) - i(a + b) \sin\left(\frac{k\pi}{n}\right)}{-2i \sin\left(\frac{k\pi}{n}\right)} \\ &= \frac{a + b}{2} + i \frac{a - b}{2} \cot\left(\frac{k\pi}{n}\right). \end{aligned}$$

On constate que les images des solutions appartiennent toutes à la droite d'équation

$$x = \frac{a + b}{2}.$$

# Nombres complexes et géométrie

$a = a_1 + i a_2$  et  $b = b_1 + i b_2$  sont deux nombres complexes donnés (cf. fiche 9).

## I Transformations géométriques

- **Translation**

L'application de  $\mathbb{C}$  dans  $\mathbb{C} : z \mapsto z + b$ , se traduit sur les images par la translation de vecteur  $b_1 \vec{u} + b_2 \vec{v}$ .

- **Similitude directe**

Si  $a \neq 1$ , l'application de  $\mathbb{C}$  dans  $\mathbb{C} : z \mapsto az + b$ , se traduit sur les images par la similitude de rapport  $|a|$ , d'angle  $\arg a$ , et dont le centre  $\Omega$ , a pour affixe

$$z_{\Omega} = \frac{b}{1 - a}.$$

Cette transformation est la composée, dans n'importe quel ordre, de la rotation de centre  $\Omega$  et d'angle  $\arg a$ , et de l'homothétie de centre  $\Omega$  et de rapport  $|a|$ .

## II Distances et angles

- **Avec deux points**

Soit  $A$  et  $B$  deux points distincts, d'affixes respectifs  $z_A$  et  $z_B$ .

$|z_B - z_A|$  est la longueur  $AB$  ;  $\arg(z_B - z_A)$  est une mesure de l'angle  $(\vec{u}, \vec{AB})$ .

- **Avec trois points**

Soit  $A$ ,  $B$  et  $C$  trois points, deux à deux distincts, d'affixes respectifs  $z_A$ ,  $z_B$ ,  $z_C$ .

$\frac{z_B - z_A}{z_C - z_A}$  a pour module  $\frac{AB}{AC}$  et pour argument une mesure de l'angle  $(\vec{AC}, \vec{AB})$ .

### III Applications

- **Alignement**

Les points  $A$ ,  $B$  et  $C$  sont alignés si, et seulement si,  $\frac{z_B - z_A}{z_C - z_A}$  est un réel.

- **Orthogonalité**

$\overrightarrow{AB}$  et  $\overrightarrow{AC}$  sont orthogonaux si, et seulement si,  $\frac{z_B - z_A}{z_C - z_A}$  est un imaginaire pur.

- **Triangle équilatéral**

Le triangle  $ABC$  est équilatéral, de sens direct, si, et seulement si,

$$z_C - z_A = e^{i\frac{\pi}{3}}(z_B - z_A).$$

- **Triangle rectangle isocèle**

Le triangle  $ABC$  est isocèle et rectangle en  $A$  si, et seulement si :

$$z_C - z_A = \pm i(z_B - z_A).$$

- **Points cocycliques ou alignés**

Soit  $A$ ,  $B$ ,  $C$  et  $D$  quatre points, deux à deux distincts, d'affixes respectifs  $z_A$ ,  $z_B$ ,  $z_C$ ,  $z_D$ . Ils sont cocycliques ou alignés si, et seulement si :

$$\left(\frac{z_B - z_C}{z_A - z_C}\right) / \left(\frac{z_B - z_D}{z_A - z_D}\right) \in \mathbb{R}.$$

## Application

Montrez qu'une condition nécessaire et suffisante pour que  $M_1(z_1)$ ,  $M_2(z_2)$  et  $M_3(z_3)$  soient, dans le plan complexe, les sommets d'un triangle équilatéral est :

$$z_1^2 + z_2^2 + z_3^2 - z_1z_2 - z_2z_3 - z_1z_3 = 0.$$

## Solution

Le triangle  $M_1M_2M_3$  est équilatéral si, et seulement si,  $M_1M_2 = M_1M_3$  et  $(\overrightarrow{M_1M_2}, \overrightarrow{M_1M_3}) = (\overrightarrow{u}, \overrightarrow{M_1M_3}) - (\overrightarrow{u}, \overrightarrow{M_1M_2}) = \pm \frac{\pi}{3} (2\pi)$ .

Cette condition nécessaire et suffisante se traduit par :

$$\begin{cases} |z_2 - z_1| = |z_3 - z_1| \\ \arg(z_3 - z_1) - \arg(z_2 - z_1) = \pm \frac{\pi}{3} (2\pi), \end{cases}$$

ce qui équivaut à :

$$z_3 - z_1 = (z_2 - z_1) e^{i\frac{\pi}{3}} \quad \text{ou} \quad z_3 - z_1 = (z_2 - z_1) e^{-i\frac{\pi}{3}}.$$

La condition cherchée peut s'écrire :

$$(z_3 - z_1 - (z_2 - z_1) e^{i\frac{\pi}{3}})(z_3 - z_1 - (z_2 - z_1) e^{-i\frac{\pi}{3}}) = 0.$$

En développant, il vient :

$$z_1^2 + z_2^2 + z_3^2 - z_1z_2 - z_2z_3 - z_1z_3 = 0.$$

## Application

Trouvez les points  $M$  d'affixe  $z$  tels que les images de  $z$ ,  $z^2$  et  $z^3$  forment un triangle rectangle.

## Solution

Si  $z = 0$  ou  $z = 1$ , le triangle est réduit à un point. Si  $z = -1$ , le triangle est aplati. Supposons donc que  $z$  est différent de ces trois valeurs, et notons  $M_1$ ,  $M_2$ ,  $M_3$  les images respectives de  $z$ ,  $z^2$ ,  $z^3$ . Trois cas sont à considérer.

• **Triangle rectangle en  $M_1$**

**Première solution**

Le triangle  $M_1M_2M_3$  est rectangle en  $M_1$  si, et seulement si :

$$\begin{aligned} \arg(z^3 - z) - \arg(z^2 - z) &= \pm \frac{\pi}{2} \iff \arg\left(\frac{z^3 - z}{z^2 - z}\right) = \arg(z + 1) = \pm \frac{\pi}{2} \\ &\iff z + 1 = ib \quad \text{soit} \quad z = -1 + ib \quad \text{avec } b \in \mathbb{R}. \end{aligned}$$

**Deuxième solution**

Le théorème de Pythagore s'écrit :

$$\begin{aligned} |z^3 - z|^2 + |z^2 - z|^2 &= |z^3 - z^2|^2 \\ &\iff |z|^2|z - 1|^2|z + 1|^2 + |z|^2|z - 1|^2 = |z|^4|z - 1|^2 \\ &\iff |z + 1|^2 + 1 = |z|^2. \end{aligned}$$

En posant  $z = x + iy$ , cette égalité devient :

$$(x + 1)^2 + y^2 + 1 = x^2 + y^2 \iff 2x + 2 = 0 \iff x = -1.$$

• **Triangle rectangle en  $M_2$**

**Première solution**

Le triangle  $M_1M_2M_3$  est rectangle en  $M_2$  si, et seulement si :

$$\arg(z^3 - z^2) - \arg(z - z^2) = \pm \frac{\pi}{2} = \arg(-z) \iff z = ib \quad \text{avec } b \in \mathbb{R}.$$

**Deuxième solution**

Le théorème de Pythagore s'écrit :

$$|z^3 - z^2|^2 + |z - z^2|^2 = |z^3 - z|^2 \iff |z|^2 + 1 = |z + 1|^2 \iff x = 0$$

• **Triangle rectangle en  $M_3$**

Dans ce cas, la solution utilisant le théorème de Pythagore devient préférable :

$$|z^2 - z^3|^2 + |z - z^3|^2 = |z^2 - z|^2 \iff |z|^2 + |z + 1|^2 = 1.$$

En posant  $z = x + iy$ , cette égalité devient  $x^2 + y^2 + x = 0$ .

Comme  $x^2 + y^2 + x = \left(x + \frac{1}{2}\right)^2 + y^2 - \frac{1}{4}$  il s'agit de l'équation du cercle (C) de centre  $\Omega\left(-\frac{1}{2}, 0\right)$  et de rayon  $R = \frac{1}{2}$ .

• **En conclusion**, l'ensemble cherché comporte la droite  $x = -1$ , la droite  $x = 0$ , le cercle (C), sauf les points d'affixes 0 et  $-1$ .

## I Polynômes à une indéterminée

### • Définitions

#### *Polynôme formel*

Un polynôme à une indéterminée, à coefficients dans un corps  $\mathbb{K}$ , est une suite de valeurs  $a_i$  de  $\mathbb{K}$ , nulle à partir d'un certain rang  $p$ . Un tel polynôme se note  $P$  ou  $P(X)$  :

$$P(X) = a_0 + a_1 X + \cdots + a_p X^p.$$

Les nombres  $a_i$  sont les coefficients du polynôme  $P$ .

Si  $P \neq 0$ , le plus grand entier  $p$  tel que  $a_p \neq 0$  est le degré du polynôme  $P$ . On le note  $d^\circ P$ , ou  $\deg P$ .

$a_p$  est le coefficient dominant de  $P$ . Lorsque  $a_p = 1$ , le polynôme est dit unitaire, ou normalisé.

Pour le polynôme nul  $P = 0$ , on convient de poser  $d^\circ P = -\infty$ .

L'ensemble des polynômes à une indéterminée  $X$ , à coefficients dans  $\mathbb{K}$ , se note  $\mathbb{K}[X]$ .

On note  $\mathbb{K}_n[X]$  l'ensemble des polynômes de degré inférieur ou égal à  $n$ .

#### *Fonction polynomiale*

$P = \sum_{i=0}^p a_i X^i$  étant un polynôme de  $\mathbb{K}[X]$ , la fonction polynomiale associée à  $P$

est l'application  $\tilde{P}$ , de  $\mathbb{K}$  dans  $\mathbb{K}$ , définie par :

$$x \mapsto \tilde{P}(x) = \sum_{i=0}^p a_i x^i.$$

Si  $\mathbb{K}$  est infini, vous pouvez confondre sans risque  $P$  et  $\tilde{P}$ . Ce n'est pas le cas si  $\mathbb{K}$  est fini.

### • Opérations

Soit  $P = \sum_{i=0}^p a_i X^i$  et  $Q = \sum_{j=0}^q b_j X^j$  deux éléments de  $\mathbb{K}[X]$ , et  $\lambda \in \mathbb{K}$ .

### Addition de deux polynômes

$$P + Q = \sum_{k=0}^r c_k X^k \quad \text{avec } r = \max(p, q) \text{ et } c_k = a_k + b_k.$$

On a :  $d^\circ(P + Q) \leq \max(d^\circ P, d^\circ Q)$ . Si  $d^\circ P \neq d^\circ Q$ , il y a égalité.

### Produit par un scalaire

$$\lambda P = \sum_{i=0}^p (\lambda a_i) X^i. \quad \text{Si } \lambda \neq 0, \text{ on a : } d^\circ(\lambda P) = d^\circ P.$$

### Produit de deux polynômes

$$PQ = \sum_{k=0}^{p+q} d_k X^k \quad \text{avec } d_k = \sum_{i+j=k} a_i b_j.$$

On a :  $d^\circ(PQ) = d^\circ P + d^\circ Q$ .

- Divisibilité**

Si  $A = BQ$  (avec  $Q \in \mathbb{K}[X]$ ), on dit que  $A$  est un multiple de  $B$ , ou que  $B$  est un diviseur de  $A$ .

On dit que  $A$  et  $B$  sont des polynômes associés lorsque  $A = \lambda B$ , avec  $\lambda \in K^*$ .

- Division euclidienne**

Soit  $A$  et  $B$  deux polynômes de  $\mathbb{K}[X]$ , avec  $B \neq 0$ . Il existe des polynômes uniques  $Q$  et  $R$  dans  $\mathbb{K}[X]$ , tels que :

$$A = BQ + R \quad \text{avec } d^\circ R < d^\circ B.$$

On dit que  $Q$  est le quotient, et  $R$  le reste, dans la division euclidienne de  $A$  par  $B$ .

- Polynôme dérivé**

Si  $\mathbb{K}$  est un sous-corps de  $\mathbb{C}$ , la définition et les propriétés du polynôme dérivé sont analogues à celles de la fonction associée.

## II Racines d'un polynôme

- Définition et caractérisation**

Une équation algébrique est de la forme  $\tilde{P}(x) = 0$  où  $P$  est un polynôme. Ses racines sont les zéros, ou racines, de  $P$ .

Un zéro  $\alpha$  de  $P$  est dit d'ordre  $k$ , ou de multiplicité  $k$  (avec  $k \in \mathbb{N}^*$ ), si  $\alpha$  est racine d'ordre  $k$  de l'équation  $\tilde{P}(x) = 0$ . Cela signifie qu'il existe  $Q \in \mathbb{K}[X]$  tel que  $P = (X - \alpha)^k Q$  avec  $Q(\alpha) \neq 0$ .

Pour  $\mathbb{K} = \mathbb{R}$  ou  $\mathbb{C}$ , un zéro  $\alpha$  de  $P$  est d'ordre  $\geq k$  si, et seulement si :

$$P(\alpha) = P'(\alpha) = \dots = P^{(k-1)}(\alpha) = 0.$$

L'ordre est égal à  $k$  si, en plus,  $P^{(k)}(\alpha) \neq 0$ .

- **Théorème de d'Alembert-Gauss**

Tout polynôme de  $\mathbb{C}[X]$  a au moins une racine dans  $\mathbb{C}$ .

On en déduit qu'un polynôme de  $\mathbb{C}[X]$ , de degré  $n$ , a exactement  $n$  racines dans  $\mathbb{C}$ , en comptant chaque racine autant de fois que son ordre de multiplicité.

- **Polynôme irréductible**

Un polynôme  $P$  de  $\mathbb{K}[X]$  est irréductible si  $d^\circ P \geq 1$ , et s'il n'est divisible que par les polynômes associés à 1 et à  $P$ .

- **Polynôme scindé**

Un polynôme  $P \in \mathbb{K}[X]$ , de degré  $n$ , est scindé s'il s'écrit comme produit de polynômes de degré 1, soit :

$$P = a_n \prod_{i=1}^r (X - \alpha_i)^{k_i} \quad \text{avec } a_n \neq 0.$$

- **Relations entre les coefficients et les racines**

Si  $P = \sum_{i=0}^n a_i X^i$  est de la forme ci-dessus, désignons par  $\sigma_p$  la somme des produits  $p$  à  $p$  des racines. On a la relation :

$$\sigma_p = (-1)^p \frac{a_{n-p}}{a_n}.$$

- **Décomposition d'un polynôme**

Tout polynôme de degré  $\geq 1$  se factorise en un produit d'un élément de  $\mathbb{K}^*$  et de polynômes irréductibles unitaires.

Cette décomposition est unique, à l'ordre près.

Dans  $\mathbb{C}[X]$ , les polynômes irréductibles sont les polynômes de degré 1.

Dans  $\mathbb{R}[X]$ , les polynômes irréductibles sont les polynômes de degré 1, et les polynômes  $aX^2 + bX + c$  avec  $b^2 - 4ac < 0$ .

Si  $P \in \mathbb{R}[X]$ , on peut le considérer dans  $\mathbb{C}[X]$ , et si  $\alpha$  est un zéro non réel de  $P$ , alors  $P$  admet aussi le conjugué  $\bar{\alpha}$  pour zéro, avec le même ordre de multiplicité que  $\alpha$ .

## Application

Déterminez les entiers naturels  $n$  tels que  $A_n = (X + 1)^n - X^n - 1$  soit divisible par  $P = X^2 + X + 1$ .

## Solution

On a  $X^2 + X + 1 = (X - j)(X - \bar{j})$  où  $j = \exp\left(i\frac{2\pi}{3}\right)$ .

Par conséquent,  $P$  divise  $A_n$  si, et seulement si,  $A_n(j) = 0$  et  $A_n(\bar{j}) = 0$ .

Et comme  $A_n \in \mathbb{R}[X]$ , il suffit que  $A_n(j) = 0$ .

La condition cherchée s'écrit donc  $(j + 1)^n - j^n - 1 = 0$ ,

ou encore, sachant que  $1 + j = -j^2$ ,  $(-1)^n j^{2n} - j^n - 1 = 0$ .

Compte-tenu de la périodicité des puissances de  $j$ , considérons trois cas, dans lesquels  $k \in \mathbb{N}$ .

– Si  $n = 3k$ , on a  $(-1)^n j^{2n} - j^n - 1 = (-1)^{3k} - 2 \neq 0$ .

– Si  $n = 3k + 1$ , on a  $(-1)^n j^{2n} - j^n - 1 = (-1)^{3k+1} j^2 - j - 1$ . Le résultat sera nul si, et seulement si,  $3k$  est pair, c'est-à-dire  $k$  pair.

– Si  $n = 3k + 2$ , on a  $(-1)^n j^{2n} - j^n - 1 = (-1)^{3k} j - j^2 - 1$ . Le résultat sera nul si, et seulement si,  $3k$  est impair, c'est-à-dire  $k$  impair.

Les entiers qui conviennent sont donc de la forme  $6p + 1$  ou  $6p + 5$ , avec  $p \in \mathbb{N}$ .

## Application

Décomposez  $P = X^8 + X^4 + 1$  en facteurs irréductibles dans  $\mathbb{R}[X]$ .

## Solution

On peut chercher les racines de  $P$  dans  $\mathbb{C}$  et les regrouper par paires de racines conjuguées. Mais on va plus vite avec les transformations algébriques :

$$X^8 + X^4 + 1 = (X^4 + 1)^2 - X^4 = (X^4 + 1 + X^2)(X^4 + 1 - X^2)$$

$$(X^4 + 1 + X^2) = (X^2 + 1)^2 - X^2 = (X^2 + 1 + X)(X^2 + 1 - X)$$

$$(X^4 + 1 - X^2) = (X^2 + 1)^2 - 3X^2 = (X^2 + 1 + \sqrt{3}X)(X^2 + 1 - \sqrt{3}X)$$

Donc :

$$P = (X^2 + X + 1)(X^2 - X + 1)(X^2 + \sqrt{3}X + 1)(X^2 - \sqrt{3}X + 1).$$

## Application

Déterminez le reste de la division euclidienne de  $A_n = (\cos \alpha + \sin \alpha X)^n$  par  $(X^2 + 1)^2$ .

## Solution

Il existe des polynômes  $Q_n$  et  $R_n$  de  $\mathbb{R}[X]$  uniques tels que :

$$(*) \quad (\cos \alpha + \sin \alpha X)^n = (X^2 + 1)^2 Q_n + R_n \quad \text{avec} \quad d^\circ R_n \leq 3.$$

Si  $n \leq 3$ , alors  $R_n = A_n$ .

Supposons donc que  $n \geq 4$ , et écrivons  $R_n = a + bX + cX^2 + dX^3$ .

En donnant à  $X$  la valeur  $i$ , on obtient  $R_n(i) = e^{in\alpha} = a - c + (b - d)i$ .

On en déduit :

$$\begin{cases} a - c &= \cos n\alpha \\ b - d &= \sin n\alpha \end{cases}$$

Dérivons l'égalité (\*) par rapport à  $X$ . Il vient :

$$\begin{aligned} n \sin \alpha (\cos \alpha + \sin \alpha X)^{n-1} \\ = (X^2 + 1)[(X^2 + 1) Q'_n + 4X Q_n] + b + 2cX + 3dX^2. \end{aligned}$$

En prenant la valeur en  $i$  des fonctions polynômes associées, on obtient :

$$n \sin \alpha e^{i(n-1)\alpha} = b - 3d + 2ci,$$

d'où :

$$\begin{cases} b - 3d &= n \sin \alpha \cos (n-1)\alpha \\ 2c &= n \sin \alpha \sin (n-1)\alpha. \end{cases}$$

Des quatre équations obtenues, on déduit les coefficients cherchés :

$$\begin{cases} a &= \frac{n}{2} \sin \alpha \sin (n-1)\alpha + \cos n\alpha \\ b &= \frac{1}{2} (-n \sin \alpha \cos (n-1)\alpha + 3 \sin n\alpha) \\ c &= \frac{n}{2} \sin \alpha \sin (n-1)\alpha \\ d &= \frac{1}{2} (-n \sin \alpha \cos (n-1)\alpha + \sin n\alpha). \end{cases}$$

## Application

Déterminez trois nombres complexes dont la somme est 2, la somme des carrés 2, la somme des cubes 8.

## Solution

L'énoncé fait penser aux relations entre les coefficients et les racines d'un polynôme. On va donc chercher les nombres  $x_1, x_2, x_3$  comme racines de :

$$(X - x_1)(X - x_2)(X - x_3) = X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$$

où :

$$\sigma_1 = x_1 + x_2 + x_3 ; \sigma_2 = x_1 x_2 + x_2 x_3 + x_3 x_1 ; \sigma_3 = x_1 x_2 x_3 .$$

On connaît  $\sigma_1 = 2$ , puis on calcule :

$$\begin{aligned} 4 &= (x_1 + x_2 + x_3)^2 = x_1^2 + x_2^2 + x_3^2 + 2\sigma_2 = 2 + 2\sigma_2 \quad \text{d'où } \sigma_2 = 1, \\ 8 &= (x_1 + x_2 + x_3)^3 \\ &= x_1^3 + x_2^3 + x_3^3 + 3(x_1 + x_2 + x_3)(x_1 x_2 + x_2 x_3 + x_3 x_1) - 3x_1 x_2 x_3 . \\ &= 8 + 6 - 3\sigma_3 \quad \text{d'où } \sigma_3 = 2 \end{aligned}$$

Les nombres cherchés sont donc les racines du polynôme :

$$P = X^3 - 2X^2 + X - 2 .$$

Comme  $P(2) = 0$ ,  $P$  est divisible par  $X - 2$ . Après avoir effectué la division on obtient :

$$P = (X - 2)(X^2 + 1) .$$

Les nombres cherchés sont donc : 2,  $i$ ,  $-i$ .

# Fractions rationnelles

## I Décomposition en éléments simples

### • Définitions

De façon analogue à un nombre rationnel quotient de deux entiers, on définit une fraction rationnelle  $\frac{A}{B}$  à partir des polynômes  $A$  et  $B$  avec  $B \neq 0$ .

$F = \frac{A}{B}$  étant une fraction rationnelle irréductible, la fonction rationnelle associée à  $F$  est la fonction  $\tilde{F}$ , de  $\mathbb{K}$  dans  $\mathbb{K}$ , définie par :

$$x \mapsto \tilde{F}(x) = \frac{\tilde{A}(x)}{\tilde{B}(x)} \text{ quand } \tilde{B}(x) \neq 0.$$

$\tilde{F}$  n'est pas définie pour les zéros de  $B$ . Ce sont les pôles de  $F$ .

### • Forme générale de la décomposition

Une fraction rationnelle, de forme irréductible  $F = \frac{A}{B}$ , s'écrit de façon unique, sous la forme :

$$F = E + \frac{R}{B} \text{ avec } d^\circ R < d^\circ B.$$

$E$  est la partie entière et  $\frac{R}{B}$  la partie fractionnaire de  $F$ .

### • Partie polaire quand $\mathbb{K} = \mathbb{C}$

Si la factorisation de  $B$  en polynômes irréductibles comporte un terme  $(X - a)^k$  avec  $k \in \mathbb{N}^*$ , on appelle partie polaire de  $F$  relative à ce terme une somme d'éléments simples du type :

$$\frac{\alpha_k}{(X - a)^k} + \frac{\alpha_{k-1}}{(X - a)^{k-1}} + \cdots + \frac{\alpha_1}{X - a}.$$

Pour une fraction  $F$  donnée, les complexes  $\alpha_i$  existent et sont uniques.

- **Théorème de décomposition**

Toute fraction rationnelle, écrite sous forme irréductible, est égale, de façon unique, à la somme de sa partie entière et des parties polaires relatives à chacun des facteurs irréductibles intervenant dans la décomposition de  $B$ .

## II Méthodes pratiques de décomposition

- **Plan d'étude**

On met  $F$  sous forme irréductible en simplifiant par le PGCD du numérateur et du dénominateur.

On obtient  $E$  et  $R$  à l'aide de la division euclidienne de  $A$  par  $B$ .

On factorise  $B$  en polynômes irréductibles.

On écrit la forme littérale de la décomposition en éléments simples de  $F$ , ou de  $\frac{R}{B}$ .

On détermine les coefficients à l'aide de diverses méthodes.

- **Détermination des coefficients**

La méthode la plus rudimentaire consiste à réduire au même dénominateur la forme décomposée et à identifier les numérateurs.

Vous pouvez remplacer  $X$  par des valeurs numériques, différentes des pôles.

Sachant que la décomposition est unique, si  $F$  est paire, ou impaire, on obtient des relations entre les coefficients.

En utilisant la fraction sans partie entière,  $\lim_{x \rightarrow \infty} x F(x)$  donne une relation entre coefficients.

En multipliant  $F$  par  $(X - a)^k$  et en remplaçant  $X$  par  $a$ , on obtient  $\alpha_k$ .

Si  $a$  est un pôle simple, la partie polaire associée  $\frac{\alpha}{X - a}$  vérifie :

$$\alpha = \frac{A(a)}{B'(a)}.$$

Soit  $P$  un polynôme dont les racines sont  $a_1, \dots, a_k$ , d'ordre de multiplicité respectifs  $m_1, \dots, m_k$ . On a :

$$\frac{P'(X)}{P(X)} = \sum_{i=1}^k \frac{m_i}{X - a_i}.$$

## Application

Décomposez en éléments simples la fraction rationnelle :

$$F = \frac{X}{(X+1)^2 (X-1)^2}.$$

## Solution

Il n'y a pas de partie entière, puisque le degré du numérateur est strictement inférieur à celui du dénominateur.

La décomposition de  $F$  en éléments simples est de la forme :

$$F = \frac{a}{(X+1)^2} + \frac{b}{X+1} + \frac{c}{(X-1)^2} + \frac{d}{(X-1)},$$

où  $a, b, c, d$  sont des réels à déterminer.

En remplaçant  $X$  par  $-1$  dans  $(X+1)^2 F$ , on obtient  $a = -\frac{1}{4}$ .

En remplaçant  $X$  par  $1$  dans  $(X-1)^2 F$ , on obtient  $c = \frac{1}{4}$ .

La fonction rationnelle associée à  $F$  est impaire. L'unicité de la décomposition en éléments simples entraîne alors :

$$a = -c \quad \text{et} \quad b = d.$$

En multipliant par  $X$  et en faisant tendre  $X$  vers  $+\infty$ , on obtient de plus  $b + d = 0$ . Par conséquent  $b = d = 0$ . La décomposition est donc :

$$F = \frac{1}{4} \left( \frac{-1}{(X+1)^2} + \frac{1}{(X-1)^2} \right).$$

## Application

Pour  $n \in \mathbb{N}^*$ , on pose  $u_n = \frac{2n^3 + 6n^2 + 7n + 2}{n^2(n+1)^2(n+2)}$ .

Déterminez la limite de la suite  $(v_n)$  définie pour  $n \in \mathbb{N}^*$  par  $v_n = \sum_{p=1}^n u_p$ .

## Solution

Considérons la fraction rationnelle :

$$F = \frac{2X^3 + 6X^2 + 7X + 2}{X^2(X+1)^2(X+2)}.$$

La forme de sa décomposition en éléments simples est :

$$F = \frac{a}{X} + \frac{b}{X^2} + \frac{c}{X+1} + \frac{d}{(X+1)^2} + \frac{e}{X+2}$$

où  $a, b, c, d$  et  $e$  sont des réels à déterminer.

En remplaçant  $X$  par 0 dans  $X^2 F$ , on obtient  $b = 1$ .

En remplaçant  $X$  par  $-1$  dans  $(X+1)^2 F$ , on obtient  $d = -1$ .

En remplaçant  $X$  par  $-2$  dans  $(X+2) F$ , on obtient  $e = -1$ .

On a  $\lim_{X \rightarrow +\infty} X F(X) = 0 = a + c + e$ , ce qui donne  $a + c = 1$ .

En considérant  $F(1) = \frac{17}{12}$  on obtient  $1 = a + \frac{c}{2}$  d'où  $a = 1$  et  $c = 0$ .

En définitive :

$$F = \frac{1}{X} + \frac{1}{X^2} - \frac{1}{(X+1)^2} - \frac{1}{X+2}.$$

On a donc :

$$v_n = \underbrace{\sum_{p=1}^n \frac{1}{p} - \sum_{p=1}^n \frac{1}{p+2}}_{1 + \frac{1}{2} - \frac{1}{n+1} - \frac{1}{n+2}} + \underbrace{\sum_{p=1}^n \frac{1}{p^2} - \sum_{p=1}^n \frac{1}{(p+1)^2}}_{1 - \frac{1}{(n+1)^2}}$$

ce qui donne après simplification :

$$v_n = \frac{5}{2} - \frac{1}{n+1} - \frac{1}{n+2} - \frac{1}{(n+1)^2} \text{ d'où : } \lim_{n \rightarrow +\infty} v_n = \frac{5}{2}.$$

## I Généralités

Un système de  $n$  équations linéaires à  $p$  inconnues, à coefficients dans  $\mathbb{K}$ , est de la forme :

$$(S) \begin{cases} a_{11}x_1 + \cdots + a_{1p}x_p &= b_1 \\ \vdots & \vdots \\ a_{n1}x_1 + \cdots + a_{np}x_p &= b_n \end{cases}$$

Les coefficients  $a_{ij}$  et les seconds membres  $b_i$  sont des éléments donnés de  $\mathbb{K}$ .

Les inconnues  $x_1, \dots, x_p$  sont à chercher dans  $\mathbb{K}$ .

Le système homogène associé à  $(S)$  est le système obtenu en remplaçant les  $b_i$  par 0.

Une solution est un  $p$ -uplet  $(x_1, \dots, x_p)$  qui vérifie  $(S)$ . Résoudre  $(S)$ , c'est chercher toutes les solutions.

Un système est impossible, ou incompatible, s'il n'admet pas de solution.

Deux systèmes sont équivalents s'ils ont les mêmes solutions.

## II Méthodes de résolution

- **Systèmes en escalier**

### *Réduction*

Quand un système contient une équation du type :

$$0x_1 + \cdots + 0x_n = b,$$

si  $b \neq 0$ , le système est impossible ;

si  $b = 0$ , on peut supprimer cette équation, ce qui conduit au système réduit.

### *Définition*

Un système  $(S)$  est en escalier, ou échelonné, si, après réduction, le nombre de premiers coefficients nuls successifs de chaque équation est strictement croissant.

- **Méthode du pivot de Gauss**

En permutant éventuellement deux inconnues et deux équations, on peut supposer que  $a_{11} \neq 0$ .

Pour  $i > 1$ , les transformations  $E_i \leftarrow E_i - \frac{a_{i1}}{a_{11}} E_1$  (remplacement de  $E_i$  par

$E_i - \frac{a_{i1}}{a_{11}} E_1$ ) conduisent à un système équivalent et éliminent l'inconnue  $x_1$  dans

les équations autres que  $E_1$ .

Le terme  $a_{11}$  est le pivot de l'étape de l'algorithme.

En itérant le procédé, on aboutit à un système en escalier.

- **Rang d'un système**

Le nombre d'équations du système (non impossible) réduit en escalier obtenu par la méthode de Gauss est le rang  $r$  du système ( $S$ ).

- **Inconnues principales, inconnues secondaires**

Soit  $r$  le rang de ( $S$ ) et  $p$  le nombre d'inconnues.

Si  $r = p$ , ( $S$ ) a une solution unique. On dit que le système est de Cramer.

Si  $p > r$ , ( $S$ ) a une infinité de solutions. Les  $r$  inconnues qui figurent au début des  $r$  équations issues de la méthode de Gauss sont les inconnues principales. Elles peuvent se calculer de façon unique en fonction des  $p - r$  autres inconnues, dites inconnues secondaires.

Le choix des inconnues principales et secondaires d'un système est largement arbitraire. Mais leur nombre est toujours le même.

## Application

Résolvez le système linéaire :

$$(S) \begin{cases} x_1 + 2x_2 - x_3 = 1 \\ 2x_1 - 3x_2 + 2x_3 = -2 \\ 3x_1 + x_2 - x_3 = 3 \end{cases}$$

## Solution

L'algorithme du pivot de Gauss permet d'écrire des systèmes équivalents :

$$\begin{aligned} (S) &\iff \begin{cases} x_1 + 2x_2 - x_3 = 1 \\ 7x_2 - 4x_3 = 4 \\ 5x_2 - 2x_3 = 0 \end{cases} & \begin{array}{l} L_1 \leftarrow L_1 \\ L_2 \leftarrow 2L_1 - L_2 \\ L_3 \leftarrow 3L_1 - L_3 \end{array} \\ &\iff \begin{cases} x_1 + 2x_2 - x_3 = 1 \\ 7x_2 - 4x_3 = 4 \\ 6x_3 = -20 \end{cases} & \begin{array}{l} L_1 \leftarrow L_1 \\ L_2 \leftarrow L_2 \\ L_3 \leftarrow -5L_2 + 7L_3 \end{array} \end{aligned}$$

Le système obtenu est triangulaire à trois équations. Le système (S) est donc de rang 3 et admet une solution unique. On peut finir la résolution par des substitutions, ou poursuivre avec le même algorithme (méthode de Gauss-Jordan).

$$\begin{aligned} &\iff \begin{cases} 6x_1 + 12x_2 = -14 \\ 21x_2 = -28 \\ 6x_3 = -20 \end{cases} & \begin{array}{l} L_1 \leftarrow 6L_1 + L_3 \\ L_2 \leftarrow 3L_2 + 2L_3 \\ L_3 \leftarrow L_3 \end{array} \\ &\iff \begin{cases} -42x_1 = -14 \\ 21x_2 = -28 \\ 6x_3 = -20 \end{cases} & \begin{array}{l} L_1 \leftarrow -7L_1 + 4L_2 \\ L_2 \leftarrow L_2 \\ L_3 \leftarrow L_3 \end{array} \end{aligned}$$

La solution de (S) est donc :

$$x_1 = \frac{1}{3} ; \quad x_2 = -\frac{4}{3} ; \quad x_3 = -\frac{10}{3}.$$

## Application

En discutant suivant les valeurs de  $a, b, c$ , résolvez le système linéaire :

$$(S) \begin{cases} 3x - 5y + z = a \\ x + 2y - 3z = b \\ 5x - 12y + 5z = c \end{cases}$$

## Solution

L'algorithme du pivot de Gauss permet d'écrire des systèmes équivalents :

$$\begin{aligned} (S) &\Leftrightarrow \begin{cases} x + 2y - 3z = b \\ 11y - 10z = 3b - a \\ 22y - 20z = 5b - c \end{cases} & \begin{array}{l} L_1 \leftarrow L_2 \\ L_2 \leftarrow 3L_2 - L_1 \\ L_3 \leftarrow 5L_2 - L_3 \end{array} \\ &\Leftrightarrow \begin{cases} x + 2y - 3z = b \\ 11y - 10z = 3b - a \\ 0 = b - 2a + c \end{cases} & \begin{array}{l} L_1 \leftarrow L_1 \\ L_2 \leftarrow L_2 \\ L_3 \leftarrow 2L_2 - L_3 \end{array} \end{aligned}$$

– Si  $b - 2a + c \neq 0$ , le système est impossible.

– Si  $b - 2a + c = 0$ , le système est de rang 2.

On peut, par exemple, prendre  $z$  comme inconnue secondaire et calculer  $x$  et  $y$ , ce qui donne l'ensemble des solutions exprimées avec un paramètre :

$$\begin{cases} x = \frac{1}{11}(2a + 5b + 13\lambda) \\ y = \frac{1}{11}(-a + 3b + 10\lambda) \\ z = \lambda \end{cases} \quad \lambda \in \mathbb{R}.$$

# Espaces vectoriels

## I Définitions et premières propriétés

### • Espace vectoriel

Soit  $\mathbb{K}$  un corps d'éléments neutres notés 0 et 1.

On dit qu'un ensemble non vide  $E$  est un espace vectoriel sur  $\mathbb{K}$ , ou est un  $\mathbb{K}$ -espace vectoriel, s'il est muni :

- d'une loi de composition interne notée  $+$  ;
  - d'une loi de composition externe sur  $\mathbb{K}$ , c'est-à-dire d'une application qui à  $(\lambda, x) \in \mathbb{K} \times E$  fait correspondre  $\lambda x \in E$ , telles que :
- $(E, +)$  est un groupe commutatif,

$$\forall \lambda \in \mathbb{K} \quad \forall \mu \in \mathbb{K} \quad \forall x \in E \quad \forall y \in E \quad (\lambda \mu) x = \lambda (\mu x) \quad ;$$

$$(\lambda + \mu) x = \lambda x + \mu x \quad ; \quad \lambda (x + y) = \lambda x + \lambda y \quad ; \quad 1 x = x.$$

Les éléments de  $E$  sont des vecteurs ; les éléments de  $\mathbb{K}$  sont des scalaires.

### • Exemples

- L'ensemble des vecteurs du plan ou de l'espace est un  $\mathbb{R}$ -espace vectoriel.
- $\mathbb{K}$  est un espace vectoriel sur  $\mathbb{K}$ .
- $\mathbb{C}$  est un  $\mathbb{C}$ -espace vectoriel, mais aussi un  $\mathbb{R}$ -espace vectoriel.
- Le produit  $E_1 \times \cdots \times E_n$  de  $n$  espaces vectoriels sur le même corps  $\mathbb{K}$  est un  $\mathbb{K}$ -espace vectoriel pour les lois :

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

$$\lambda (x_1, \dots, x_n) = (\lambda x_1, \dots, \lambda x_n).$$

- L'ensemble  $\mathcal{F}(X, F)$  des applications d'un ensemble  $X$  dans un espace vectoriel  $F$ , est un espace vectoriel pour les opérations  $f + g$  et  $\lambda f$ .
- L'ensemble  $\mathbb{K}[X]$  des polynômes à coefficients dans  $\mathbb{K}$ , l'ensemble  $\mathbb{K}_n[X]$  des polynômes de degré  $\leq n$ , sont des  $\mathbb{K}$ -espaces vectoriels.

### • Propriété

$$\forall \lambda \in \mathbb{K} \quad \forall x \in E \quad \lambda x = 0_E \iff \lambda = 0_{\mathbb{K}} \text{ ou } x = 0_E.$$

De ce fait, les éléments neutres pour l'addition de  $\mathbb{K}$  et de  $E$ ,  $0_{\mathbb{K}}$  et  $0_E$ , seront représentés par le même symbole  $0$  sans inconvénient.

## II Sous-espaces vectoriels

### • Définition

Une partie non vide  $F$  d'un  $\mathbb{K}$ -espace vectoriel  $E$  est un sous-espace vectoriel de  $E$  si elle est stable pour les deux lois, et si la restriction à  $F$  des lois de  $E$  définit dans  $F$  une structure d'espace vectoriel.

En fait, il faut et il suffit que  $F$  vérifie :

$$\forall \lambda \in \mathbb{K} \quad \forall x \in F \quad \forall y \in F \quad x + y \in F \quad \lambda x \in F ;$$

ou encore :

$$\forall \lambda \in \mathbb{K} \quad \forall x \in F \quad \forall y \in F \quad x + \lambda y \in F .$$

Pour montrer que  $F$  n'est pas vide, on vérifie en général que  $0 \in F$ .

### • Sous-espace engendré par une partie

– Toute intersection de sous-espaces vectoriels de  $E$  est un sous-espace vectoriel de  $E$ .

Attention, la réunion de sous-espaces vectoriels n'est pas en général un sous-espace vectoriel.

– L'intersection  $F$  de tous les sous-espaces vectoriels de  $E$  contenant une partie  $A$  donnée est le sous-espace vectoriel engendré par  $A$ . C'est le plus petit (au sens de l'inclusion) sous-espace vectoriel contenant  $A$ .

On dit aussi que  $A$  est une partie génératrice de  $F$ . On note  $F = \text{Vect}(A)$ .

– Le sous-espace vectoriel engendré par  $A$  est égal à l'ensemble des combinaisons linéaires finies de vecteurs de  $A$ , c'est-à-dire l'ensemble des vecteurs du type :

$$\sum_{i=1}^n \lambda_i x_i \quad \text{avec } n \in \mathbb{N}^*, \quad \forall i \quad \lambda_i \in \mathbb{K} \quad x_i \in A .$$

### • Somme de deux sous-espaces vectoriels

$E_1$  et  $E_2$  étant deux sous-espaces vectoriels de  $E$ , on appelle somme de  $E_1$  et de  $E_2$ , et on note  $E_1 + E_2$ , l'ensemble des vecteurs du type  $x_1 + x_2$  où  $x_1 \in E_1$  et  $x_2 \in E_2$ .

$E_1 + E_2$  est le sous-espace vectoriel engendré par  $E_1 \cup E_2$ .

- **Somme directe de deux sous-espaces vectoriels**

### Définitions

Quand tout vecteur  $x$  de  $F = E_1 + E_2$  s'écrit, de façon unique, sous la forme  $x = x_1 + x_2$  avec  $x_1 \in E_1$  et  $x_2 \in E_2$ , on dit que  $F$  est somme directe de  $E_1$  et de  $E_2$ , et on note  $F = E_1 \oplus E_2$ .

On dit aussi que  $E_1$  et  $E_2$  sont supplémentaires dans  $F$ .

### Théorème

$$E = E_1 \oplus E_2 \iff E = E_1 + E_2 \quad \text{et} \quad E_1 \cap E_2 = \{0\}.$$

- **Généralisation**

### Somme de sous-espaces vectoriels

Soit  $(E_i)_{i \in I}$  une famille finie de sous-espaces vectoriels d'un espace vectoriel  $E$ .

On appelle somme des  $E_i$ , et on note  $\sum_{i \in I} E_i$ , l'ensemble des vecteurs du type  $\sum_{i \in I} x_i$

où  $x_i \in E_i$  pour tout  $i \in I$ .

$\sum_{i \in I} E_i$  est le sous-espace vectoriel engendré par  $\bigcup_{i \in I} E_i$ .

Si  $I = \{1, \dots, n\}$ , la somme se note aussi  $E_1 + \dots + E_n$ .

### Somme directe de sous-espaces vectoriels

Quand tout vecteur  $x$  de  $\sum_{i \in I} E_i$  s'écrit de façon unique sous la forme  $\sum_{i \in I} x_i$  avec

$x_i \in E_i$  pour tout  $i \in I$ , on dit que la somme des  $E_i$  est directe et on la note  $\bigoplus_{i \in I} E_i$ .

Si  $I = \{1, \dots, n\}$ , on note aussi  $E_1 \oplus \dots \oplus E_n$ .

Pour démontrer que la somme des  $E_i$  est directe, la méthode la plus rapide est de partir d'une somme nulle  $x_1 + \dots + x_n = 0$  avec  $x_i \in E_i$  pour tout  $i$ , et de démontrer que cela entraîne que tous les  $x_i$  sont nuls.

## Application

Dans  $\mathbb{R}^3$  considéré comme  $\mathbb{R}$ -espace vectoriel, les parties suivantes sont-elles des sous-espaces vectoriels ?

1.  $E_1 = \{(x, y, z) \in \mathbb{R}^3 ; x + y = 0\}$ ;
2.  $E_2 = \{(x, y, z) \in \mathbb{R}^3 ; xy = 0\}$ .

## Solution

1.  $E_1$  est l'ensemble des vecteurs de  $\mathbb{R}^3$  de la forme

$$(x, -x, z) = x(1, -1, 0) + z(0, 0, 1) \text{ avec } x \text{ et } z \text{ réels quelconques.}$$

$E_1$  est donc égal à  $\text{Vect}((1, -1, 0), (0, 0, 1))$ , ce qui prouve que c'est un sous-espace vectoriel de  $\mathbb{R}^3$  qui admet  $((1, -1, 0), (0, 0, 1))$  comme famille génératrice.

2. Les vecteurs  $(1, 0, 0)$  et  $(0, 1, 0)$  appartiennent à  $E_2$  alors que ce n'est pas le cas de leur somme  $(1, 1, 0)$ .

$E_2$  n'est donc pas un sous-espace vectoriel de  $\mathbb{R}^3$ .

## Application

Soit  $x_1, \dots, x_n$  des vecteurs d'un espace vectoriel  $E$ .

On pose  $y_1 = \sum_{i=1}^n \lambda_i x_i$  avec  $\lambda_1 \neq 0$ . Montrez que :

$$\text{Vect}(y_1, x_2, \dots, x_n) = \text{Vect}(x_1, x_2, \dots, x_n).$$

## Solution

Tout vecteur  $z$  de  $\text{Vect}(y_1, x_2, \dots, x_n)$  peut s'écrire sous la forme

$z = \alpha_1 y_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$  où les  $\alpha_i$  sont des scalaires.

On a donc aussi  $z = \alpha_1 \lambda_1 x_1 + (\alpha_1 \lambda_2 + \alpha_2) x_2 + \dots + (\alpha_1 \lambda_n + \alpha_n) x_n$ ,

ce qui prouve que  $z \in \text{Vect}(x_1, x_2, \dots, x_n)$ .

Réciproquement, tout vecteur de  $\text{Vect}(x_1, x_2, \dots, x_n)$  s'écrit :

$$\begin{aligned} z &= \beta_1 x_1 + \dots + \beta_n x_n \\ &= \frac{\beta_1}{\lambda_1} (\lambda_1 x_1 + \dots + \lambda_n x_n) + \left(\beta_2 - \frac{\beta_1 \lambda_2}{\lambda_1}\right) x_2 + \dots + \left(\beta_n - \frac{\beta_1 \lambda_n}{\lambda_1}\right) x_n. \end{aligned}$$

Il appartient donc aussi à  $\text{Vect}(y_1, x_2, \dots, x_n)$ .

La double inclusion que nous venons de démontrer prouve l'égalité :

$$\text{Vect}(y_1, x_2, \dots, x_n) = \text{Vect}(x_1, x_2, \dots, x_n).$$

Comme l'espace vectoriel engendré n'est pas modifié par l'opération élémentaire effectuée, nous obtenons un outil efficace dans la recherche du rang d'une famille de vecteurs.

## Application

Déterminez les réels  $x$  et  $y$  pour que le vecteur  $(2, 3, x, y)$  appartienne au sous-espace vectoriel de  $\mathbb{R}^4$  engendré par  $(2, -1, 3, 5)$  et  $(1, 3, 7, 2)$ .

## Solution

Pour que le vecteur  $(2, 3, x, y)$  appartienne au sous-espace vectoriel de  $\mathbb{R}^4$  engendré par  $(2, -1, 3, 5)$  et  $(1, 3, 7, 2)$ , il faut et il suffit qu'il existe des réels  $\alpha$  et  $\beta$  tels que :

$$(2, 3, x, y) = \alpha (2, -1, 3, 5) + \beta (1, 3, 7, 2),$$

soit :

$$\begin{cases} 2\alpha + \beta = 2 & (1) \\ -\alpha + 3\beta = 3 & (2) \\ 3\alpha + 7\beta = x & (3) \\ 5\alpha + 2\beta = y & (4) \end{cases}$$

La résolution du sous-système formé par les équations (1) et (2) donne  $\alpha = \frac{3}{7}$  et  $\beta = \frac{8}{7}$ .

Pour que les équations (3) et (4) soient compatibles, il faut que  $x$  et  $y$  vérifient les égalités obtenues en reportant ces valeurs, soit  $x = \frac{65}{7}$  et  $y = \frac{31}{7}$ .

## Application

Soit  $\mathcal{F}(\mathbb{R}, \mathbb{R})$  l'espace vectoriel des fonctions de  $\mathbb{R}$  dans  $\mathbb{R}$ . On désigne par  $\mathcal{P}$  l'ensemble des fonctions paires et par  $\mathcal{I}$  l'ensemble des fonctions impaires.

Démontrez que  $\mathcal{F}(\mathbb{R}, \mathbb{R}) = \mathcal{P} \oplus \mathcal{I}$ .

Quelle est la décomposition de la fonction exponentielle ?

## Solution

• Démontrons d'abord l'unicité d'une décomposition. Soit  $f$  une fonction quelconque de  $\mathbb{R}$  dans  $\mathbb{R}$  et supposons qu'il existe une fonction paire  $g$  et une fonction impaire  $h$  telles que  $f = g + h$ . On a alors :

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

$$\forall x \in \mathbb{R} \quad f(-x) = g(-x) + h(-x) = g(x) - h(x).$$

On a donc, pour tout  $x \in \mathbb{R}$ ,  $g(x) = \frac{f(x) + f(-x)}{2}$  et  $h(x) = \frac{f(x) - f(-x)}{2}$ , ce qui prouve l'unicité d'une éventuelle décomposition.

• Le calcul précédent va inspirer la démonstration de l'existence d'une décomposition. Soit  $f$  une fonction quelconque de  $\mathbb{R}$  dans  $\mathbb{R}$ .

Considérons les fonctions  $g$  et  $h$ , de  $\mathbb{R}$  dans  $\mathbb{R}$ , définie pour tout  $x$  par :

$$g(x) = \frac{f(x) + f(-x)}{2} \quad \text{et} \quad h(x) = \frac{f(x) - f(-x)}{2}.$$

On a bien :

$$\forall x \in \mathbb{R} \quad f(x) = g(x) + h(x), \text{ soit } f = g + h.$$

et, d'autre part :

$$\forall x \in \mathbb{R} \quad g(-x) = \frac{f(-x) + f(x)}{2} = g(x), \text{ soit } g \text{ paire ;}$$

$$\forall x \in \mathbb{R} \quad h(-x) = \frac{f(-x) - f(x)}{2} = -h(x), \text{ soit } h \text{ impaire.}$$

On a donc décomposé  $f$  comme somme d'une fonction paire et d'une fonction impaire, ce qui achève de démontrer que  $\mathcal{F}(\mathbb{R}, \mathbb{R}) = \mathcal{P} \oplus \mathcal{I}$ .

• Si  $f$  est la fonction exponentielle,  $g$  est la fonction cosinus hyperbolique et  $h$  la fonction sinus hyperbolique.

# Espaces vectoriels de dimension finie

## I Cas d'un espace vectoriel

### • Dépendance et indépendance linéaire

On dit qu'une famille  $(x_1, \dots, x_n)$  de vecteurs de  $E$  est une famille libre, ou que les vecteurs sont linéairement indépendants, si :

$$\sum_{i=1}^n \lambda_i x_i = 0 \implies \forall i \in \{1, \dots, n\} \quad \lambda_i = 0.$$

Dans le cas contraire, on dit que la famille est liée, ou que les vecteurs sont linéairement dépendants.

Toute sous-famille non vide d'une famille libre est libre.

Pour qu'une famille  $(x_1, \dots, x_n)$  soit liée, il faut, et il suffit, que l'un de ses éléments soit combinaison linéaire des autres.

Cas particuliers : une famille qui contient le vecteur 0 est liée ; deux vecteurs sont liés si, et seulement si, ils sont colinéaires.

### • Bases

- On appelle base d'un espace vectoriel  $E$  toute famille libre de  $E$  qui engendre  $E$ .
- La famille  $(e_1, \dots, e_n)$  est une base de  $E$  si, et seulement si, tout vecteur  $x$  de  $E$  peut s'écrire de façon unique sous la forme :

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

Les scalaires  $x_i$  sont les composantes du vecteur  $x$ .

- Théorème de la base incomplète

Si  $E$  est un espace vectoriel non réduit à  $\{0\}$ , toute famille libre de  $E$  peut être complétée en une base de  $E$ .

- Tout espace vectoriel non réduit à  $\{0\}$  possède au moins une base.

Attention à ne jamais écrire ou dire la base de  $E$ , car il n'y a pas unicité.

- **Dimension d'un espace vectoriel**

Si  $E$  possède une base comportant un nombre fini  $n$  de vecteurs, on dit que  $E$  est de dimension finie.

Dans ce cas, toute base de  $E$  comporte aussi  $n$  vecteurs. On dit que  $n$  est la dimension de  $E$  ; on la note  $\dim E$ .

On convient que l'espace vectoriel  $\{0\}$  est de dimension nulle.

- **Recherche de bases**

Soit  $E$  un espace vectoriel de dimension finie  $n$ .

Toute famille libre de  $E$  a au plus  $n$  vecteurs. Si elle comporte  $n$  vecteurs, c'est une base.

Toute famille génératrice de  $E$  a au moins  $n$  vecteurs. Si elle comporte  $n$  vecteurs, c'est une base.

Si on connaît déjà la dimension  $n$  de  $E$ , et si on considère une famille de  $n$  vecteurs, pour démontrer que c'est une base, il suffit de démontrer : soit que la famille est libre, soit que la famille est génératrice.

- **Dimension d'un produit cartésien  $E \times F$**

Soit  $E$  et  $F$  deux espaces vectoriels de dimensions finies.

Si  $(e_1, \dots, e_n)$  est une base de  $E$ , et  $(f_1, \dots, f_p)$  une base de  $F$ , alors l'ensemble des couples  $(e_i, 0)$  et  $(0, f_j)$  où  $1 \leq i \leq n$  et  $1 \leq j \leq p$ , est une base de  $E \times F$ .

Par conséquent :  $\dim(E \times F) = \dim E + \dim F$ .

## II Cas d'un sous-espace vectoriel

- **Dimension d'un sous-espace vectoriel**

Soit  $E$  un espace vectoriel de dimension finie et  $F$  un sous-espace vectoriel de  $E$ .

–  $F$  est alors de dimension finie, et l'on a :  $\dim F \leq \dim E$ .

– Si  $\dim F = \dim E$ , alors  $F = E$ .

L'égalité des dimensions ne suffit pas pour conclure que  $F = E$ . Il faut aussi une inclusion de l'un des espaces vectoriels dans l'autre.

– Si  $\dim F = \dim E - 1$ , on dit que  $F$  est un hyperplan de  $E$ .

Comme exemples d'hyperplans, vous pouvez penser à une droite dans le plan ou à un plan dans l'espace à trois dimensions.

- **Dimension d'une somme**

– Si  $F$  et  $G$  sont deux sous-espaces vectoriels de  $E$ , on a :

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

En particulier, si  $F$  et  $G$  sont en somme directe :

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

– Tout sous-espace vectoriel  $F$  de  $E$  admet des supplémentaires, qui ont tous pour dimension :  $\dim E - \dim F$ .

–  $F$  et  $G$  sont supplémentaires dans  $E$  si, et seulement si, en réunissant une base de  $F$  et une base de  $G$ , on obtient une base de  $E$ .

On dit qu'on a choisi une base de  $E$  adaptée à la somme directe.

Attention à ne pas partir d'une base de  $E$ , car il n'y a aucune raison de pouvoir en extraire une base de  $F$  et une base de  $G$ , ni même des vecteurs de  $F$  ou de  $G$ .

- **Généralisation**

Soit  $E$  un espace vectoriel de dimension finie et des sous-espaces vectoriels  $E_i$  de  $E$  en nombre fini.

Si la somme  $\bigoplus_{i \in I} E_i$  est directe, alors :

$$\dim \bigoplus_{i \in I} E_i = \sum_{i \in I} \dim E_i.$$

Pour que  $E = \bigoplus_{i \in I} E_i$ , il faut et il suffit que :

$$\dim E = \sum_{i \in I} \dim E_i.$$

Si aucun  $E_i$  n'est réduit à  $\{0\}$ , la réunion d'une base de chaque  $E_i$  constitue une base de  $E$  si, et seulement si,  $E = \bigoplus_{i \in I} E_i$ .

- **Rang d'une famille de vecteurs**

Le rang d'une famille finie de vecteurs est la dimension du sous-espace vectoriel qu'ils engendrent.

C'est aussi le nombre maximum de vecteurs linéairement indépendants que l'on peut extraire de la famille.

## Application

Soit le  $\mathbb{R}$ -espace vectoriel  $\mathcal{F}(]-1, 1[, \mathbb{R})$ .

On considère le sous-espace vectoriel  $E$  engendré par  $(f_1, f_2, f_3, f_4)$  où les  $f_i$  sont les fonctions de  $] -1, 1[$  dans  $\mathbb{R}$  définies par :

$$\begin{aligned} f_1(x) &= \sqrt{\frac{1+x}{1-x}} & ; & \quad f_2(x) = \sqrt{\frac{1-x}{1+x}} ; \\ f_3(x) &= \frac{1}{\sqrt{1-x^2}} & ; & \quad f_4(x) = \frac{x}{\sqrt{1-x^2}} . \end{aligned}$$

Déterminez une base de  $E$ . Déduisez-en la dimension de  $E$ .

## Solution

$$\forall x \in ]-1, 1[ \quad f_1(x) + f_2(x) = \frac{1+x+1-x}{\sqrt{1-x}\sqrt{1+x}} = 2f_3(x) .$$

$$\forall x \in ]-1, 1[ \quad f_1(x) - f_2(x) = \frac{1+x-1+x}{\sqrt{1-x}\sqrt{1+x}} = 2f_4(x) .$$

On a donc  $f_1 + f_2 = 2f_3$  et  $f_1 - f_2 = 2f_4$ .

Par conséquent,  $E$  est aussi le sous-espace vectoriel de  $\mathcal{F}(]-1, 1[, \mathbb{R})$  engendré par  $(f_1, f_2)$ .

Montrons qu'il s'agit d'une famille libre.

Soit  $\lambda_1$  et  $\lambda_2$  des réels tels que  $\lambda_1 f_1 + \lambda_2 f_2 = 0$ , c'est-à-dire :

$$\forall x \in ]-1, 1[ \quad \lambda_1 \sqrt{\frac{1+x}{1-x}} + \lambda_2 \sqrt{\frac{1-x}{1+x}} = 0 .$$

Pour  $x = 0$ , il vient  $\lambda_1 + \lambda_2 = 0$ .

Pour  $x = \frac{1}{2}$ , il vient  $\lambda_1 \sqrt{3} + \lambda_2 \frac{1}{\sqrt{3}} = 0$ .

On en déduit  $\lambda_1 = \lambda_2 = 0$ .

Comme  $(f_1, f_2)$  est une famille libre qui engendre  $E$ , c'est une base de  $E$ , qui est donc un  $\mathbb{R}$ -espace vectoriel de dimension 2.

## Application

Dans  $\mathbb{R}^3$ , on considère les vecteurs :

$$V_1(1, 4, -1) \quad ; \quad V_2(2, 3, 1) \quad ; \quad V_3(4, -1, 2) \quad ; \quad V_4(3, 5, -3) .$$

Montrez que  $(V_1, V_1, V_3)$  est une base de  $\mathbb{R}^3$ . Déterminez les coordonnées de  $V_4$  dans cette base.

## Solution

Pour grouper les deux questions, considérons un vecteur quelconque  $(a, b, c)$  de  $\mathbb{R}^3$  et montrons qu'il s'écrit, de façon unique, comme combinaison linéaire en  $V_1, V_2, V_3$ .

Pour répondre à la première question seule, il suffit de montrer que  $(V_1, V_2, V_3)$  est une famille libre, puisque cette famille comporte trois vecteurs dans un espace vectoriel de dimension 3.

Il s'agit de montrer l'existence et l'unicité des trois réels  $\alpha, \beta, \gamma$  tels que :

$$\begin{aligned} & \begin{cases} \alpha & +2\beta & +4\gamma & = & a \\ 4\alpha & +3\beta & -\gamma & = & b \\ -\alpha & +\beta & +2\gamma & = & c \end{cases} \\ \\ \Leftrightarrow & \begin{cases} \alpha & +2\beta & +4\gamma & = & a & L_1 \leftarrow L_1 \\ & 5\beta & +17\gamma & = & 4a - b & L_2 \leftarrow 4L_1 - L_2 \\ & 3\beta & +6\gamma & = & a + c & L_3 \leftarrow L_1 + L_3 \end{cases} \\ \\ \Leftrightarrow & \begin{cases} \alpha & +2\beta & +4\gamma & = & a & L_1 \leftarrow L_1 \\ & 5\beta & +17\gamma & = & 4a - b & L_2 \leftarrow L_2 \\ & & 21\gamma & = & 7a - 3b - 5c & L_3 \leftarrow 3L_2 - 5L_3 \end{cases} \\ \\ \Leftrightarrow & \begin{cases} 21\alpha & +42\beta & & = & -7a + 12b + 20c & L_1 \leftarrow 21L_1 - 4L_3 \\ & 105\beta & & = & -35a + 30b + 85c & L_2 \leftarrow 21L_2 - 17L_3 \\ & & 21\gamma & = & 7a - 3b - 5c & L_3 \leftarrow L_3 \end{cases} \\ \\ \Leftrightarrow & \begin{cases} \alpha & = & \frac{1}{21}(7a - 14c) \\ \beta & = & \frac{1}{21}(-7a + 6b + 17c) \\ \gamma & = & \frac{1}{21}(7a - 3b - 5c) \end{cases} \end{aligned}$$

On a donc démontré que  $(V_1, V_2, V_3)$  est une base de  $\mathbb{R}^3$ .

Avec  $a = 3$ ,  $b = 5$  et  $c = -3$ , on obtient  $\alpha = 3$ ,  $\beta = -2$  et  $\gamma = 1$ , soit :

$$V_4 = 3V_1 - 2V_2 + V_3.$$

## Application

Soit  $a, b, c$  trois réels. Déterminez une base de  $\mathbb{R}_2[X]$  dans laquelle les coordonnées de tout vecteur  $P$  sont  $(P(a), P'(b), P''(c))$ .

## Solution

Il s'agit de déterminer trois polynômes  $A, B, C$  de  $\mathbb{R}_2[X]$  tels que :

$$\forall P \in \mathbb{R}_2[X] \quad P = P(a)A + P'(b)B + P''(c)C.$$

Cette propriété devant être vérifiée pour tout  $P$ , écrivons-la pour les polynômes de la base canonique  $(1, X, X^2)$  de  $\mathbb{R}_2[X]$ .

Avec  $P = 1$ , on obtient  $A = 1$  ;

puis avec  $P = X$ , on obtient  $X = a + B$ , soit  $B = X - a$  ;

puis avec  $P = X^2$ , on obtient  $X^2 = a^2 + 2b(X - a) + 2C$ ,

soit  $C = \frac{1}{2}(X^2 - 2bX + 2ab - a^2)$ .

Comme  $d^\circ A = 0$ ,  $d^\circ B = 1$  et  $d^\circ C = 2$ ,  $(A, B, C)$  est bien une base de  $\mathbb{R}_2[X]$  car, comme les degrés sont tous distincts, c'est une famille libre ; et il y a autant de vecteurs que la dimension de  $\mathbb{R}_2[X]$ .

## I Généralités

### • Définitions

Une application  $f$  de  $E$  dans  $F$  est dite linéaire si c'est un morphisme d'espaces vectoriels, c'est-à-dire si :

$$\forall x \in E \quad \forall y \in E \quad \forall \lambda \in \mathbb{K} \quad f(x + y) = f(x) + f(y) ; f(\lambda x) = \lambda f(x)$$

ou encore :

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

La propriété précédente s'étend à toute combinaison linéaire :

$$f\left(\sum_{i=1}^n \lambda_i x_i\right) = \sum_{i=1}^n \lambda_i f(x_i).$$

Si  $f$  est bijective, c'est un isomorphisme ; si  $E = F$ , c'est un endomorphisme ; si  $f$  est bijective avec  $E = F$ , c'est un automorphisme.

On note :

$\mathcal{L}(E, F)$  l'ensemble des applications linéaires de  $E$  dans  $F$ ,

$\mathcal{L}(E)$  l'ensemble des applications linéaires de  $E$  dans  $E$ ,

$\text{GL}(E)$  l'ensemble des automorphismes de  $E$ .

### • Opérations algébriques

La composée de deux applications linéaires est linéaire.

Si  $f$  est un isomorphisme,  $f^{-1}$  est aussi un isomorphisme.

$\mathcal{L}(E, F)$  est un espace vectoriel.

Si  $\dim E = n$  et  $\dim F = p$ , on a  $\dim \mathcal{L}(E, F) = np$ .

$(\text{GL}(E), \circ)$  est un groupe, appelé groupe linéaire de  $E$ .

## II Noyau et image d'une application linéaire

### • Définitions

Soit  $f$  une application linéaire de  $E$  dans  $F$ .

- L'image par  $f$  d'un sous-espace vectoriel de  $E$  est un sous-espace vectoriel de  $F$ . En particulier,  $f(E)$  est un sous-espace vectoriel de  $F$  appelé image de  $f$ , et noté  $\text{Im } f$ . Il est engendré par les images des vecteurs d'une partie génératrice de  $E$ .
- L'image réciproque par  $f$  d'un sous-espace vectoriel de  $F$  est un sous-espace vectoriel de  $E$ .  
En particulier,  $f^{-1}(\{0\})$  est un sous-espace vectoriel de  $E$ . On l'appelle le noyau de  $f$ , et on le note  $\text{Ker } f$ .

- **Théorème**

$$f \text{ surjective} \iff \text{Im } f = F \quad ; \quad f \text{ injective} \iff \text{Ker } f = \{0\}.$$

- **Noyau d'une restriction**

Soit  $f$  une application linéaire de  $E$  dans  $F$  et  $E_1$  un sous-espace vectoriel de  $E$ . La restriction de  $f$  à  $E_1$  a pour noyau :

$$\text{Ker}(f|_{E_1}) = \text{Ker } f \cap E_1.$$

La restriction de  $f$  à tout supplémentaire  $G$  de  $\text{Ker } f$  définit donc un isomorphisme de  $G$  sur  $\text{Im } f$ .

- **Réflexe utile pour les applications**

$$f \circ g = 0 \iff \text{Im } g \subset \text{Ker } f.$$

### III Image d'une famille de vecteurs

Soit  $f$  une application linéaire de  $E$  dans  $F$ .

- **Image d'une famille génératrice**

Si  $G$  engendre  $E$ , alors  $f(G)$  engendre  $f(E)$ .

L'image d'une famille génératrice de  $E$  est une famille génératrice de  $F$  si, et seulement si,  $f$  est surjective.

- **Image d'une famille libre**

Si  $A$  est une partie liée dans  $E$ , alors  $f(A)$  est une partie liée dans  $F$ , ou, par contraposition :

$$f(A) \text{ libre dans } F \implies A \text{ libre dans } E.$$

$f$  est injective si, et seulement si, pour toute partie libre  $L$  de  $E$ ,  $f(L)$  est une partie libre de  $F$ .

- **Image d'une base**

L'image d'une base de  $E$  est une base de  $F$  si, et seulement si,  $f$  est bijective.

## IV Rang d'une application linéaire

- **Théorème du rang**

Si  $E$  est de dimension finie, on a :

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

La dimension  $\dim \operatorname{Im} f$  est appelée rang de  $f$ , et souvent notée  $\operatorname{rg} f$ .

- **Théorème**

Si  $E$  et  $F$  sont de même dimension finie, alors on a :

$$f \text{ bijective} \iff f \text{ injective} \iff f \text{ surjective}.$$

N'oubliez pas l'hypothèse sur  $E$  et  $F$ .

- **Forme linéaire et hyperplan**

### *Forme linéaire*

Soit  $E$  un  $\mathbb{K}$ -espace vectoriel. On appelle forme linéaire sur  $E$  toute application linéaire de  $E$  dans  $\mathbb{K}$ .

L'ensemble des formes linéaires sur  $E$  est le  $\mathbb{K}$ -espace vectoriel  $\mathcal{L}(E, \mathbb{K})$ . On l'appelle l'espace dual de  $E$  et on le note  $E^*$ .

Si  $E$  est de dimension finie, on a  $\dim E = \dim E^*$ .

### *Écriture d'une forme linéaire*

Si  $E$  est de dimension finie et admet  $(e_1, \dots, e_n)$  pour base, toute forme linéaire  $f$  sur  $E$  est de la forme :

$$x = \sum_{i=1}^n x_i e_i \in E \mapsto f(x) = \sum_{i=1}^n \alpha_i x_i \in \mathbb{K}$$

où les  $\alpha_i = f(e_i)$  sont des scalaires qui caractérisent  $f$ .

### *Forme linéaire et hyperplan*

– Étant donnée une forme linéaire  $\varphi$  sur  $E$  non nulle, le sous-espace vectoriel  $H = \operatorname{Ker} \varphi$  est un hyperplan de  $E$ .

Toute forme linéaire  $\psi$  nulle sur  $H$  est colinéaire à  $\varphi$ .

– En dimension finie, un hyperplan admet donc une équation de la forme :

$$\sum_{i=1}^n \alpha_i x_i = 0.$$

**Base duale**

Soit  $\mathcal{B} = (e_1, \dots, e_n)$  une base d'un espace vectoriel  $E$  de dimension finie.  
 Les formes linéaires coordonnées  $(\varphi_1, \dots, \varphi_n)$  définies par :

$$\forall i \in \{1, \dots, n\} \quad \forall j \in \{1, \dots, n\} \quad \varphi_i(e_j) = \delta_i^j$$

constituent une base  $\mathcal{B}^*$  de  $E^*$  appelée base duale de  $\mathcal{B}$ .

Le symbole de Kronecker  $\delta_i^j$  vaut 1 si  $i = j$  et 0 si  $i \neq j$ .

## V Détermination d'une application linéaire

Soit  $A = (a_1, \dots, a_n)$  une base de  $E$  et  $B = (b_1, \dots, b_n)$  une famille de  $n$  vecteurs de  $F$ .

Il existe une application linéaire unique  $f$  de  $E$  dans  $F$  telle que :

$$\forall i \in \{1, \dots, n\} \quad f(a_i) = b_i.$$

On a :  $f$  injective  $\iff B$  libre dans  $F$  ;

$f$  surjective  $\iff B$  engendre  $F$  ;

$f$  bijective  $\iff B$  est une base de  $F$ .

Conséquence : deux espaces vectoriels  $E$  et  $F$  de dimensions finies sont isomorphes si, et seulement si,  $\dim E = \dim F$ .

## Application

Soit  $\mathbb{R}^4$  considéré comme espace vectoriel sur  $\mathbb{R}$  et muni de sa base canonique  $\mathcal{B} = (e_1, e_2, e_3, e_4)$ .

Soit  $f$  l'endomorphisme de  $\mathbb{R}^4$  défini par :

$$\begin{cases} f(e_1) &= e_1 & -e_3 & +e_4 \\ f(e_2) &= -e_1 & +e_2 & +e_3 \\ f(e_3) &= -e_1 & +3e_2 & +e_3 & +2e_4 \\ f(e_4) &= -3e_1 & +e_2 & +3e_3 & -2e_4 \end{cases}$$

Déterminez le rang de la famille  $(f(e_1), f(e_2), f(e_3), f(e_4))$ .

Déduisez-en la dimension de  $\text{Im } f$  et une base de  $\text{Im } f$ .

Déterminez une base de  $\text{Ker } f$ .

$\text{Im } f$  et  $\text{Ker } f$  sont-ils supplémentaires ?

## Solution

Une transformation élémentaire sur les vecteurs ne modifie pas l'espace vectoriel engendré.

Le rang de la famille  $(f(e_1), f(e_2), f(e_3), f(e_4))$  est donc le même que celui de la famille des 4 vecteurs :

$$\begin{cases} f(e_1) &= e_1 & -e_3 & +e_4 \\ f(e_2) + f(e_1) &= e_2 & & +e_4 \\ f(e_3) + f(e_1) &= 3e_2 & & +3e_4 \\ f(e_4) + 3f(e_1) &= e_2 & & +e_4 \end{cases}$$

On constate que :

$$f(e_1) + f(e_2) = 3f(e_1) + f(e_4) = \frac{1}{3}(f(e_1) + f(e_3)).$$

Par conséquent,  $\text{Im } f$  qui est engendré par  $(f(e_1), f(e_2), f(e_3), f(e_4))$ , est aussi engendré par  $(f(e_1), f(e_2))$ .

Ces deux vecteurs sont linéairement indépendants puisqu'ils ne sont pas colinéaires. Ils constituent donc une base de  $\text{Im } f$  et on a  $\dim \text{Im } f = 2$ .

Le théorème du rang donne alors :

$$\dim \text{Ker } f = \dim \mathbb{R}^4 - \dim \text{Im } f = 4 - 2 = 2.$$

Des combinaisons linéaires existant entre les  $f(e_i)$ , on déduit :

$$f(2e_1 - e_2 + e_4) = 0 = f(2e_1 + 3e_2 - e_3).$$

Les deux vecteurs  $2e_1 - e_2 + e_4$  et  $2e_1 + 3e_2 - e_3$  étant linéairement indépendants constituent une base de  $\text{Ker } f$ .

Pour que  $\text{Im } f$  et  $\text{Ker } f$  soient supplémentaires, il suffit que la famille de vecteurs obtenue en juxtaposant une base de  $\text{Im } f$  et une base de  $\text{Ker } f$  soit libre, c'est-à-dire de rang 4.

Pour déterminer ce rang, nous allons écrire des familles de vecteurs successives, toutes de même rang jusqu'à obtenir un système triangulaire dont le rang est évident.

Pour ceci, il est courant d'utiliser une écriture en colonnes.

$$\begin{array}{cccc|cccc}
 C_1 & C_2 & C_3 & C_4 & C_1 & C'_2 & C'_3 & C'_4 \\
 1 & -1 & 2 & 2 & 1 & 0 & 0 & 0 \\
 0 & 1 & -1 & 3 & 0 & 1 & -1 & 3 \\
 -1 & 1 & 0 & -1 & -1 & 0 & 2 & 1 \\
 1 & 0 & 1 & 0 & 1 & 1 & -1 & -2
 \end{array}$$

où l'on a posé :  $C'_2 = C_2 + C_1$ ,  $C'_3 = C_3 - 2C_1$ ,  $C'_4 = C_4 - 2C_1$ .

$$\begin{array}{cccc|cccc}
 C_1 & C'_2 & C''_3 & C''_4 & C_1 & C'_2 & C''_3 & C''_4 \\
 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
 -1 & 0 & 2 & 1 & -1 & 0 & 2 & 0 \\
 1 & 1 & 0 & -5 & 1 & 1 & 0 & -10
 \end{array}$$

où l'on a posé :

$$C''_3 = C'_3 + C'_2, \quad C''_4 = C'_4 - 3C'_2, \quad \text{puis } C'''_4 = 2C''_4 - C''_3.$$

On a  $\text{rg}(C_1, C_2, C_3, C_4) = \text{rg}(C_1, C'_2, C''_3, C''_4) = 4$ .

Ainsi la famille obtenue par réunion d'une base de  $\text{Im } f$  et d'une base de  $\text{Ker } f$  est une base de  $\mathbb{R}^4$ , ce qui démontre que  $\text{Im } f$  et  $\text{Ker } f$  sont supplémentaires.

## Application

Soit  $E$  un espace vectoriel de dimension  $n$  et  $f \in \mathcal{L}(E)$ .

Montrez que les trois propositions suivantes sont équivalentes :

$$(a) \text{ Im } f = \text{Im } f^2 ; \quad (b) \text{ Ker } f = \text{Ker } f^2 ; \quad (c) E = \text{Im } f \oplus \text{Ker } f.$$

## Solution

On a toujours :

$\text{Ker } f \subset \text{Ker } f^2$  car  $x \in \text{Ker } f \iff f(x) = 0 \implies f^2(x) = f(0) = 0$ ,

$\text{Im } f^2 \subset \text{Im } f$  car si  $x \in \text{Im } f^2$ , il existe  $y \in E$  tel que  $x = f^2(y) = f(f(y))$ .

**(a)  $\implies$  (b)**

D'après le théorème du rang appliqué à  $f$  et à  $f^2$ , on a :

$$n = \dim \text{Ker } f + \dim \text{Im } f = \dim \text{Ker } f^2 + \dim \text{Im } f^2.$$

L'hypothèse entraîne :  $\dim \text{Im } f = \dim \text{Im } f^2$ , et par conséquent :

$$\dim \text{Ker } f = \dim \text{Ker } f^2.$$

Comme on a toujours  $\text{Ker } f \subset \text{Ker } f^2$ , on en déduit  $\text{Ker } f = \text{Ker } f^2$ .

**(b)  $\implies$  (c)**

Sachant que  $\dim \text{Ker } f + \dim \text{Im } f = n$ , il reste à démontrer que

$\text{Ker } f \cap \text{Im } f = \{0\}$ . En effet, on aura alors :

$$\dim (\text{Ker } f + \text{Im } f) = \dim \text{Ker } f + \dim \text{Im } f - \dim (\text{Ker } f \cap \text{Im } f) = n,$$

ce qui entraînera  $\text{Ker } f + \text{Im } f = E$ .

Soit  $x \in \text{Ker } f \cap \text{Im } f$ . On a  $f(x) = 0$ , et il existe  $y \in E$  tel que  $x = f(y)$ .

Par conséquent  $f^2(y) = 0$ , soit  $y \in \text{Ker } f^2$ .

D'après l'hypothèse, on a donc  $y \in \text{Ker } f$ , soit  $f(y) = 0$ , puis  $x = 0$ .

**(c)  $\implies$  (a)**

Comme  $\text{Im } f^2 \subset \text{Im } f$ , il reste à démontrer que  $\text{Im } f \subset \text{Im } f^2$ .

Soit  $x = f(y)$  un élément de  $\text{Im } f$ . Utilisons l'hypothèse pour décomposer  $y$  sous la forme :

$$y = a + f(b),$$

avec  $a \in \text{Ker } f$ . Alors  $x = f(y) = f(a) + f^2(b) = f^2(b)$ , ce qui montre que  $x \in \text{Im } f^2$ . Donc  $\text{Im } f^2 = \text{Im } f$ .

## Application

On considère deux endomorphismes  $f$  et  $g$  d'un espace vectoriel  $E$  de dimension finie  $n$  tels que :

$$f + g \text{ bijectif} \quad \text{et} \quad f \circ g = 0.$$

Démontrez que  $\text{rg } f + \text{rg } g = n$ .

## Solution

- Si  $f + g$  est bijectif, on a  $\text{Im}(f + g) = E$ .

On a toujours  $\text{Im}(f + g) \subset \text{Im } f + \text{Im } g$  puisqu'un élément de  $\text{Im}(f + g)$  est de la forme  $f(x) + g(x)$  avec  $x \in E$ . On sait aussi que :

$$\dim(\text{Im } f + \text{Im } g) = \dim \text{Im } f + \dim \text{Im } g - \dim(\text{Im } f \cap \text{Im } g).$$

On en déduit :

$$n \leq \dim(\text{Im } f + \text{Im } g) \leq \text{rg } f + \text{rg } g.$$

- L'hypothèse  $f \circ g = 0$  est équivalente à  $\text{Im } g \subset \text{Ker } f$ .

On en déduit  $\text{rg } g \leq \dim \text{Ker } f = n - \text{rg } f$ , soit  $\text{rg } f + \text{rg } g \leq n$ .

- Avec les deux inégalités obtenues, on conclut :

$$\text{rg } f + \text{rg } g = n.$$

## Application

$E$  est un  $\mathbb{K}$ -espace vectoriel de dimension  $n$  ;  $f$  et  $g$  sont des endomorphismes de  $E$ . Montrez que :

$$\text{rg } f + \text{rg } g - n \leq \text{rg}(g \circ f) \leq \min(\text{rg } f, \text{rg } g).$$

## Solution

- Montrons que  $\text{rg}(g \circ f) \leq \min(\text{rg } f, \text{rg } g)$ .

Comme  $\text{Im}(g \circ f) \subset \text{Im } g$ , on a  $\text{rg}(g \circ f) \leq \text{rg } g$ .

Soit  $(u_i)_{i \in \{1, \dots, p\}}$  une base de  $\text{Im } f$ . La famille  $(g(u_i))_{i \in \{1, \dots, p\}}$  est alors génératrice de  $g(\text{Im } f) = \text{Im}(g \circ f)$ , ce qui entraîne  $\text{rg}(g \circ f) \leq p = \text{rg } f$ .

On a donc bien  $\text{rg}(g \circ f) \leq \min(\text{rg } f, \text{rg } g)$ .

- Montrons que  $\text{rg } f + \text{rg } g - n \leq \text{rg}(g \circ f)$ , ou, ce qui est équivalent :

$$\text{rg } f - \dim \text{Ker } g \leq \text{rg}(g \circ f).$$

Soit  $h$  la restriction de  $g$  à  $\text{Im } f$ .

$h$  étant une application linéaire de  $\text{Im } f$  dans  $E$ , on a :

$$\dim \text{Im } h = \dim \text{Ker } h + \dim \text{Im } h$$

On a  $\text{Im } h = \text{Im}(g \circ f)$ ,

et  $\text{Ker } h = \{x \in \text{Im } f ; h(x) = g(x) = 0\} = \text{Im } f \cap \text{Ker } g \subset \text{Ker } g$ .

D'où  $\dim \text{Im } f = \dim \text{Im}(g \circ f) + \dim(\text{Im } f \cap \text{Ker } g)$ .

On en déduit  $\text{rg } f \leq \text{rg}(g \circ f) + \dim \text{Ker } g$ , ce qui est équivalent à l'inégalité demandée.

## I Homothéties

Soit  $k \in \mathbb{K}^*$ . L'homothétie de rapport  $k$  est l'automorphisme linéaire de  $E$  :

$$\begin{array}{ccc} h_k : E & \longrightarrow & E \\ x & \longmapsto & kx. \end{array}$$

Dans cette définition, n'oubliez pas que  $k$  ne dépend pas de  $x$ .

II Projecteurs  
et symétries vectorielles

## • Définitions

Soit  $F$  et  $G$  deux sous-espaces vectoriels supplémentaires de  $E$ . Tout vecteur  $x$  de  $E$  s'écrit de façon unique sous la forme  $x = x_1 + x_2$  avec  $x_1 \in F$  et  $x_2 \in G$ .

L'application  $p$  de  $E$  dans  $E : x \mapsto p(x) = x_1$  est linéaire.

C'est le projecteur sur  $F$ , parallèlement à  $G$ .

L'application  $s_F$  de  $E$  dans  $E : x \mapsto s_F(x) = x_1 - x_2$  est linéaire.

C'est la symétrie par rapport à  $F$ , parallèlement à  $G$ .

On définit de même le projecteur  $q$  sur  $G$ , parallèlement à  $F$ , et la symétrie  $s_G$  par rapport à  $G$ , parallèlement à  $F$ .

## • Propriétés

$$p + q = \text{Id}_E \quad ; \quad p \circ q = q \circ p = 0 \quad ; \quad p^2 = p \quad ; \quad q^2 = q \quad ; \quad s_F^2 = \text{Id}_E.$$

$$\text{Ker } p = \text{Im } q = G \quad ; \quad \text{Ker } q = \text{Im } p = F.$$

$p$  et  $s_F$  sont liées par l'égalité :

$$s_F = 2p - \text{Id}_E.$$

- **Projecteurs**

D'une façon générale, on appelle projecteur de  $E$  tout endomorphisme  $p$  de  $E$  tel que  $p \circ p = p$ .

On a alors :

$$E = \text{Ker } p \oplus \text{Im } p,$$

et  $p$  est le projecteur sur  $\text{Im } p$ , parallèlement à  $\text{Ker } p$ .

Attention, l'égalité  $E = \text{Ker } f \oplus \text{Im } f$  entraîne seulement que  $\text{Im } f = \text{Im } f^2$ , et pas que  $f$  soit un projecteur.

- **Symétries vectorielles**

D'une façon générale, on appelle symétrie de  $E$  toute application linéaire  $s$ , de  $E$  dans  $E$ , telle que  $s \circ s = \text{Id}_E$ .

Alors  $F = \{x \in E ; s(x) = x\}$  et  $G = \{x \in E ; s(x) = -x\}$  sont des sous-espaces supplémentaires de  $E$ , et  $s$  est la symétrie par rapport à  $F$ , parallèlement à  $G$ .

## Application

On considère un  $\mathbb{K}$ -espace vectoriel  $E$  de dimension  $n$ , deux projecteurs  $p$  et  $q$  de  $E$  vérifiant  $p \circ q = q \circ p$ .

Montrez que  $p \circ q$  est un projecteur.

Déterminez  $\text{Im}(p \circ q)$  et  $\text{Ker}(p \circ q)$ .

## Solution

- Des règles de calcul dans  $\mathcal{L}(E)$ , il vient :

$$(p \circ q) \circ (p \circ q) = p \circ (q \circ p) \circ q = p \circ (p \circ q) \circ q = p^2 \circ q^2 = p \circ q.$$

$p \circ q$  est donc un projecteur de  $E$ .

Rappelons que, si  $u$  est un projecteur de  $E$ , les vecteurs  $x$  de  $\text{Im } u$  sont caractérisés par la condition  $u(x) = x$ .

- Soit  $x \in \text{Im}(p \circ q)$ . On a alors  $(p \circ q)(x) = x$ , d'où  $x \in \text{Im } p$ .

Comme  $p \circ q = q \circ p$ , on a aussi  $(q \circ p)(x) = x$ , d'où  $x \in \text{Im } q$ .

On en déduit que  $\text{Im}(p \circ q) \subset \text{Im } p \cap \text{Im } q$ .

Soit  $x \in \text{Im } p \cap \text{Im } q$  ; on a alors  $p(x) = q(x) = x$ ,

d'où  $(p \circ q)(x) = p(x) = x$ , et donc  $x \in \text{Im}(p \circ q)$ .

On conclut que  $\text{Im}(p \circ q) = \text{Im } p \cap \text{Im } q$ .

- Soit  $x \in \text{Ker } p$  ; on a alors  $p(x) = 0$ , ce qui entraîne  $(q \circ p)(x) = 0$ , puis  $(p \circ q)(x) = 0$  puisque  $p \circ q = q \circ p$ .

On en déduit  $\text{Ker } p \subset \text{Ker}(p \circ q)$ .

On montre de même que  $\text{Ker } q \subset \text{Ker}(p \circ q)$ .

$\text{Ker}(p \circ q)$  contient donc le sous-espace vectoriel engendré par  $\text{Ker } p \cup \text{Ker } q$ , soit  $\text{Ker } p + \text{Ker } q$ .

Réciproquement, soit  $x \in \text{Ker}(p \circ q)$ . Comme on a  $E = \text{Ker } p \oplus \text{Im } p$  puisque  $p$  est un projecteur, il existe des vecteurs uniques  $x_1 \in \text{Ker } p$  et  $x_2 \in \text{Im } p$  tels que  $x = x_1 + x_2$ . De

$$0 = (p \circ q)(x) = (q \circ p)(x) = (q \circ p)(x_1) + (q \circ p)(x_2),$$

on tire  $(q \circ p)(x_2) = 0$ .

Comme  $x_2 \in \text{Im } p$ , on a  $p(x_2) = x_2$ , d'où  $q(x_2) = 0$  soit  $x_2 \in \text{Ker } q$ , et par conséquent  $x \in \text{Ker } p + \text{Ker } q$ .

On conclut donc que  $\text{Ker}(p \circ q) = \text{Ker } p + \text{Ker } q$ .

## Application

Dans  $E = \mathbb{R}^3$ , on considère les deux sous-espaces vectoriels :

$$E_1 = \{(x, y, z) \in E ; x + y + z = 0\} \quad ; \quad E_2 = \{(x, y, z) \in E ; x = -y = z\}.$$

1. Démontrez que  $E = E_1 \oplus E_2$ .

2. Soit  $p$  la projection sur  $E_1$  parallèlement à  $E_2$  et  $s$  la symétrie par rapport à  $E_1$  parallèlement à  $E_2$ . Déterminez  $p[(x, y, z)]$  et  $s[(x, y, z)]$ .

## Solution

Si l'exercice s'arrêtait à la première question, démontrez que  $E_1 \cap E_2 = \{0\}$ , puis  $\dim E_1 = 2$  et  $\dim E_2 = 1$ .

1. Démontrons que tout vecteur  $(x, y, z)$  de  $E$  se décompose de façon unique comme somme d'un vecteur de  $E_1$  et d'un vecteur de  $E_2$ .

• Commençons par l'unicité. Soit  $(x, y, z) \in E$  et supposons qu'il s'écrive :

$$(x, y, z) = (x_1, y_1, z_1) + (x_2, y_2, z_2)$$

avec  $(x_1, y_1, z_1) \in E_1$  et  $(x_2, y_2, z_2) \in E_2$ . On a alors :

$$\begin{cases} x = x_1 + x_2 \\ y = y_1 + y_2 \\ z = z_1 + z_2 \end{cases} \quad \text{et} \quad \begin{cases} x_1 + y_1 + z_1 = 0 \\ x_2 = -y_2 = z_2. \end{cases}$$

En additionnant membre à membre les égalités du premier système et en utilisant les autres égalités, on obtient :

$$x + y + z = x_2 + y_2 + z_2 = x_2,$$

ce qui donne :

$$x_2 = x + y + z ; \quad y_2 = -x - y - z ; \quad z_2 = x + y + z,$$

puis :

$$x_1 = x - x_2 = -y - z ; \quad y_1 = y - y_2 = x + 2y + z ; \quad z_1 = z - z_2 = -x - y.$$

• Pour démontrer l'existence de la décomposition de tout vecteur, considérons un vecteur quelconque  $(x, y, z)$  de  $E$ .

Définissons  $(x_1, y_1, z_1)$  et  $(x_2, y_2, z_2)$  par les valeurs qui précèdent.

On observe que  $(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x, y, z)$ ,

que  $(x_1, y_1, z_1) \in E_1$  et  $(x_2, y_2, z_2) \in E_2$ ,

ce qui démontre l'existence de la décomposition.

2. Il résulte de la décomposition précédente que :

$$p[(x, y, z)] = (x_1, y_1, z_1) = (-y - z, x + 2y + z, -x - y).$$

$$s[(x, y, z)] = (-x - 2y - 2z, 2x + 3y + 2z, -2x - 2y - z).$$

## I Définitions

### • Matrices

Une matrice à  $n$  lignes et  $p$  colonnes sur un corps  $\mathbb{K}$  est un tableau d'éléments de  $\mathbb{K}$  comportant  $n$  lignes et  $p$  colonnes.

On note  $a_{ij}$  l'élément d'une matrice  $A$  situé sur la ligne  $i$  et la colonne  $j$ . La matrice  $A$  s'écrit :

$$\begin{pmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{np} \end{pmatrix} \quad \text{ou} \quad (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \quad \text{ou} \quad (a_{ij}).$$

On dit que  $A$  est de format  $(n, p)$ , ou de type  $(n, p)$ , ou de taille  $(n, p)$ .

L'ensemble des matrices à  $n$  lignes et  $p$  colonnes, à coefficients dans  $\mathbb{K}$ , est noté  $\mathcal{M}_{n,p}(\mathbb{K})$ .

Si  $p = 1$ ,  $A$  est une matrice colonne que l'on peut assimiler à un vecteur de  $\mathbb{K}^n$ .

Si  $n = 1$ ,  $A$  est une matrice ligne que l'on peut assimiler à une forme linéaire appartenant à  $(\mathbb{K}^p)^*$ .

Si  $n = p$ ,  $A$  est une matrice carrée d'ordre  $n$ .  $\mathcal{M}_{n,n}(\mathbb{K})$  se note  $\mathcal{M}_n(\mathbb{K})$ . Les éléments  $a_{11}, \dots, a_{nn}$  forment la diagonale principale de  $A$ .

Deux matrices  $A$  et  $B$  sont égales si elles sont de même format, et si  $a_{ij} = b_{ij}$  pour tout  $i \in \{1, \dots, n\}$  et pour tout  $j \in \{1, \dots, p\}$ .

### • Matrices particulières

Soit  $A = (a_{ij})$  une matrice carrée d'ordre  $n$ .

–  $A$  est triangulaire supérieure si  $a_{ij} = 0$  pour  $i > j$ .

–  $A$  est triangulaire inférieure si  $a_{ij} = 0$  pour  $i < j$ .

–  $A$  est diagonale si  $a_{ij} = 0$  pour  $i \neq j$ .

On peut alors la noter :  $A = \text{diag}(a_{11}, \dots, a_{nn})$ .

–  $A$  est scalaire si  $A = a I_n$ .

## II Opérations sur les matrices

- **Espace vectoriel  $\mathcal{M}_{n,p}(\mathbb{K})$**

Soit  $\lambda \in \mathbb{K}$ , et  $A = (a_{ij})$  et  $B = (b_{ij})$  deux matrices de  $\mathcal{M}_{n,p}(\mathbb{K})$ .

On définit :

$$\lambda A = (\lambda a_{ij}) \quad \text{et} \quad A + B = (a_{ij} + b_{ij}).$$

Attention, on ne peut additionner deux matrices que si elles sont de même format.

Pour ces deux lois,  $\mathcal{M}_{n,p}(\mathbb{K})$  est un espace vectoriel.

Pour  $i \in \{1, \dots, n\}$  et  $j \in \{1, \dots, p\}$  fixés, on note  $E_{ij}$  la matrice dont le coefficient situé sur la ligne  $i$  et la colonne  $j$  est égal à 1, et dont les autres coefficients sont égaux à 0.  $(E_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}}$  est la base canonique de  $\mathcal{M}_{n,p}(\mathbb{K})$ , qui est donc de dimension  $n p$ .

- **Produit de matrices**

Si  $A$  est de format  $(n, p)$  et  $B$  de format  $(p, q)$ , on définit la matrice  $C = AB$ , de format  $(n, q)$ , par :

$$\forall i \in \{1, \dots, n\} \quad \forall j \in \{1, \dots, q\} \quad c_{ij} = \sum_{k=1}^p a_{ik} b_{kj}.$$

Attention à la condition d'existence de  $AB$  :

nombre de colonnes de  $A$  = nombre de lignes de  $B$ .

Ce produit est associatif et non commutatif.

## III Matrices carrées d'ordre $n$

- **Formule du binôme de Newton**

Si  $AB = BA$ , alors :

$$\forall m \in \mathbb{N} \quad (A + B)^m = \sum_{k=0}^m \binom{m}{k} A^k B^{m-k}.$$

- **Matrices inversibles**

Une matrice  $A \in \mathcal{M}_n(\mathbb{K})$  est inversible s'il existe  $B \in \mathcal{M}_n(\mathbb{K})$  telle que :

$$AB = BA = I_n.$$

Si  $B$  existe, elle est unique et on la note  $A^{-1}$ .

Les éléments inversibles de  $\mathcal{M}_n(\mathbb{K})$  forment un groupe  $\text{GL}_n(\mathbb{K})$ , isomorphe au groupe linéaire  $\text{GL}(\mathbb{K}^n)$ . On a en particulier :

$$(A B)^{-1} = B^{-1} A^{-1}.$$

Si  $A$  est inversible, alors l'endomorphisme  $f$  de  $E$ , muni d'une base  $\mathcal{B}$ , qui lui est associé (pour le lien entre matrices et applications linéaires, voir la fiche 19) est inversible ; et  $A^{-1}$  est la matrice de  $f^{-1}$ .

Dans  $\mathcal{M}_n(\mathbb{K})$ , pour que  $A$  soit inversible, il suffit qu'elle soit inversible à droite, ou à gauche.

## IV Transposition

- **Définition**

La transposée d'une matrice  $A$  de format  $(n, p)$ , est la matrice de format  $(p, n)$ , notée  ${}^t A$ , de terme général  $b_{ij}$  :

$$\forall i \in \{1, \dots, p\} \quad \forall j \in \{1, \dots, n\} \quad b_{ij} = a_{ji}.$$

Elle est donc obtenue à partir de  $A$  en échangeant les lignes et les colonnes.

- **Propriétés**

$${}^t({}^t A) = A \quad ; \quad {}^t(\lambda A) = \lambda {}^t A \quad ; \quad {}^t(A + B) = {}^t A + {}^t B \quad ;$$

$${}^t(A B) = {}^t B {}^t A \quad ; \quad {}^t(A^{-1}) = ({}^t A)^{-1}.$$

- **Matrices symétriques, antisymétriques**

Une matrice carrée  $A$  est symétrique si  ${}^t A = A$ ,

$$\text{antisymétrique si } {}^t A = -A.$$

Les matrices symétriques et les matrices antisymétriques constituent des sous-espaces vectoriels supplémentaires de  $\mathcal{M}_n(\mathbb{K})$ .

## Application

Soit  $A = (a_{ij})$  la matrice carrée d'ordre  $n$  définie par son terme général :

$$\begin{cases} a_{ij} = 0 & \text{si } i > j \\ a_{ij} = (-1)^{i-1} \binom{j-1}{i-1} & \text{si } i \leq j. \end{cases}$$

Calculez  $A^2$ .

## Solution

Soit  $b_{ij}$  le terme général de  $A^2$ . On a  $b_{ij} = \sum_{k=1}^n a_{ik} a_{kj}$ .

$a_{ik} a_{kj}$  est non nul si, et seulement si,  $i \leq k \leq j$ .

On peut donc déjà dire que  $b_{ij} = 0$  quand  $i > j$ .

Quand  $i \leq j$ , la somme précédente comporte des termes non nuls.

$$\begin{aligned} b_{ij} &= \sum_{k=i}^j (-1)^{i-1} \binom{k-1}{i-1} (-1)^{k-1} \binom{j-1}{k-1} \\ &= (-1)^i \sum_{k=i}^j \frac{(k-1)!}{(i-1)!(k-i)!} (-1)^k \frac{(j-1)!}{(k-1)!(j-k)!} \\ &= (-1)^i \frac{(j-1)!}{(i-1)!} \sum_{k=i}^j (-1)^k \frac{1}{(k-i)!(j-k)!} \\ &= (-1)^i \binom{j-1}{i-1} \sum_{k=i}^j (-1)^k \binom{j-i}{k-i} \\ &= \binom{j-1}{i-1} \sum_{k'=0}^{j-i} (-1)^{k'} \binom{j-i}{k'} = \binom{j-1}{i-1} (1-1)^{j-i} \end{aligned}$$

Si  $i < j$ , on obtient donc  $b_{ij} = 0$ . Mais si  $i = j$ , on obtient  $b_{ii} = 1$ .

Par conséquent  $A^2 = I_n$ .

Soit  $E = \mathbb{R}_{n-1}[X]$  muni de sa base canonique  $(1, X, \dots, X^{n-1})$ .

La matrice  $A$  est celle de l'endomorphisme :

$$P(X) \mapsto P(1-X).$$

Il n'est donc pas miraculeux d'avoir obtenu  $A^2 = I_n$ .

## Application

$a$  et  $b$  étant deux réels donnés, on considère la matrice :

$$A = \begin{pmatrix} a & b & b \\ b & a & b \\ b & b & a \end{pmatrix}.$$

Calculez  $A^n$  pour  $n \in \mathbb{N}^*$ .

## Solution

Il est normal de penser à utiliser la formule du binôme pour calculer  $A^n$ . Mais toutes les décompositions ne permettent pas de conclure. En voici une qui est efficace :

$$A = (a - b) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + b \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = (a - b) I_3 + b B.$$

On constate que  $B^2 = 3B$ , et on démontre par récurrence que, pour tout  $k \in \mathbb{N}^*$ , on a  $B^k = 3^{k-1} B$ .

Comme  $I_3 B = B I_3$ , on peut appliquer la formule du binôme, et on obtient, pour tout  $n \in \mathbb{N}^*$  :

$$\begin{aligned} A^n &= (a - b)^n I_3 + \left( \sum_{k=1}^n \binom{n}{k} (a - b)^{n-k} b^k 3^{k-1} \right) B \\ &= (a - b)^n I_3 + \frac{1}{3} \left( \sum_{k=1}^n \binom{n}{k} (3b)^k (a - b)^{n-k} \right) B \\ &= (a - b)^n I_3 + \frac{1}{3} \left[ (a + 2b)^n - (a - b)^n \right] B. \end{aligned}$$

## Application

Calculez l'inverse de la matrice :

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

## Solution

Il s'agit de trouver la matrice  $A' = \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix}$  vérifiant  $A A' = I_3$ .

Les coefficients de  $A'$  vérifient donc :

$$\begin{cases} x_1 + 2y_1 + 2z_1 = 1 \\ x_1 + 2y_1 + z_1 = 0 \\ x_1 + y_1 + z_1 = 0 \end{cases} \quad \begin{cases} x_2 + 2y_2 + 2z_2 = 0 \\ x_2 + 2y_2 + z_2 = 1 \\ x_2 + y_2 + z_2 = 0 \end{cases} \quad \begin{cases} x_3 + 2y_3 + 2z_3 = 0 \\ x_3 + 2y_3 + z_3 = 0 \\ x_3 + y_3 + z_3 = 1 \end{cases}$$

Les trois systèmes ne diffèrent que par leurs seconds membres. On peut les résoudre en même temps en juxtaposant les seconds membres. On part de la matrice augmentée :

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

Avec les opérations  $L_2 \leftarrow L_2 - L_1$  et  $L_3 \leftarrow L_3 - L_1$ ,  
puis  $L_2 \leftrightarrow L_3$ ,  $L_2 \leftarrow -L_2$ ,  $L_3 \leftarrow -L_3$  et  $L_1 \leftarrow L_1 - 2L_2$ ,  
on obtient successivement :

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

Avec  $L_2 \leftarrow L_2 - L_3$ , on obtient enfin  $I_3$  dans la partie gauche du tableau :

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

On a donc :  $A^{-1} = \begin{pmatrix} -1 & 0 & 2 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix}$ .

## I Écritures matricielles

### • Matrice d'une application linéaire de $E$ dans $F$

Soit  $E$  et  $F$  des espaces vectoriels de dimensions  $p$  et  $n$ , munis de bases respectives  $\mathcal{B} = (e_1, \dots, e_p)$  et  $\mathcal{C} = (f_1, \dots, f_n)$ .

Soit  $f$  une application linéaire de  $E$  dans  $F$ . Elle est déterminée par la donnée des vecteurs :

$$f(e_j) = \sum_{i=1}^n a_{ij} f_i \quad \text{pour } 1 \leq j \leq p,$$

c'est-à-dire par la matrice  $A = (a_{ij})$  dont les vecteurs colonnes sont les composantes de  $f(e_j)$  dans la base de  $F$  qui a été choisie.

On dit que  $A$  est la matrice de  $f$  dans les bases  $\mathcal{B}$  et  $\mathcal{C}$ .

$A$  dépend donc à la fois de l'application linéaire qu'elle représente et des bases choisies dans les espaces vectoriels de départ et d'arrivée.

Si  $E$  est de dimension  $n$ , dans toute base l'identité de  $E$  est représentée par la matrice carrée  $I_n$  qui comporte des 1 sur sa diagonale principale et des 0 ailleurs.

### • Traduction matricielle de l'égalité vectorielle $y = f(x)$

Soit  $E$  et  $F$  deux espaces vectoriels de dimensions finies munis de bases respectives  $\mathcal{B}$  et  $\mathcal{C}$ , et  $f$  une application linéaire de  $E$  dans  $F$ .

Soit  $x \in E$  et  $y \in F$ . Notons  $X$  la matrice colonne des composantes de  $x$  dans  $\mathcal{B}$ ,  $Y$  la matrice colonne des composantes de  $y$  dans  $\mathcal{C}$ ,  $M$  la matrice de  $f$  dans les bases  $\mathcal{B}$  et  $\mathcal{C}$ .

L'égalité vectorielle  $y = f(x)$  est équivalente à l'égalité matricielle :

$$Y = MX.$$

## II Changement de bases

### • Matrice de passage

Soit  $\mathcal{B} = (e_1, \dots, e_p)$  et  $\mathcal{B}' = (e'_1, \dots, e'_p)$  deux bases d'un espace vectoriel  $E$  de dimension  $p$ . On appelle matrice de passage de la base  $\mathcal{B}$  à la base  $\mathcal{B}'$ , la matrice  $P$  dont les colonnes  $C_j$  sont les composantes des vecteurs  $e'_j$  dans la base  $\mathcal{B}$ .

$P$  est la matrice de l'identité de  $E$  muni de  $\mathcal{B}'$ , dans  $E$  muni de  $\mathcal{B}$ .

Si  $P'$  est la matrice de passage de  $\mathcal{B}'$  à  $\mathcal{B}$ , on a  $P P' = P' P = I_p$ .

Toute matrice de passage est donc inversible.

Réciproquement, toute matrice inversible peut être considérée comme une matrice de passage.

### • Effet d'un changement de bases

#### *Sur les coordonnées d'un vecteur*

Si  $X$  est la matrice colonne des composantes de  $x$  dans  $\mathcal{B}$ ,  $X'$  la matrice colonne des composantes de  $x$  dans  $\mathcal{B}'$  et  $P$  la matrice de passage de  $\mathcal{B}$  à  $\mathcal{B}'$ , on a :

$$X = P X' \quad \text{ou encore} \quad X' = P^{-1} X.$$

#### *Sur l'expression d'une forme linéaire*

Si une forme linéaire sur  $E$  est représentée par une matrice ligne

$U = (\alpha_1, \dots, \alpha_n)$  dans une base  $\mathcal{B}$ , par  $U'$  dans une base  $\mathcal{B}'$  et si  $P$  est la matrice de passage de  $\mathcal{B}$  à  $\mathcal{B}'$ , on a  $f(x) = U X = U' X'$ , soit :

$$U' = U P.$$

### • Matrices équivalentes, matrices semblables

Soit  $f$  une application linéaire de  $E$  dans  $F$ ,  $\mathcal{B}$  et  $\mathcal{B}'$  deux bases de  $E$ ,  $\mathcal{C}$  et  $\mathcal{C}'$  deux bases de  $F$ .

Notons  $P$  la matrice de passage de  $\mathcal{B}$  à  $\mathcal{B}'$ ,

$Q$  la matrice de passage de  $\mathcal{C}$  à  $\mathcal{C}'$ ,

$A$  la matrice de  $f$  dans les bases  $\mathcal{B}$  et  $\mathcal{C}$ ,

$A'$  la matrice de  $f$  dans les bases  $\mathcal{B}'$  et  $\mathcal{C}'$ .

On a alors :

$$A' = Q^{-1} A P.$$

Les matrices  $A$  et  $A'$  sont dites équivalentes. Elles représentent la même application linéaire dans des bases différentes.

Si  $E = F$  avec  $\mathcal{B} = \mathcal{C}$  et  $\mathcal{B}' = \mathcal{C}'$ , alors  $P = Q$ , soit  $A' = P^{-1} A P$ .

Les matrices  $A$  et  $A'$  sont dites semblables.

### III Rang d'une matrice

- **Définition**

Soit  $A$  une matrice de format  $(n, p)$ ,  $E$  un espace vectoriel de dimension  $p$ ,  $F$  un espace vectoriel de dimension  $n$ .

Quelles que soient les bases  $\mathcal{B}$  et  $\mathcal{C}$  choisies dans  $E$  et  $F$ , le rang de l'application linéaire  $f$  associée à  $A$  est toujours le même. Ce rang est appelé rang de  $A$ .

C'est aussi le rang des vecteurs colonnes de  $A$ , c'est-à-dire la dimension du sous-espace vectoriel qu'ils engendrent.

Une matrice carrée d'ordre  $n$  est donc inversible si, et seulement si, son rang est égal à  $n$ .

- **Rang de la transposée**

$A$  et  ${}^tA$  ont même rang. On peut donc définir le rang de  $A$  à partir de ses lignes.

- **Calcul du rang**

Les opérations élémentaires sur les lignes, ou les colonnes, d'une matrice ne modifient pas le rang. On les utilise pour se ramener à une matrice de rang connu.

### IV Trace

- **Trace d'une matrice**

La trace d'une matrice  $A = (a_{ij})$ , carrée d'ordre  $n$ , est la somme de ses éléments diagonaux, soit :

$$\text{tr } A = \sum_{i=1}^n a_{ii} \in \mathbb{K}.$$

Elle vérifie les propriétés :

$$\text{tr } (A + B) = \text{tr } A + \text{tr } B \quad ; \quad \text{tr } (\lambda A) = \lambda \text{tr } A$$

$$\text{tr } (AB) = \text{tr } (BA) \quad ; \quad \text{tr } (PMP^{-1}) = \text{tr } M.$$

Attention, en général  $\text{tr } (ABC) \neq \text{tr } (BAC)$ .

- **Trace d'un endomorphisme**

Si  $f$  est un endomorphisme d'un espace vectoriel  $E$  de dimension finie, toutes les matrices qui le représentent sont semblables et ont la même trace.

Cette trace commune est la trace de l'endomorphisme  $f$ .

## Application

Soit  $f$  un endomorphisme d'un espace vectoriel  $E$  de dimension finie  $n$ , tel que  $f^n = 0$  et  $f^{n-1} \neq 0$ .

Déterminez une base de  $E$  dans laquelle la matrice de  $f$  soit :

$$\begin{pmatrix} 0 & 0 & \dots & \dots & 0 \\ 1 & \ddots & & & \vdots \\ 0 & 1 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}.$$

## Solution

Il s'agit de trouver une base  $(e_1, \dots, e_n)$  telle que :

$$\begin{cases} f(e_i) = e_{i+1} & \text{pour } 1 \leq i \leq n-1 \\ f(e_n) = 0. \end{cases}$$

On doit avoir  $e_i = f^{i-1}(e_1)$  pour  $1 \leq i \leq n$ , et, en particulier, il faut que  $e_n = f^{n-1}(e_1)$  soit non nul.

Après cette phase d'étude, construisons une base convenable.

Comme  $f^{n-1} \neq 0$ , il existe  $e_1$  tel que  $f^{n-1}(e_1) \neq 0$ .

Pour  $2 \leq i \leq n$ , posons  $e_i = f^{i-1}(e_1)$ , et montrons que  $\mathcal{B} = (e_1, \dots, e_n)$  est une base de  $E$ .

Comme  $E$  est de dimension  $n$ , il suffit de montrer que c'est une famille libre, puisque le nombre de vecteurs est égal à la dimension.

Soit  $\lambda_1, \dots, \lambda_n$  des scalaires tels que  $\sum_{i=1}^n \lambda_i e_i = 0$ . On a :

$$f^{n-1} \left( \sum_{i=1}^n \lambda_i e_i \right) = 0 = \lambda_1 f^{n-1}(e_1).$$

Comme  $f^{n-1}(e_1) \neq 0$ , on en déduit que  $\lambda_1 = 0$ .

À partir de  $f^{n-2} \left( \sum_{i=1}^n \lambda_i e_i \right) = 0$ , on obtient  $\lambda_2 = 0$ , et ainsi de suite.

On a bien construit une base de  $E$ . Et la matrice de  $f$  dans cette base est de la forme annoncée.

## Application

Déterminez (en discutant suivant les valeurs de  $\alpha$  et  $\beta$ ) le rang de :

$$A = \begin{pmatrix} 1 & -2 & 3 & 1 \\ -2 & 1 & 4 & 5 \\ 1 & \alpha & 1 & \beta \end{pmatrix}.$$

## Solution

Le rang de  $A$  est celui des vecteurs colonnes  $(C_1, C_2, C_3, C_4)$ .

C'est le même que celui de

$$(C_1, C'_2 = C_3 - 3C_1, C'_3 = C_2 + 2C_1, C'_4 = C_4 - C_1),$$

puis  $(C_1, C'_2, 3C'_2 + 10C'_3, -7C'_2 + 10C'_4)$ .

Sous forme matricielle, les matrices suivantes ont le même rang que  $A$  :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & 10 & -3 & 7 \\ 1 & -2 & \alpha + 2 & \beta - 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & 10 & 0 & 0 \\ 1 & -2 & 10\alpha + 14 & 10\beta + 4 \end{pmatrix}$$

Si  $\alpha = -\frac{7}{5}$  et  $\beta = -\frac{2}{5}$  alors le rang de  $A$  est égal à 2.

Sinon, le rang de  $A$  est égal à 3.

Le plan  $P = \text{Vect}(C_1, C_3)$  a pour équation  $-3x + y + 5z = 0$ . Les valeurs particulières obtenues pour  $\alpha$  et  $\beta$  correspondent à  $C_2 \in P$  et  $C_4 \in P$ .

## Application

Soit  $A$  une matrice de  $\mathcal{M}_n(\mathbb{R})$ . On définit l'endomorphisme  $\psi$  de  $\mathcal{M}_n(\mathbb{R})$  par :

$$X \mapsto \psi(X) = AX + XA.$$

Calculez la trace de  $\psi$  en fonction de celle de  $A$ .

## Solution

Soit  $E_{ij}$  la matrice de  $\mathcal{M}_n(\mathbb{R})$  qui comporte la valeur 1 à l'intersection de la ligne  $i$  et de la colonne  $j$ , et la valeur 0 partout ailleurs.

L'ensemble des  $E_{ij}$  pour  $1 \leq i \leq n$  et  $1 \leq j \leq n$  constitue la base canonique de  $\mathcal{M}_n(\mathbb{R})$  et leur produit vérifie  $E_{ij} E_{kl} = \delta_{jk} E_{il}$  où  $\delta_{jk}$  est le symbole de Kronecker.

Si  $A = (a_{ij})$ , on peut aussi écrire  $A = \sum_{i,j} a_{ij} E_{ij}$ . On a alors :

$$A E_{kl} = \sum_{i,j} a_{ij} E_{ij} E_{kl} = \sum_{i=1}^n a_{ik} E_{il} \quad \text{et} \quad E_{kl} A = \sum_{j=1}^n a_{lj} E_{kj},$$

$$\text{d'où} \quad \psi(E_{kl}) = \sum_{i=1}^n a_{ik} E_{il} + \sum_{j=1}^n a_{lj} E_{kj}.$$

La composante de  $\psi(E_{kl})$  sur  $E_{kl}$  est  $a_{kk} + a_{ll}$ . La trace de  $\psi$  est donc :

$$\begin{aligned} \text{tr } \psi &= \sum_{k,l} (a_{kk} + a_{ll}) = \sum_{k,l} a_{kk} + \sum_{k,l} a_{ll} = n \sum_{k=1}^n a_{kk} + n \sum_{l=1}^n a_{ll} \\ &= 2n \text{tr } A \end{aligned}$$

## Application

Dans  $\mathcal{M}_3(\mathbb{R})$ , quelles sont les racines de  $M^2 = O$  ?

## Solution

Considérons  $f \in \mathcal{L}(\mathbb{R}^3)$  tel que  $f \circ f = 0$ . On a alors  $\text{Im } f \subset \text{Ker } f$ .

D'après le théorème du rang,  $\dim \text{Im } f + \dim \text{Ker } f = 3$  ; d'où :  $\dim \text{Im } f \leq 1$ .

Si  $f$  n'est pas nul, c'est donc un endomorphisme de rang 1 dont l'image est incluse dans le noyau.

Soit  $(V_3)$  une base d'un supplémentaire du noyau. Le vecteur  $V_1 = f(V_3)$  est alors une base de  $\text{Im } f$  car  $V_1 \neq 0$ .

Comme  $\text{Im } f \subset \text{Ker } f$ , on peut alors choisir  $V_2$  pour que  $(V_1, V_2)$  soit une base de  $\text{Ker } f$ .

$\mathcal{B} = (V_1, V_2, V_3)$  est une base de  $\mathbb{R}^3$  et la matrice de  $f$  dans cette base est :

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Les solutions de l'équation sont donc la matrice nulle et toutes les matrices semblables à  $A$ .

## I Formes multilinéaires alternées

### • Définitions

Soit  $E$  un  $\mathbb{K}$ -espace vectoriel. Une application  $f$ , de  $E^n$  dans  $\mathbb{K}$ , est une forme  $n$ -linéaire si chacune de ses applications partielles

$$x_i \mapsto f(x_1, \dots, x_i, \dots, x_n)$$

est linéaire.

On dit de plus que  $f$  est alternée si  $f(x_1, \dots, x_i, \dots, x_n) = 0$  dès que deux vecteurs, au moins, sont égaux.

$f$  étant une forme  $n$ -linéaire alternée,  $\sigma$  une permutation appartenant à  $\mathcal{S}_n$ , de signature  $\varepsilon(\sigma)$ , on a :

$$f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = f(x_1, \dots, x_n) \varepsilon(\sigma).$$

### • Cas où $\dim E = n$

Soit  $E$  un  $\mathbb{K}$ -espace vectoriel de dimension  $n$ .

Pour toute base  $(e_1, \dots, e_n)$  de  $E$  et tout  $\lambda \in \mathbb{K}$ , il existe une forme  $n$ -linéaire alternée unique  $f$  telle que

$$f(e_1, \dots, e_n) = \lambda.$$

$f$  étant une forme  $n$ -linéaire alternée non nulle, on a :

$$(x_1, \dots, x_n) \text{ famille liée de } E \iff f(x_1, \dots, x_n) = 0.$$

## II Déterminants

### • Déterminant de $n$ vecteurs

Soit  $E$  un  $\mathbb{K}$ -espace vectoriel de dimension  $n$ , et  $\mathcal{B} = (e_1, \dots, e_n)$  une base de  $E$ .

On appelle déterminant de  $n$  vecteurs  $x_1, \dots, x_n$  de  $E$ , relativement à la base  $\mathcal{B}$  de  $E$ , la valeur notée  $\det_{\mathcal{B}}(x_1, \dots, x_n)$  de l'unique forme  $n$ -linéaire alternée  $\det_{\mathcal{B}}$  telle que  $\det_{\mathcal{B}}(e_1, \dots, e_n) = 1$ .

Si pour tout  $i \in \{1, \dots, n\}$ , on décompose  $x_i = \sum_{j=1}^n a_{ij} e_j$ , alors :

$$\det_B(x_1, \dots, x_n) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \times a_{1, \sigma(1)} \times \dots \times a_{n, \sigma(n)}.$$

- **Déterminant d'une matrice carrée**

Soit  $A = (a_{ij})$  une matrice carrée d'ordre  $n$ .

On appelle déterminant de  $A$  le déterminant de ses  $n$  vecteurs colonnes, considérés comme éléments de  $\mathbb{K}^n$  rapporté à sa base canonique.

- **Déterminant d'un endomorphisme**

Après avoir montré que deux matrices semblables ont le même déterminant, on appelle déterminant d'un endomorphisme  $f$ , le déterminant commun à ses matrices représentatives.

### III Propriétés des déterminants

- **Transposée**

$$\det A = \det {}^t A.$$

Les propriétés relatives aux colonnes sont donc aussi valables pour les lignes.

- **Propriétés d'une forme multilinéaire alternée**

- On ne change pas la valeur d'un déterminant en ajoutant à une de ses lignes (resp. colonnes) une combinaison linéaire des autres lignes (resp. colonnes). Cette propriété est très utilisée pour faire apparaître des 0 sur une colonne (resp. ligne).
- Multiplier une ligne (ou une colonne) d'un déterminant par un scalaire, c'est multiplier le déterminant par ce scalaire.

Si  $A \in \mathcal{M}_n(\mathbb{K})$ , on a donc  $\det(\lambda A) = \lambda^n \det(A)$  puisqu'on peut mettre  $\lambda$  en facteur dans chacune des  $n$  colonnes de  $A$ .

- Toute transposition sur les lignes (ou les colonnes) transforme  $\det A$  en  $-\det A$ .

- **Produit**

$$\det (A \ B) = \det A \times \det B.$$

- **Développement suivant une rangée**

**Définitions**

On appelle mineur de l'élément  $a_{ij}$  de  $\Delta$ , déterminant d'ordre  $n$ , le déterminant d'ordre  $n - 1$  obtenu en supprimant la  $i$ -ième ligne et la  $j$ -ième colonne de  $\Delta$ , sans changer l'ordre des autres rangées.

Notation :  $D_{ij}$ .

On appelle cofacteur de l'élément  $a_{ij}$ , le nombre  $A_{ij} = (-1)^{i+j} D_{ij}$ .

**Théorème**

Un déterminant est égal à la somme des produits deux à deux des éléments d'une rangée (ligne ou colonne) par leurs cofacteurs.

On utilise ce résultat après avoir fait apparaître sur une même rangée le plus possible de zéros.

Ce mode de calcul peut aussi servir de définition par récurrence d'un déterminant après avoir démontré que le résultat du développement est indépendant de la ligne, ou de la colonne, considérée.

C'est une définition plus accessible pour tous ceux que rebute un trop grand formalisme mathématique.

**Application**

Le déterminant d'une matrice triangulaire est égal au produit des éléments diagonaux.

- **Calcul par blocs**

Soit  $M$  une matrice carrée de la forme

$$M = \begin{pmatrix} A & C \\ 0 & D \end{pmatrix}$$

où  $A$  et  $D$  sont des matrices carrées. On a :

$$\det M = \det A \times \det D.$$

- **Matrice carrée inversible**

$$A \text{ inversible} \iff \det A \neq 0.$$

On a alors  $\det (A^{-1}) = (\det A)^{-1}$ .

## Application

Calculez le déterminant :

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

## Solution

Les transformations  $C_2 \leftarrow C_2 + C_1$  et  $C_4 \leftarrow C_4 + C_1$  ne modifient pas le déterminant. On peut ensuite, en développant suivant la troisième ligne, se ramener à un déterminant d'ordre 3 :

$$D = \begin{vmatrix} 1 & 4 & 1 & -1 \\ 2 & 2 & -2 & -2 \\ -1 & 0 & 0 & 0 \\ 2 & 7 & 3 & 8 \end{vmatrix} = (-1) \times (-1)^{3+1} \begin{vmatrix} 4 & 1 & -1 \\ 2 & -2 & -2 \\ 7 & 3 & 8 \end{vmatrix}.$$

Le déterminant d'ordre 3 peut se réduire à un déterminant d'ordre 2 avec, par exemple, les transformations  $C_2 \leftarrow C_2 + C_1$  et  $C_3 \leftarrow C_3 + C_1$  :

$$D = - \begin{vmatrix} 4 & 5 & 3 \\ 2 & 0 & 0 \\ 7 & 10 & 15 \end{vmatrix} = -2 \times (-1)^{2+1} \begin{vmatrix} 5 & 3 \\ 10 & 15 \end{vmatrix} = 90.$$

## Application

Calculez le déterminant d'ordre  $n \geq 1$  :

$$D_n = \begin{vmatrix} 1 & 1 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \ddots & \vdots \\ 0 & \ddots & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & 1 & 1 \end{vmatrix}.$$

## Solution

En développant suivant la première ligne, on obtient une expression de  $D_n$  sous la forme d'une différence de deux déterminants d'ordre  $n - 1$  :

$$D_n = \begin{vmatrix} 1 & 1 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix} - \begin{vmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix}.$$

En développant le deuxième déterminant suivant la première colonne on obtient :

$$D_n = D_{n-1} - D_{n-2} \quad \text{pour tout } n \geq 3.$$

On peut alors utiliser les résultats relatifs aux suites récurrentes linéaires (cf. Express Analyse fiche 11), ou remarquer que  $D_{n-1} = D_{n-2} - D_{n-3}$  pour  $n \geq 4$ , ce qui entraîne  $D_n = -D_{n-3}$  pour  $n \geq 4$ .

Il est alors possible de calculer  $D_{3p+1}$  en fonction de  $D_1 = 1$ ,  $D_{3p+2}$  en fonction de  $D_2 = 0$  et  $D_{3p}$  en fonction de  $D_3 = -1$ .

On a ainsi :

$$D_{3p+1} = -D_{3(p-1)+1} = (-1)^2 D_{3(p-2)+1} = \cdots = (-1)^p D_1 = (-1)^p.$$

De la même manière :

$$D_{3p+2} = -D_{3(p-1)+2} = (-1)^2 D_{3(p-2)+2} = \cdots = (-1)^p D_2 = 0$$

et :

$$D_{3p} = -D_{3(p-1)} = (-1)^2 D_{3(p-2)} = \cdots = (-1)^{p-1} D_3 = (-1)^p.$$

## Application

Soit  $n \in \mathbb{N}^*$ . On note  $\omega = \exp\left(i \frac{2\pi}{n}\right)$  et on considère la matrice carrée  $M$ , d'ordre  $n$ , dont le terme général situé sur la ligne  $p$  et la colonne  $q$  est :

$$m_{pq} = \omega^{(p-1)(q-1)}.$$

1. Calculez  $M^2$ .

2. Déduisez-en :  $|\det M|$ .

## Solution

1. Notons  $A = M^2 = (a_{pq})$ . Par définition d'un produit de matrices, on a :

$$\begin{aligned} a_{pq} &= \sum_{k=1}^n m_{pk} m_{kq} = \sum_{k=1}^n \omega^{(p-1)(k-1)} \omega^{(k-1)(q-1)} = \sum_{k=1}^n \omega^{(k-1)(p+q-2)} \\ &= \sum_{k=1}^n (\omega^{p+q-2})^{k-1}. \end{aligned}$$

On reconnaît une somme de termes d'une suite géométrique de raison  $\omega^{p+q-2}$ .

• Si  $\omega^{p+q-2} \neq 1$ , soit  $p+q-2 \neq 0$  et  $p+q-2 \neq n$ , on a :

$$a_{pq} = \frac{1 - (\omega^{p+q-2})^n}{1 - \omega^{p+q-2}} = 0 \quad \text{car } \omega^n = 1.$$

• Si  $\omega^{p+q-2} = 1$ , soit  $p+q-2 = 0$  ou  $p+q-2 = n$ , on a  $a_{pq} = n$ .

Donc :

$$M^2 = \begin{pmatrix} n & 0 & & 0 \\ 0 & 0 & & n \\ \vdots & & \ddots & \vdots \\ \vdots & n & 0 & \dots \\ 0 & n & 0 & \dots & 0 \end{pmatrix}.$$

2. Dans  $M^2$ , effectuons la permutation des colonnes :

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 1 & n & \dots & 3 & 2 \end{pmatrix},$$

dont la signature est :

$$\varepsilon(\sigma) = (-1)^{(n-1)+(n-2)+\dots+1} = (-1)^{\frac{n(n-1)}{2}}.$$

On se ramène ainsi à la matrice scalaire  $n I_n$  dont le déterminant est égal à  $n^n$ .

On obtient donc :

$$\det(M^2) = (\det M)^2 = \varepsilon(\sigma) n^n,$$

d'où l'on tire :

$$|\det M| = n^{\frac{n}{2}}.$$

## I Éléments propres d'un endomorphisme

Soit  $E$  un  $\mathbb{K}$ -espace vectoriel et  $f \in \mathcal{L}(E)$ .

### • Définitions

- Un vecteur non nul  $x \in E$  est un vecteur propre de  $f$  s'il existe  $\lambda \in \mathbb{K}$  tel que  $f(x) = \lambda x$ . Le scalaire  $\lambda$  est la valeur propre associée à  $x$ .
- Un scalaire  $\lambda \in \mathbb{K}$  est une valeur propre de  $f$  s'il existe un vecteur non nul  $x \in E$  tel que  $f(x) = \lambda x$ . Le vecteur  $x$  est un vecteur propre associé à  $\lambda$ .
- L'ensemble  $E_\lambda = \{x \in E ; f(x) = \lambda x\} = \text{Ker}(f - \lambda \text{Id}_E)$  est le sous-espace propre associé à  $\lambda$ .
- Le spectre de  $f$  est l'ensemble  $S_p(f)$  des valeurs propres de  $f$ .

### • Propriétés

- $\lambda$  est une valeur propre de  $f$  si, et seulement si,  $\text{Ker}(f - \lambda \text{Id}_E) \neq \{0\}$ .  
En particulier, 0 est valeur propre de  $f$  si, et seulement si,  $\text{Ker} f \neq \{0\}$ , soit  $f$  non injectif.
- Toute famille de vecteurs propres associés à des valeurs propres toutes distinctes, est libre.
- La somme de sous-espaces propres associés à des valeurs propres distinctes est directe.

### • Polynôme caractéristique

Soit  $E$  de dimension finie  $n$  et  $A$  une matrice carrée représentant un endomorphisme  $f$  dans une base fixée.

– Définitions

Le polynôme  $P(\lambda) = \det(A - \lambda I_n)$  est le polynôme caractéristique de  $A$ .

Deux matrices semblables ont le même polynôme caractéristique, ce qui permet de définir le polynôme caractéristique d'un endomorphisme.

Les zéros de  $P_A$  sont les valeurs propres de  $A$ . Si  $\lambda$  est racine d'ordre  $m_\lambda$  de  $P_A$ , on dit que  $\lambda$  est valeur propre d'ordre  $m_\lambda$ .

On a toujours  $1 \leq \dim(E_\lambda) \leq m_\lambda$  où  $E_\lambda$  est l'espace propre associé.

– Cas où  $P_A$  est scindé

En désignant par  $\lambda_i$  ( $1 \leq i \leq n$ ) les valeurs propres de  $A$ , on a alors :

$$\operatorname{tr} A = \sum_{k=1}^n \lambda_k \quad \text{et} \quad \det A = \prod_{k=1}^n \lambda_k.$$

## II Diagonalisation

Soit  $E$  de dimension finie.

### • Définitions

Un endomorphisme  $f \in \mathcal{L}(E)$  est diagonalisable s'il existe une base de  $E$  dans laquelle la matrice de  $f$  est diagonale, c'est-à-dire s'il existe une base de  $E$  formée de vecteurs propres de  $f$ .

Une matrice carrée  $A$  est diagonalisable si elle est semblable à une matrice diagonale  $D$ , c'est-à-dire si elle s'écrit

$$A = PDP^{-1}$$

où  $P$  est la matrice de passage de la base canonique de  $\mathbb{K}^n$  à une base de vecteurs propres de  $A$ .

### • Condition suffisante

Si  $\dim E = n$  et si  $f$  a  $n$  valeurs propres distinctes, alors  $f$  est diagonalisable.

### • Condition nécessaire et suffisante

$f$  diagonalisable

$\iff E$  est somme directe des sous-espaces propres ;

$\iff E$  admet une base de vecteurs propres ;

$\iff$  le polynôme caractéristique de  $f$  est scindé et, pour toute valeur propre  $\lambda_k$  d'ordre  $m_k$ , on a :

$$\dim(E_{\lambda_k}) = m_k.$$

### • Calcul de $A^m$

Si  $A$  est diagonalisable, il existe  $P$  telle que  $A = PDP^{-1}$ . On a alors  $A^m = PD^mP^{-1}$ .

Et si  $D = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$  alors  $D^m = \operatorname{diag}(\lambda_1^m, \dots, \lambda_n^m)$ .

### III Polynômes annulateurs

- **Définitions**

*Polynôme d'un endomorphisme*

Étant donné un endomorphisme  $f$  d'un  $\mathbb{K}$ -espace vectoriel  $E$  et un polynôme  $P(X) = a_0 + a_1 X + \cdots + a_p X^p$  à coefficients dans  $\mathbb{K}$ , on note  $P(f)$  l'endomorphisme de  $E$  défini par :

$$P(f) = a_0 \text{Id}_E + a_1 f + \cdots + a_p f^p.$$

*Polynôme annulateur*

On dit que  $P$  est un polynôme annulateur de  $f$  si  $P(f) = 0$ .

- **Condition nécessaire et suffisante pour  $f$  diagonalisable**

$f$  est diagonalisable si, et seulement si, il existe un polynôme scindé, annulateur de  $f$ , dont toutes les racines sont simples.

- **Théorème de Cayley-Hamilton**

*Théorème*

Si  $E$  est de dimension finie, le polynôme caractéristique de  $f$  est un polynôme annulateur de  $f$ .

*Application au calcul de  $A^m$*

Si  $P$  est un polynôme annulateur de  $A$ , la division euclidienne

$$X^m = P(X) Q_m(X) + R_m(X)$$

entraîne  $A^m = R_m(A)$ .

Cette méthode reste valable même si  $A$  n'est pas diagonalisable.

## Application

Diagonalisez la matrice

$$A = \begin{pmatrix} 1 & 1 & \dots & \dots & 1 \\ 1 & -1 & 0 & \dots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 1 & 0 & \dots & 0 & -1 \end{pmatrix} \in \mathcal{M}_n(\mathbb{R})$$

pour  $n \geq 2$ .

## Solution

$\lambda$  est une valeur propre de  $A$  si, et seulement si, il existe  $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$  non nul tel que

$AX = \lambda X$ , c'est-à-dire vérifie le système :

$$(S) \begin{cases} x_1 + \dots + x_n &= \lambda x_1 \\ x_1 &= (\lambda + 1)x_2 \\ &\vdots \\ x_1 &= (\lambda + 1)x_n \end{cases}$$

• **Premier cas**  $\lambda = -1$

$(S)$  se réduit alors à  $\begin{cases} x_1 &= 0 \\ x_2 + \dots + x_n &= 0 \end{cases}$

$\text{Ker}(A + I)$  est donc de dimension  $n - 2$ .

• **Second cas**  $\lambda \neq -1$

$(S)$  s'écrit alors :

$$\begin{cases} x_2 = x_3 = \dots = x_n = \frac{x_1}{\lambda + 1} \\ x_1 + \dots + x_n = \lambda x_1 \end{cases} \iff \begin{cases} x_2 = x_3 = \dots = x_n = \frac{x_1}{\lambda + 1} \\ x_1 + (n-1) \frac{x_1}{\lambda + 1} = \lambda x_1 \end{cases}$$

La dernière équation est équivalente à  $x_1 (\lambda^2 - n) = 0$ .

Donc  $\lambda = \varepsilon \sqrt{n}$  (avec  $\varepsilon = \pm 1$ ) est valeur propre de  $A$ , le sous-espace propre associé étant engendré par  $(\lambda + 1, 1, 1, \dots, 1)$ .

- En conclusion,  $A$  est diagonalisable. Elle est semblable à :

$$D = \begin{pmatrix} \sqrt{n} & 0 & \dots & \dots & 0 \\ 0 & -\sqrt{n} & \ddots & & \vdots \\ \vdots & \ddots & -1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & -1 \end{pmatrix}$$

une matrice de passage possible étant :

$$P = \begin{pmatrix} 1 + \sqrt{n} & 1 - \sqrt{n} & 0 & \dots & 0 \\ 1 & 1 & 1 & \dots & 1 \\ \vdots & \vdots & -1 & & 0 \\ \vdots & \vdots & & \ddots & \\ 1 & 1 & 0 & & -1 \end{pmatrix}.$$

## Application

Soit  $E$  un espace vectoriel de dimension  $n$  et  $f$  un endomorphisme de  $E$  de rang 1. Montrez que  $\text{Im } f \subset \text{Ker } f$  si, et seulement si,  $f$  n'est pas diagonalisable.

## Solution

- Supposons  $\text{Im } f \subset \text{Ker } f$ . Cette inclusion est équivalente à  $f^2 = 0$ . La seule valeur propre possible est donc 0.

Si  $f$  était diagonalisable, on aurait alors  $f = 0$ , ce qui serait contradictoire avec  $\text{rg } f = 1$ .

$f$  n'est donc pas diagonalisable.

- Montrons la contraposée de l'autre implication. Pour ceci, supposons que  $\text{Im } f$  ne soit pas inclus dans  $\text{Ker } f$ .

$\text{Im } f$  est une droite par hypothèse, ce qui entraîne que  $\text{Ker } f$  est un hyperplan d'après le théorème du rang. S'il n'y a pas inclusion, on a

$$E = \text{Im } f \oplus \text{Ker } f.$$

La matrice de  $f$  dans une base adaptée à cette somme directe est diagonale puisque  $f(e_1) \in \text{Im } f$  et  $(e_1)$  base de  $\text{Im } f$ .

$f$  est donc diagonalisable.

## Application

Calculez  $A^n$  pour  $A = \begin{pmatrix} -1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$  et  $n \in \mathbb{N}$ .

## Solution

Le polynôme caractéristique de  $A$  s'écrit :

$$\begin{aligned} \det(A - \lambda I_3) &= \begin{vmatrix} -\lambda & 0 & 1 \\ -\lambda & -1 - \lambda & 0 \\ -\lambda & 1 & -1 - \lambda \end{vmatrix} \\ &= \begin{vmatrix} -\lambda & 0 & 1 \\ 0 & -1 - \lambda & -1 \\ 0 & 1 & -2 - \lambda \end{vmatrix} \quad \text{par } C_1 \leftarrow C_1 + C_2 + C_3 \\ &= -\lambda(\lambda^2 + 3\lambda + 3) \quad \text{par } L_2 \leftarrow L_2 - L_1 \quad \text{puis } L_3 \leftarrow L_3 - L_1 \end{aligned}$$

$A$  est donc diagonalisable sur  $\mathbb{C}$  car elle a trois valeurs propres complexes distinctes :

$$0, \frac{-3 + i\sqrt{3}}{2} = \sqrt{3} e^{\frac{5i\pi}{6}} \text{ et } \sqrt{3} e^{-\frac{5i\pi}{6}}.$$

Pour  $n \geq 1$ ,  $A^n$  est donc de la forme :

$$A^n = (\sqrt{3})^n \left( e^{\frac{5in\pi}{6}} B + e^{-\frac{5in\pi}{6}} C \right) = (\sqrt{3})^n \left[ P \cos\left(\frac{5n\pi}{6}\right) + Q \sin\left(\frac{5n\pi}{6}\right) \right].$$

Pour  $n = 1$  et  $n = 2$  on a :

$$\begin{cases} A &= \sqrt{3} \left( -\frac{\sqrt{3}}{2} P + \frac{1}{2} Q \right) \\ A^2 &= 3 \left( \frac{1}{2} P - \frac{\sqrt{3}}{2} Q \right) \end{cases} \iff \begin{cases} P &= -\frac{1}{3} (3A + A^2) \\ Q &= -\frac{1}{\sqrt{3}} (A + A^2) \end{cases}$$

soit

$$P = -\frac{1}{3} \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix} \text{ et } Q = -\frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}.$$

## I Forme bilinéaire et forme quadratique

- **Définitions**

### *Forme bilinéaire symétrique*

Une forme bilinéaire  $f$  sur  $E$  est une application de  $E \times E$  dans  $\mathbb{K}$  (sous-corps de  $\mathbb{C}$ ), linéaire par rapport à chaque variable.

Elle est symétrique si :

$$\forall (x, y) \in E \times E \quad f(x, y) = f(y, x).$$

### *Forme quadratique*

Une application  $q$  de  $E$  dans  $\mathbb{K}$  est une forme quadratique sur  $E$  s'il existe une forme bilinéaire symétrique  $f$  telle que :

$$\forall x \in E \quad q(x) = f(x, x).$$

$q$  est la forme quadratique associée à  $f$ .

### *Forme polaire d'une forme quadratique*

Une forme quadratique  $q$  sur  $E$  est associée à une seule forme bilinéaire symétrique  $f$  donnée par :

$$\forall (x, y) \in E \times E \quad f(x, y) = \frac{1}{2} [q(x + y) - q(x) - q(y)].$$

$f$  est la forme polaire de  $q$ .

### *Forme positive*

Si  $K = \mathbb{R}$ , une forme quadratique  $q$ , et sa forme polaire  $f$ , sont dites positives si :

$$\forall x \in E \quad q(x) \geq 0.$$

### *Forme définie positive*

Si  $K = \mathbb{R}$ , une forme quadratique  $q$ , et sa forme polaire  $f$ , sont dites définies positives si :

$$\forall x \in E \setminus \{0\} \quad q(x) > 0.$$

- **Cas où  $E$  est de dimension finie**

Soit  $E$  de dimension  $n$  et  $\mathcal{B} = (e_1, \dots, e_n)$  une base de  $E$ .

### Matrice d'une forme bilinéaire

Si  $x = \sum_{i=1}^n x_i e_i$  et  $y = \sum_{j=1}^n y_j e_j$ , alors  $f(x, y) = \sum_{i,j} x_i y_j f(e_i, e_j)$ .

La matrice de  $f$  dans la base  $\mathcal{B}$  est la matrice  $A$  de  $\mathcal{M}_n(\mathbb{K})$  de terme général  $a_{ij} = f(e_i, e_j)$ .

En posant  $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$  et  $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ , on a :

$$f(x, y) = {}^t X A Y = {}^t Y A X$$

$f$  est symétrique si, et seulement si, la matrice  $A$  est symétrique.

### Expression d'une forme quadratique

$q(x)$  est un polynôme homogène de degré 2 en  $x_1, \dots, x_n$  (combinaison linéaire d'expressions du type  $x_i^2$  ou  $x_i x_j$  avec  $i \neq j$ ).

Réciproquement, tout polynôme homogène de degré 2 par rapport aux coordonnées de  $x$  dans  $\mathcal{B}$  est une forme quadratique sur  $E$ .

## II Espaces préhilbertiens réels

### • Produit scalaire

#### Définitions

Soit  $E$  un  $\mathbb{R}$ -espace vectoriel. Un produit scalaire sur  $E$  est une forme bilinéaire  $\varphi$ , symétrique, définie, positive.

On dit que  $(E, \varphi)$  est un espace préhilbertien réel.

$\varphi(x, y)$  se note :  $\langle x | y \rangle$  ou  $(x | y)$  ou  $x \cdot y$ .

#### Exemples

Dans  $\mathbb{R}^n$   $\langle X | Y \rangle = {}^t X Y = \sum_{i=1}^n x_i y_i$ .

Dans  $E = \mathcal{C}([a, b], \mathbb{R})$   $\langle f | g \rangle = \int_a^b f(t)g(t)dt$ .

Dans  $\mathcal{M}_n(\mathbb{R})$   $\langle A | B \rangle = \text{tr}({}^t A B)$ .

- **Norme euclidienne**

$E$  étant un  $\mathbb{R}$ -espace vectoriel muni d'un produit scalaire, en posant

$$\forall x \in E \quad \|x\| = \sqrt{\langle x | x \rangle},$$

on définit une norme sur  $E$ .

- **Relations entre produit scalaire et norme**

*Égalité de polarisation*

$$\forall x \in E \quad \forall y \in E \quad \|x + y\|^2 = \|x\|^2 + \|y\|^2 + 2 \langle x | y \rangle$$

ce qui permet d'obtenir le produit scalaire  $\langle x | y \rangle$  en fonction des normes.

*Identité du parallélogramme*

$$\forall x \in E \quad \forall y \in E \quad \|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2).$$

- **Inégalité de Cauchy-Schwarz**

$$\forall x \in E \quad \forall y \in E \quad |\langle x | y \rangle| \leq \|x\| \|y\|.$$

Dans cette inégalité, l'égalité a lieu si, et seulement si,  $x$  et  $y$  sont liés.

### III Espaces euclidiens

- **Définition**

Un espace vectoriel euclidien  $E$  est un espace préhilbertien réel de dimension finie  $n$ .

- **Propriétés**

Il existe une base orthonormale  $\mathcal{B} = (e_1, \dots, e_n)$  de  $E$  et, dans une telle base, pour tout  $x \in E$  et  $y \in E$ , on a :

$$x = \sum_{i=1}^n \langle e_i | x \rangle e_i ; \quad \langle x | y \rangle = {}^t X Y ; \quad \|x\| = \sqrt{\sum_{i=1}^n x_i^2}$$

où  $X$  et  $Y$  sont les matrices colonnes des composantes de  $x$  et de  $y$  dans  $\mathcal{B}$ .

- **Orientation**

*Orientation de  $E$*

Une base orthonormale  $\mathcal{B}_0$  étant choisie, on dit que  $\mathcal{B}$  est une base directe si  $\det_{\mathcal{B}_0} \mathcal{B} > 0$  et indirecte si  $\det_{\mathcal{B}_0} \mathcal{B} < 0$ .

*Orientation d'un hyperplan*

Un hyperplan est orienté par le choix d'un vecteur normal  $\vec{n}$ .

Une base  $\mathcal{B}$  de  $H$  est dite directe si, et seulement si,  $(\mathcal{B}, \vec{n})$  est une base directe de  $E$ .

## Application

Soit  $E = \mathbb{R}_2[X]$ . On définit :

$$\langle P|Q \rangle = P(-1) Q(-1) + P(0) Q(0) + P(1) Q(1).$$

Montrez que c'est un produit scalaire sur  $E$ .

## Solution

Il est immédiat que l'application  $\varphi$ , de  $E^2$  dans  $\mathbb{R}$ , définie par :

$$\varphi(P, Q) = P(-1) Q(-1) + P(0) Q(0) + P(1) Q(1)$$

est symétrique et bilinéaire.

Elle est positive puisque  $\varphi(P, P) = [P(-1)]^2 + [P(0)]^2 + [P(1)]^2 \geq 0$  pour tout  $P$ .

Pour montrer qu'elle est définie, considérons un polynôme  $P$  tel que

$$\varphi(P, P) = [P(-1)]^2 + [P(0)]^2 + [P(1)]^2 = 0.$$

On a alors  $P(-1) = P(0) = P(1) = 0$ . Le polynôme admet 3 racines distinctes, alors qu'il est de degré  $\leq 2$ . On a donc bien  $P = 0$ .

## Application

1. Si  $A = (a_{ij})$  est une matrice carrée d'ordre  $n$ , on appelle trace de  $A$  la somme de ses éléments diagonaux, c'est-à-dire le scalaire  $\text{tr} A = \sum_{i=1}^n a_{ii}$ .

Montrez que  $\text{tr} A = \text{tr}({}^t A)$ , que  $\text{tr}(AB) = \text{tr}(BA)$  et que  $\text{tr}$  est une forme linéaire sur  $\mathcal{M}_n(\mathbb{R})$ .

2. On considère l'application  $\varphi$  de  $\mathcal{M}_n(\mathbb{R}) \times \mathcal{M}_n(\mathbb{R})$  dans  $\mathbb{R}$  définie par :

$$\varphi(M, N) = \text{tr}({}^t M N).$$

Montrez que  $\varphi$  est un produit scalaire sur  $\mathcal{M}_n(\mathbb{R})$  et que la base canonique de  $\mathcal{M}_n(\mathbb{R})$  est orthonormale.

3. Soit  $A \in \mathcal{M}_n(\mathbb{R})$ . Montrez que  $|\text{tr} A| \leq \sqrt{n \text{tr}({}^t A A)}$ . Quand a-t-on l'égalité ?

## Solution

1. Une matrice carrée et sa transposée ont la même trace puisque les éléments diagonaux sont les mêmes.

Soit  $A$  et  $B$  deux matrices de  $\mathcal{M}_n(\mathbb{R})$  et  $C = AB = (c_{ij})$ .

Comme  $c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}$ , on a

$$\operatorname{tr} C = \sum_{i=1}^n \sum_{k=1}^n a_{ik} b_{ki} = \sum_{k=1}^n \sum_{i=1}^n b_{ik} a_{ki} = \operatorname{tr}(BA).$$

$\operatorname{tr}$  est une forme linéaire sur  $\mathcal{M}_n(\mathbb{R})$  puisque elle est à valeurs réelles et :

$$\operatorname{tr}(\alpha A + \beta B) = \sum_{i=1}^n (\alpha a_{ii} + \beta b_{ii}) = \alpha \sum_{i=1}^n a_{ii} + \beta \sum_{i=1}^n b_{ii} = \alpha \operatorname{tr} A + \beta \operatorname{tr} B.$$

2. • Pour tout  $(M, N) \in \mathcal{M}_n^2(\mathbb{R})$ , on a :

$$\varphi(M, N) = \operatorname{tr}({}^t MN) = \operatorname{tr}({}^t({}^t MN)) = \operatorname{tr}({}^t NM) = \varphi(N, M).$$

$\varphi$  est donc symétrique.

Pour tout  $(M, N, N') \in \mathcal{M}_n^3(\mathbb{R})$  et tout  $(\lambda, \lambda') \in \mathbb{R}^2$ , on a :

$$\begin{aligned} \varphi(M, \lambda N + \lambda' N') &= \operatorname{tr}({}^t M(\lambda N + \lambda' N')) \\ &= \lambda \operatorname{tr}({}^t MN) + \lambda' \operatorname{tr}({}^t MN') = \lambda \varphi(M, N) + \lambda' \varphi(M, N') \end{aligned}$$

$\varphi$  est donc bilinéaire symétrique.

Si  $M = (m_{ij})$ , le terme de  ${}^t MM$  situé sur la  $i$ -ième ligne et la  $j$ -ième colonne est

$$\sum_{k=1}^n m_{ki} m_{kj}. \text{ On a donc : } \varphi(M, M) = \sum_{i=1}^n \left( \sum_{k=1}^n m_{ki}^2 \right) \geq 0.$$

D'autre part, si  $\varphi(M, M) = 0$ , l'expression précédente montre que  $m_{ki} = 0$  pour tous  $k$  et  $i$ , soit  $M = 0$ .

$\varphi$  est donc définie positive, ce qui achève la démonstration de  $\varphi$  produit scalaire.

• Soit  $(E_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$  la base canonique de  $\mathcal{M}_n(\mathbb{R})$ .

Vous savez déjà (sinon, vérifiez les résultats) que :

$$\begin{aligned} E_{ij} \times E_{kl} &= 0 & \text{si } j \neq k \\ &= E_{il} & \text{si } j = k. \end{aligned}$$

$$\text{Calculons } \varphi(E_{ij}, E_{kl}) = \operatorname{tr}({}^t E_{ij} E_{kl}) = \operatorname{tr}(E_{ji} E_{kl}).$$

Si  $(i, j) = (k, l)$ , on a  $\varphi(E_{ij}, E_{ij}) = \text{tr}(E_{ji} E_{ij}) = \text{tr}(E_{jj}) = 1$ .

Si  $(i, j) \neq (k, l)$ , on a  $i \neq k$  ou  $j \neq l$ .

Pour  $i \neq k$ , on a  $E_{ji} E_{kl} = 0$ , d'où  $\varphi(E_{ij}, E_{kl}) = 0$ .

Pour  $i = k$ , on a  $E_{ji} E_{kl} = E_{jl}$ , d'où  $\varphi(E_{ij}, E_{kl}) = \text{tr}(E_{jl}) = 0$  puisque  $j \neq l$ .

La famille  $(E_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$  est donc une base orthonormale de  $\mathcal{M}_n(\mathbb{R})$ .

**3.** En appliquant l'inégalité de Cauchy-Schwarz au produit scalaire  $\varphi$  et aux matrices  $A$  et  $I_n$ , on obtient :

$$|\varphi(I_n, A)| \leq \sqrt{\varphi(I_n, I_n) \varphi(A, A)}$$

c'est-à-dire :

$$|\text{tr} A| \leq \sqrt{n \text{tr}(A A)}.$$

L'égalité a lieu si, et seulement si, les deux vecteurs  $A$  et  $I_n$  sont colinéaires, c'est-à-dire si  $A$  est une matrice scalaire.

## Application

Soit  $\mathbb{R}^n$  muni de sa base canonique  $(e_i)$ ,  $q$  une forme quadratique définie positive et  $f$  sa forme polaire. La matrice de  $f$  est  $A = (a_{ij})$ . Montrez que :

1. on a  $a_{ii} > 0$  pour tout  $i$  ;
2. on a  $\max_{ij} |a_{i,j}| = \max_i |a_{ii}|$ .

## Solution

**1.** Comme  $q$  est définie positive, on a :  $a_{ii} = f(e_i, e_i) = q(e_i) > 0$ .

**2.** On a toujours  $\max_{ij} |a_{i,j}| \geq \max_i |a_{ii}|$ .

Pour démontrer l'autre inégalité, considérons  $i \neq j$  quelconques. On a :

$$q(e_i + e_j) = q(e_i) + q(e_j) + 2a_{ij} > 0 \text{ et}$$

$$q(e_i - e_j) = q(e_i) + q(e_j) - 2a_{ij} > 0,$$

$$\text{ce qui entraîne : } 2|a_{ij}| < a_{ii} + a_{jj} \leq 2 \max_i |a_{ii}|$$

puis :  $\max_{ij} |a_{i,j}| \leq \max_i |a_{ii}|$ . L'égalité annoncée est donc démontrée.

## I Vecteurs orthogonaux

- **Définitions**

Deux vecteurs  $x$  et  $y$  sont orthogonaux si  $\langle x|y \rangle = 0$  ; on note  $x \perp y$ .

Une famille de vecteurs  $(x_i)_{i \in I}$  est orthogonale si ses vecteurs sont deux à deux orthogonaux.

Une famille de vecteurs  $(x_i)_{i \in I}$  est orthonormale si elle est orthogonale et si les vecteurs sont tous unitaires (c'est-à-dire de norme égale à 1).

- **Propriété**

Une famille orthogonale de vecteurs non nuls est libre.

- **Théorème de Pythagore**

Si  $(x_i)_{i \in I}$  est une famille orthogonale finie, on a :

$$\left\| \sum_{i \in I} x_i \right\|^2 = \sum_{i \in I} \|x_i\|^2.$$

## II Sous-espaces vectoriels orthogonaux

- **Définitions**

Soit  $F$  et  $G$  deux sous-espaces vectoriels d'un espace préhilbertien  $E$ .

On dit que  $F$  et  $G$  sont orthogonaux, et on note  $F \perp G$ , quand :

$$\forall x \in F \quad \forall y \in G \quad \langle x|y \rangle = 0.$$

Dans  $\mathbb{R}^3$ , on définit ainsi l'orthogonalité d'une droite et d'un plan, mais deux plans ne peuvent pas être orthogonaux.

L'orthogonal de  $F$  est le sous-espace vectoriel défini par :

$$F^\perp = \{x \in E ; \forall y \in F \langle x|y \rangle = 0\}.$$

- **Propriétés**

$$E^\perp = \{0\}; \{0\}^\perp = E; F \perp G \iff F \subset G^\perp \iff G \subset F^\perp.$$

$$F \subset G \implies G^\perp \subset F^\perp; F \subset (F^\perp)^\perp; F \cap F^\perp = \{0\}.$$

### III Supplémentaire orthogonal

- **Définition**

Dans un espace préhilbertien  $E$ , deux sous-espaces vectoriels  $F$  et  $G$  sont dits supplémentaires orthogonaux dans  $E$  quand :

$$E = F \oplus G \quad \text{et} \quad F \perp G.$$

On note souvent cette situation :  $E = F \overset{\perp}{\oplus} G$ .

- **Propriété**

Si  $F$  et  $G$  sont supplémentaires orthogonaux dans  $E$ , on a  $F = G^\perp$ ,  $G = F^\perp$ , d'où  $(F^\perp)^\perp = F$ .

- **Projecteur orthogonal, symétrie vectorielle orthogonale**

- $p \in \mathcal{L}(E)$  est un projecteur orthogonal quand  $p^2 = p$  et  $\text{Im } p \perp \text{Ker } p$ .  $\text{Im } p$  et  $\text{Ker } p$  sont alors supplémentaires orthogonaux.
- Dans ce cas, la symétrie vectorielle associée  $s = 2p - \text{Id}_E$  est une symétrie orthogonale par rapport à  $\text{Im } p$ , qui est aussi l'ensemble des vecteurs invariants de  $s$ .

### IV Cas d'un espace euclidien

- **Méthode d'orthogonalisation de Schmidt**

Soit  $(x_1, \dots, x_n)$  une famille libre de  $E$  ; il existe une famille libre orthogonale  $(y_1, \dots, y_n)$  telle que  $\text{Vect}(x_1, \dots, x_n) = \text{Vect}(y_1, \dots, y_n)$ .

Dans la méthode de Schmidt, elle se construit par récurrence en posant :

$$y_1 = x_1 \text{ puis } y_k = x_k - \sum_{i=1}^{k-1} \lambda_i y_i \quad \text{avec} \quad \lambda_i = \frac{\langle y_i | x_k \rangle}{\langle y_i | y_i \rangle}.$$

Les dénominateurs ci-dessus ne s'annulent jamais.

- **Intérêt d'une base orthonormale**

Soit  $E$  muni d'une base orthonormale  $(e_1, \dots, e_n)$ .

$$\text{Si } x = \sum_{i=1}^n x_i e_i, \quad \text{on a : } x_i = \langle x | e_i \rangle.$$

## V Cas d'un sous-espace $F$ de dimension finie

- **Théorème**

$$E = F \oplus F^\perp.$$

On peut donc définir le projecteur orthogonal  $p_F$  sur  $F$ .

Si  $(e_1, \dots, e_p)$  est une base orthonormale de  $F$ , on a :

$$\forall x \in E \quad p_F(x) = \sum_{i=1}^p \langle e_i | x \rangle e_i.$$

- **Définition**

On appelle distance d'un élément  $x$  de  $E$  au sous-espace de dimension finie  $F$  le nombre :

$$d(x, F) = \inf_{z \in F} \|x - z\|.$$

- **Théorème**

$d(x, F)$  est un minimum atteint en un point, et un seul,  $z = p_F(x)$ , et l'on a :

$$\|x\|^2 = \|p_F(x)\|^2 + d(x, F)^2.$$

## Application

Soit  $E$  un espace vectoriel euclidien et  $f$  une application de  $E$  dans  $E$  qui conserve le produit scalaire, soit

$$\forall x \in E \quad \forall y \in E \quad \langle f(x)|f(y) \rangle = \langle x|y \rangle.$$

Montrez que  $f$  est linéaire.

## Solution

Soit  $x_1 \in E$ ,  $x_2 \in E$ ,  $\lambda_1 \in \mathbb{R}$  et  $\lambda_2 \in \mathbb{R}$  ; montrons que :

$$z = f(\lambda_1 x_1 + \lambda_2 x_2) - \lambda_1 f(x_1) - \lambda_2 f(x_2) = 0.$$

Le vecteur  $z$  appartient à  $\text{Vect}(f(E))$ .

Pour tout  $y \in E$ , l'hypothèse vérifiée par  $f$  et les propriétés d'un produit scalaire entraînent :

$$\begin{aligned} \langle f(\lambda_1 x_1 + \lambda_2 x_2)|f(y) \rangle &= \langle \lambda_1 x_1 + \lambda_2 x_2|y \rangle \\ &= \lambda_1 \langle x_1|y \rangle + \lambda_2 \langle x_2|y \rangle \\ &= \lambda_1 \langle f(x_1)|f(y) \rangle + \lambda_2 \langle f(x_2)|f(y) \rangle \\ &= \langle \lambda_1 f(x_1) + \lambda_2 f(x_2)|f(y) \rangle \end{aligned}$$

Par conséquent  $\langle z|f(y) \rangle = 0$  pour tout  $y \in E$ , soit  $z \in [\text{Vect}(f(E))]^\perp$ .

On a donc :  $z \in \text{Vect}(f(E)) \cap [\text{Vect}(f(E))]^\perp$ , c'est-à-dire  $z = 0$ .

## Application

Dans un espace vectoriel euclidien  $E$ , on considère une famille  $(e_1, \dots, e_n)$  de vecteurs unitaires tels que

$$\forall x \in E \quad \|x\|^2 = \sum_{i=1}^n \langle x|e_i \rangle^2.$$

Montrez qu'il s'agit d'une base orthonormale de  $E$ .

## Solution

• En écrivant l'hypothèse pour  $x = e_j$ , on a :

$$\|e_j\|^2 = \sum_{i=1}^n \langle e_j|e_i \rangle^2 = \|e_j\|^2 + \sum_{\substack{1 \leq i \leq n \\ i \neq j}} \langle e_j|e_i \rangle^2$$

D'où  $\langle e_j|e_i \rangle = 0$  pour  $j \neq i$ .

Le système est donc orthogonal, et même orthonormal puisque les  $e_i$  sont supposés unitaires.

On sait qu'un système orthogonal de vecteurs non nuls est une famille libre.

Il reste à montrer que c'est une famille génératrice de  $E$ .

• Soit  $F = \text{Vect}(e_1, \dots, e_n)$  et montrons que  $F = E$  en déterminant  $F^\perp$ .

Soit  $x \in F^\perp$ , c'est-à-dire que  $\langle x | e_i \rangle = 0$  pour tout  $i$ . En utilisant l'hypothèse, on en déduit :

$$\|x\|^2 = \sum_{i=1}^n \langle x | e_i \rangle^2 = 0$$

d'où  $x = 0$ . On a donc  $F^\perp = \{0\}$  et, par conséquent,  $F = E$ .

## Application

Déterminez :  $\inf_{(a,b) \in \mathbb{R}^2} \int_0^1 (x \ln x - ax^2 - bx)^2 dx$ .

## Solution

Dans  $E = \mathcal{C}([0,1], \mathbb{R})$ , muni du produit scalaire

$$\langle f | g \rangle = \int_0^1 f(x) g(x) dx,$$

considérons le sous-espace vectoriel  $F = \text{Vect}(x, x^2)$ .

La fonction  $x \mapsto x \ln x$ , prolongée par continuité en 0, appartient à  $E$ .

$$\int_0^1 (x \ln x - ax^2 - bx)^2 dx$$

est alors le carré de la distance de  $x \ln x$  à  $F$ .

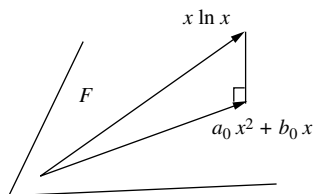


Figure 23.1

Son minimum est atteint pour un unique élément  $a_0x^2 + b_0x$  de  $F$  tel que  $x \ln x - (a_0x^2 + b_0x)$  soit orthogonal à  $F$ , ce qui est équivalent à :

$$\begin{cases} 0 = \langle x \ln x - a_0x^2 - b_0x | x \rangle = \int_0^1 (x^2 \ln x - a_0x^3 - b_0x^2) dx \\ 0 = \langle x \ln x - a_0x^2 - b_0x | x^2 \rangle = \int_0^1 (x^3 \ln x - a_0x^4 - b_0x^3) dx \end{cases}$$

En intégrant par parties, on obtient :

$$\int_0^1 x^2 \ln x dx = -\frac{1}{9} \quad ; \quad \int_0^1 x^3 \ln x dx = -\frac{1}{16},$$

d'où :

$$\left. \begin{aligned} \frac{a_0}{5} + \frac{b_0}{4} &= -\frac{1}{16} \\ \frac{a_0}{4} + \frac{b_0}{3} &= -\frac{1}{9} \end{aligned} \right\} \iff \begin{cases} a_0 = \frac{5}{3} \\ b_0 = -\frac{19}{12} \end{cases}$$

Sans calculatrice, le calcul direct de  $\int_0^1 (x \ln x - \frac{5}{3}x^2 + \frac{19}{12}x)^2 dx$  est long.

Dans ce cas, Il vaut mieux utiliser le théorème de Pythagore et calculer

$$\|x \ln x\|^2 - \left\| \frac{5}{3}x^2 - \frac{19}{12}x \right\|^2.$$

$$\|x \ln x\|^2 = \int_0^1 x^2 \ln^2 x dx = \left[ \frac{x^3}{3} \ln^2 x \right]_0^1 - \int_0^1 2 \frac{x^2}{3} \ln x dx = \frac{2}{27}$$

$$\left\| \frac{5}{3}x^2 - \frac{19}{12}x \right\|^2 = \int_0^1 \left( \frac{25}{9}x^4 - \frac{95}{18}x^3 + \frac{361}{144}x^2 \right) dx = \frac{31}{432}$$

Donc

$$\inf_{(a,b) \in \mathbb{R}^2} \int_0^1 (x \ln x - ax^2 - bx)^2 dx = \frac{2}{27} - \frac{31}{432} = \frac{1}{432}.$$

## I Endomorphismes orthogonaux

- **Définition**

Dans un espace vectoriel euclidien  $E$ , un endomorphisme  $f$  est dit orthogonal s'il conserve le produit scalaire, soit :

$$\forall x \in E \quad \forall y \in E \quad \langle f(x) | f(y) \rangle = \langle x | y \rangle .$$

On dit aussi que  $f$  est une isométrie vectorielle.

- **Conditions équivalentes**

$f \in \mathcal{L}(E)$  est orthogonal si, et seulement si, il vérifie l'une des conditions suivantes :

–  $f$  conserve la norme, soit

$$\forall x \in E \quad \|f(x)\| = \|x\|$$

– il existe une base orthonormale  $\mathcal{B}$  telle que  $f(\mathcal{B})$  soit une base orthonormale ;

– pour toute base orthonormale  $\mathcal{B}$ ,  $f(\mathcal{B})$  est une base orthonormale.

- **Corollaire**

Un endomorphisme orthogonal  $f$  appartient à  $\text{GL}(E)$ . Il est appelé automorphisme orthogonal de  $E$ .

Ses seules valeurs propres possibles sont 1 et  $-1$ .

- **Exemples**

Les symétries orthogonales sont des automorphismes orthogonaux.

Mais un projecteur orthogonal distinct de l'identité n'en est pas un ; si  $x \in \text{Ker } p$  avec  $x \neq 0$ , on a  $\|p(x)\| < \|x\|$ .

- **Groupe orthogonal**

L'ensemble des automorphismes orthogonaux de  $E$  est noté  $\text{O}(E)$  et appelé groupe orthogonal de  $E$ . C'est un sous-groupe de  $\text{GL}(E)$ .

## II Matrices orthogonales

- Définition**

Une matrice carrée  $A$  est dite orthogonale si c'est la matrice de passage d'une base orthonormale  $\mathcal{B}$  à une base orthonormale  $\mathcal{B}'$ .

L'ensemble des matrices orthogonales d'ordre  $n$  est le groupe orthogonal d'ordre  $n$  ; il est noté  $O(n)$ .

- Conditions équivalentes**

Une matrice carrée est orthogonale si, et seulement si, ses vecteurs colonnes (et aussi ses vecteurs lignes) vérifient :

$$\forall i \in \{1, \dots, n\} \quad \forall j \in \{1, \dots, n\} \quad \langle C_i | C_j \rangle = \delta_{ij}.$$

Une matrice carrée d'ordre  $n$  est orthogonale si, et seulement si :

$${}^t A A = I_n \iff {}^t A = A^{-1}.$$

- Lien avec les endomorphismes**

Soit  $\mathcal{B}$  une base orthonormale d'un espace euclidien  $E$  et  $A$  la matrice de  $f \in \mathcal{L}(E)$  dans  $\mathcal{B}$ . On a :

$$A \in O(n) \iff f \in O(E).$$

Le groupe  $O(n)$  pour le produit de matrices est isomorphe au groupe  $O(E)$  pour la composition des applications.

- Déterminant d'une matrice orthogonale**

Si  $A$  est une matrice orthogonale, on a  $\det A = \pm 1$ .

Attention, la condition est nécessaire mais non suffisante.

- Groupe spécial orthogonal**

On appelle groupe spécial orthogonal  $SO(E)$ , ou groupe des rotations de  $E$ , le sous-groupe de  $O(E)$  formé des automorphismes orthogonaux de déterminant égal à 1.

De même pour les matrices :  $SO(n) = \{A \in O(n) ; \det A = 1\}$ .

## III Cas de la dimension 2

- Rotations**

La rotation d'angle  $\theta$  appartient à  $SO(E)$ . Dans toute base  $\mathcal{B}$  orthonormale directe, sa matrice s'écrit :

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}.$$

On a  $\det A = 1$  et  $\operatorname{tr} A = 2 \cos \theta$ .

- **Réflexions**

La matrice de la réflexion d'axe  $\Delta$  dans une base  $\mathcal{B}$  est de la forme :

$$\begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}$$

mais elle dépend de  $\mathcal{B}$ . Dans une base adaptée, elle s'écrit :

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

$\Delta$  est l'ensemble des vecteurs invariants. On a  $\det B = -1$  et  $\operatorname{tr} B = 0$ .

## IV Cas de la dimension 3

Le classement se fait suivant la dimension de  $V = \operatorname{Ker}(f - \operatorname{Id}_E)$ , espace vectoriel des vecteurs invariants par  $f$ .

- Cas  $\dim V = 3$  : on a alors  $f = \operatorname{Id}_E$ .
- Cas  $\dim V = 2$  :  $f$  est alors la réflexion par rapport à  $V$ . Dans une base adaptée, sa matrice est :

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

- Cas  $\dim V = 1$  :  $f$  est alors une rotation d'axe  $V$ . Si on oriente l'axe et si on note son angle  $\theta$ , sa matrice dans une base adaptée directe, est :

$$\begin{pmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

### *Étude pratique d'une rotation*

Si  $r$  est la rotation d'axe dirigé par un vecteur unitaire  $\vec{n}$  et d'angle  $\theta$ , on a :

$$r(\vec{x}) = (\vec{n} \cdot \vec{x}) \vec{n} + \cos \theta [\vec{x} - (\vec{n} \cdot \vec{x}) \vec{n}] + \sin \theta \vec{n} \wedge \vec{x}.$$

Réciproquement, soit  $f$  un automorphisme orthogonal dont l'ensemble des vecteurs invariants est une droite de vecteur directeur unitaire  $\vec{n}$ .

C'est une rotation dont l'angle  $\theta$  vérifie  $\operatorname{tr} A = 1 + 2 \cos \theta$ .

## Application

Soit  $A = (a_{ij})$  une matrice orthogonale réelle d'ordre  $n$ . Montrez que

$$\left| \sum_{i,j} a_{ij} \right| \leq n.$$

## Solution

Notons  $C_1, \dots, C_n$  les matrices colonnes de  $A$ , que l'on peut considérer comme des vecteurs de  $\mathbb{R}^n$ . Leur somme  $C_1 + \dots + C_n$  est le vecteur de  $\mathbb{R}^n$  dont les composantes

sont  $\sum_{j=1}^n a_{ij}$ .

Pour obtenir  $\sum_{i,j} a_{ij}$ , il reste à considérer le vecteur  $U$  de  $\mathbb{R}^n$  dont toutes les composantes sont égales à 1, et le produit scalaire :

$$(C_1 + \dots + C_n) \cdot U = \sum_{i=1}^n \sum_{j=1}^n a_{ij}.$$

L'inégalité de Cauchy-Schwarz donne :

$$\left| \sum_{i,j} a_{ij} \right| \leq \left\| \sum_{j=1}^n C_j \right\| \|U\|.$$

On a  $\|U\| = \sqrt{n}$ . De plus, on a supposé  $A$  orthogonale c'est-à-dire que les vecteurs  $C_j$  sont deux à deux orthogonaux et unitaires, ce qui entraîne :

$$\left\| \sum_{j=1}^n C_j \right\|^2 = \sum_{j=1}^n \|C_j\|^2 = n \quad \text{soit} \quad \left\| \sum_{j=1}^n C_j \right\| = \sqrt{n}.$$

On obtient donc :

$$\left| \sum_{i,j} a_{ij} \right| \leq n.$$

## Application

Soit  $U = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{R})$  telle que  $\sum_{i=1}^n u_i^2 = 1$ .

Montrez que la matrice  $A = I_n - 2U^t U \in \mathcal{M}_n(\mathbb{R})$  est orthogonale. Identifiez l'automorphisme de  $\mathbb{R}^n$  qu'elle définit.

## Solution

Observons tout d'abord que  $A$  est symétrique puisque :

$${}^t A = I_n - 2 {}^t (U^t U) = I_n - 2 U^t U = A.$$

On a donc :

$${}^t A A = A^2 = (I_n - 2 U^t U) (I_n - 2 U^t U) = I_n - 4 U^t U + 4 (U^t U) (U^t U).$$

Le produit de matrices étant associatif, on a :

$$(U^t U) (U^t U) = U ({}^t U U) {}^t U = U {}^t U \quad \text{puisque} \quad {}^t U U = \sum_{i=1}^n u_i^2 = 1.$$

Par conséquent,  ${}^t A A = I_n$ , ce qui prouve que  $A$  est orthogonale.

$A$  symétrique et orthogonale est la matrice d'une symétrie orthogonale.

On a  $AU = U - 2U {}^t U U = U - 2U = -U$ .

D'autre part, si  $V$  est orthogonal à  $U$ , soit  ${}^t U V = 0$ , alors  $AV = V$ .

L'automorphisme de  $\mathbb{R}^n$  représenté par  $A$  dans la base canonique est donc la symétrie orthogonale par rapport à l'hyperplan orthogonal à  $U$ .

## Application

$E = \mathbb{R}^3$  étant rapporté à sa base canonique orthonormale, étudiez  $f \in \mathcal{L}(E)$  dont la matrice est :

$$M = \frac{1}{9} \begin{pmatrix} 8 & -1 & -4 \\ -1 & 8 & -4 \\ -4 & -4 & -7 \end{pmatrix}.$$

## Solution

Désignons par  $C_1$ ,  $C_2$  et  $C_3$  les vecteurs colonnes de  $M$ . On a :

$$\begin{cases} 0 = \langle C_1 | C_2 \rangle = \langle C_1 | C_3 \rangle = \langle C_2 | C_3 \rangle \\ 1 = \langle C_1 | C_1 \rangle = \langle C_2 | C_2 \rangle = \langle C_3 | C_3 \rangle \end{cases}$$

La matrice  $M$  est donc orthogonale et  $f$  est un automorphisme orthogonal de  $E$ .

Un vecteur  $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$  est invariant par  $f$  si, et seulement si :

$$\begin{cases} 8x - y - 4z = 9x \\ -x + 8y - 4z = 9y \\ -4x - 4y - 7z = 9z \end{cases} \iff x + y + 4z = 0.$$

L'ensemble des vecteurs invariants par  $f$  est le plan  $P$  d'équation

$$x + y + 4z = 0.$$

$f$  est donc la réflexion par rapport à  $P$ .

### Application

Dans l'espace vectoriel euclidien  $\mathbb{R}^3$  muni de sa base canonique, déterminez la matrice de la rotation d'angle  $\frac{\pi}{2}$  et d'axe dirigé par le vecteur  $(1, 1, 1)$ .

### Solution

Soit  $(\vec{e}_1, \vec{e}_2, \vec{e}_3)$  la base canonique de  $\mathbb{R}^3$  et  $\vec{w} = \frac{1}{\sqrt{3}}(1, 1, 1)$  un vecteur unitaire de l'axe de la rotation  $r$ .

On peut choisir un vecteur unitaire orthogonal à l'axe  $\vec{u} = \frac{1}{\sqrt{2}}(1, -1, 0)$ .

On aura alors  $r(\vec{u}) = \vec{v}$  avec  $\vec{v} = \vec{w} \wedge \vec{u} = \frac{1}{\sqrt{6}}(1, 1, -2)$ .

Comme  $\theta = \frac{\pi}{2}$ , on a pour tout vecteur  $\vec{x}$  de  $\mathbb{R}^3$

$$r(\vec{x}) = (\vec{w} \cdot \vec{x}) \vec{w} + \vec{w} \wedge \vec{x}.$$

En calculant  $r(\vec{e}_1)$ ,  $r(\vec{e}_2)$  et  $r(\vec{e}_3)$  dans la base canonique, on obtient les colonnes de la matrice cherchée, soit :

$$A = \frac{1}{3} \begin{pmatrix} 1 & 1 - \sqrt{3} & 1 + \sqrt{3} \\ 1 + \sqrt{3} & 1 & 1 - \sqrt{3} \\ 1 - \sqrt{3} & 1 + \sqrt{3} & 1 \end{pmatrix}.$$

## I Endomorphisme symétrique

### • Définition

Dans un espace euclidien  $E$ ,  $f \in \mathcal{L}(E)$  est symétrique si :

$$\forall x \in E \quad \forall y \in E \quad \langle f(x)|y \rangle = \langle x|f(y) \rangle.$$

### • Écriture matricielle

Si  $A$  est la matrice de  $f$  dans une base orthonormale  $\mathcal{B}$ , on a

$$f \text{ symétrique} \iff {}^t A = A.$$

## II Diagonalisation

### • Diagonalisation des endomorphismes symétriques

Soit  $f$  un endomorphisme symétrique de  $E$ .

- Le polynôme caractéristique de  $f$  est scindé sur  $\mathbb{R}$ .
- $f$  est diagonalisable dans une base orthonormale.
- $E$  est somme directe orthogonale des sous-espaces propres de  $f$ .

### • Diagonalisation des matrices symétriques réelles

Si  $A$  est une matrice carrée symétrique, il existe une matrice diagonale  $D$  et une matrice orthogonale  $P$  telles que :

$$A = PDP^{-1} = PD {}^t P.$$

Le calcul de  $P^{-1}$  est immédiat puisque  $P^{-1} = {}^t P$ .

### • Forme quadratique et valeurs propres

Soit  $A$  une matrice symétrique réelle et  $q$  la forme quadratique associée ;

$q$  est positive  $\iff$  les valeurs propres de  $A$  sont  $\geq 0$  ;

$q$  est définie positive  $\iff$  les valeurs propres de  $A$  sont  $> 0$ .

## Application

Démontrez que

$$A = \begin{pmatrix} 1-i & -7 & 4 & -5 \\ -7 & 2-i & 14 & 37 \\ 4 & 14 & 3-i & -21 \\ -5 & 37 & -21 & 4-i \end{pmatrix} \in \mathcal{M}_4(\mathbb{C})$$

est inversible.

## Solution

La matrice  $A$  s'écrit sous la forme  $A = M - iI_4$  où  $M$  est réelle et symétrique.

Comme le polynôme caractéristique de  $M$  est scindé sur  $\mathbb{R}$ , toutes les valeurs propres de  $M$  sont réelles.

$i$  n'est donc pas valeur propre de  $M$ , d'où  $\det(M - iI_4) \neq 0$  ; ou encore  $\det A \neq 0$ , ce qui démontre que  $A$  est inversible.

## Application

Soit  $A = (a_{ij})$  une matrice symétrique réelle d'ordre  $n$  dont les valeurs propres sont  $\lambda_1, \dots, \lambda_n$ . Montrez que :

$$\sum_{i,j} a_{ij}^2 = \sum_i \lambda_i^2.$$

## Solution

Pour une matrice carrée  $A$  quelconque on a  $\sum_{i,j} a_{ij}^2 = \text{tr}({}^t A A)$  (cf. fiche 22).

Comme  $A$  est symétrique, on a donc  $\sum_{i,j} a_{ij}^2 = \text{tr}(A^2)$ .

$A$  étant symétrique et réelle est semblable à une matrice diagonale

$$D = \text{diag}(\lambda_1, \dots, \lambda_n)$$

où les  $\lambda_i$  sont les valeurs propres de  $A$ . On a alors  $A^2$  semblable à  $D^2$  et, comme deux matrices semblables ont la même trace :

$$\sum_{i,j} a_{ij}^2 = \text{tr}(A^2) = \text{tr}(D^2) = \sum_{i=1}^n \lambda_i^2.$$

# Calcul vectoriel et distances

## I Calcul vectoriel

Soit  $(\vec{i}, \vec{j}, \vec{k})$  une base orthonormale de l'espace  $\mathbb{R}^3$  muni du produit scalaire canonique et  $\vec{u} = x\vec{i} + y\vec{j} + z\vec{k}$ ,  $\vec{v} = x'\vec{i} + y'\vec{j} + z'\vec{k}$  et  $\vec{w} = x''\vec{i} + y''\vec{j} + z''\vec{k}$  trois vecteurs. On sait calculer :

- le produit scalaire de deux vecteurs

$$\vec{u} \cdot \vec{v} = xx' + yy' + zz' ;$$

- le produit vectoriel de deux vecteurs

$$\vec{u} \wedge \vec{v} = (yz' - zy')\vec{i} + (zx' - xz')\vec{j} + (xy' - yx')\vec{k} ;$$

- le produit mixte de trois vecteurs

$$(\vec{u}, \vec{v}, \vec{w}) = \vec{u} \cdot (\vec{v} \wedge \vec{w}) = \det(\vec{u}, \vec{v}, \vec{w}) .$$

## II Distance d'un point à une droite ou à un plan

- Dans le plan

Soit  $\mathcal{D}$  la droite d'équation :  $ax + by + c = 0$ .

Le vecteur  $\vec{n}(a, b)$  est normal à  $\mathcal{D}$ .

La distance de  $M_0(x_0, y_0)$  à  $\mathcal{D}$  est :  $d(M_0, \mathcal{D}) = \frac{|ax_0 + by_0 + c|}{\sqrt{a^2 + b^2}}$ .

- Dans l'espace

Soit  $\mathcal{P}$  le plan d'équation :  $ax + by + cz + d = 0$ .

Le vecteur  $\vec{n}(a, b, c)$  est normal à  $\mathcal{P}$ . La distance de  $M_0(x_0, y_0, z_0)$  à  $\mathcal{P}$  est :

$$d(M_0, \mathcal{P}) = \frac{|ax_0 + by_0 + cz_0 + d|}{\sqrt{a^2 + b^2 + c^2}}.$$

La distance de  $M_0$  à la droite  $\mathcal{D}$  passant par  $A$  et de vecteur directeur  $\vec{u}$  est :

$$d(M_0, \mathcal{D}) = \frac{\|\overrightarrow{M_0A} \wedge \vec{u}\|}{\|\vec{u}\|}.$$

### III Distance entre deux droites

- Perpendiculaire commune**

Soit  $\mathcal{D}_1(A_1, \vec{u}_1)$  et  $\mathcal{D}_2(A_2, \vec{u}_2)$  deux droites non parallèles définies par un point et un vecteur directeur.

La perpendiculaire commune à  $\mathcal{D}_1$  et  $\mathcal{D}_2$  est l'unique droite  $\Delta$  qui rencontre  $\mathcal{D}_1$  et  $\mathcal{D}_2$  et qui est orthogonale à  $\mathcal{D}_1$  et  $\mathcal{D}_2$ .

Elle est définie par :

$$M \in \Delta \iff \begin{cases} \det(\overrightarrow{A_1M}, \vec{u}_1, \vec{u}_1 \wedge \vec{u}_2) = 0 \\ \det(\overrightarrow{A_2M}, \vec{u}_2, \vec{u}_1 \wedge \vec{u}_2) = 0. \end{cases}$$

- Distance entre deux droites**

$$d(\mathcal{D}_1, \mathcal{D}_2) = \frac{|\det(\overrightarrow{A_1A_2}, \vec{u}_1, \vec{u}_2)|}{\|\vec{u}_1 \wedge \vec{u}_2\|}.$$

## Application

Déterminez l'angle aigu entre les plans :

$P$  d'équation  $2x - y + z = 3$  et  $P'$  d'équation  $x + y + 2z = 7$ .

## Solution

Les plans  $P$  et  $P'$  ont pour vecteurs normaux respectifs  $\vec{n}(2, -1, 1)$  et  $\vec{n}'(1, 1, 2)$ . L'angle aigu  $\alpha$  entre les deux plans est aussi celui entre ces deux vecteurs. On a donc :

$$\cos \alpha = \frac{\vec{n} \cdot \vec{n}'}{\|\vec{n}\| \|\vec{n}'\|} = \frac{3}{\sqrt{6}\sqrt{6}} = \frac{1}{2} \quad \text{d'où} \quad \alpha = \frac{\pi}{3}.$$

## Application

Déterminez un système d'équations de la droite  $\Delta$  passant par  $A(1, -1, 2)$  et coupant les droites :

$$\mathcal{D}_1 \begin{cases} 2x - y + 3z - 1 = 0 \\ x + 2y + z + 2 = 0 \end{cases} \quad \text{et} \quad \mathcal{D}_2 \begin{cases} x - y + z + 3 = 0 \\ x + 2y + 5z + 1 = 0 \end{cases}$$

## Solution

Comme  $A \notin \mathcal{D}_1$ , le point  $A$  et la droite  $\mathcal{D}_1$  définissent un plan  $\mathcal{P}_1$ . De même, il existe un seul plan  $\mathcal{P}_2$  contenant  $A$  et  $\mathcal{D}_2$ .

La droite cherchée est l'intersection de  $\mathcal{P}_1$  et  $\mathcal{P}_2$ .

Considérons deux points de  $\mathcal{D}_1$ , par exemple  $B_1(0, -1, 0)$  et  $C_1(-7, 0, 5)$ .

Tout point  $M(x, y, z)$  de  $\mathcal{P}_1$  est tel que  $\overrightarrow{AM}$ ,  $\overrightarrow{AB_1}$  et  $\overrightarrow{AC_1}$  soient coplanaires, ce qui peut s'écrire :

$$0 = \det(\overrightarrow{AM}, \overrightarrow{AB_1}, \overrightarrow{AC_1}) = \begin{vmatrix} x-1 & -1 & -8 \\ y+1 & 0 & 1 \\ z-2 & -2 & 3 \end{vmatrix} = 2x + 19y - z + 19.$$

À partir des points  $B_2(0, 2, -1)$  et  $C_2(7, 6, -4)$  de  $\mathcal{D}_2$ , on obtient de même une équation de  $\mathcal{P}_2$  :

$$0 = \det(\overrightarrow{AM}, \overrightarrow{AB_2}, \overrightarrow{AC_2}) = \begin{vmatrix} x-1 & -1 & 6 \\ y+1 & 3 & 7 \\ z-2 & -3 & -6 \end{vmatrix} = 3x - 24y - 25z + 23.$$

$\Delta$  a donc pour équations :

$$\begin{cases} 2x + 19y - z + 19 = 0 \\ 3x - 24y - 25z + 23 = 0 \end{cases}$$

### Application

Déterminez l'équation de la perpendiculaire commune  $\Delta$  aux deux droites :

$$D \quad \begin{cases} x = 0 \\ 2y + z = 1 \end{cases} \quad \text{et} \quad D' \quad \begin{cases} x + y = 1 \\ x + z = 3 \end{cases}$$

### Solution

La droite  $D$  passe par le point  $A(0,0,1)$  et est dirigée par  $\vec{u}(0,1,-2)$ .

La droite  $D'$  passe par le point  $A'(0,1,3)$  et est dirigée par  $\vec{u'}(1,-1,-1)$ .

La perpendiculaire commune  $\Delta$  à  $D$  et à  $D'$  admet pour vecteur directeur :

$$\vec{u} \wedge \vec{u'} = (-3, -2, -1).$$

$\Delta$  est donc l'intersection des plans  $(A, \vec{u}, \vec{u} \wedge \vec{u'})$  et  $(A', \vec{u'}, \vec{u} \wedge \vec{u'})$  dont les équations s'obtiennent en écrivant que les produits mixtes  $(\vec{AM}, \vec{u}, \vec{u} \wedge \vec{u'})$  et  $(\vec{A'M}, \vec{u'}, \vec{u} \wedge \vec{u'})$  sont nuls, c'est-à-dire :

$$0 = \begin{vmatrix} x & 0 & -3 \\ y & 1 & -2 \\ z-1 & -2 & -1 \end{vmatrix} = -5x + 6y + 3z - 3$$

et

$$0 = \begin{vmatrix} x & 1 & -3 \\ y-1 & -1 & -2 \\ z+3 & -1 & -1 \end{vmatrix} = -x + 4y - 5z - 19.$$

L'équation de  $\Delta$  est donc :

$$\begin{cases} 5x - 6y - 3z + 3 = 0 \\ x - 4y + 5z + 19 = 0 \end{cases}$$

## I Définition par foyer et directrice

Soit  $F$  un point du plan affine euclidien,  $\mathcal{D}$  une droite ne passant pas par  $F$ ,  $e$  un réel strictement positif.

L'ensemble des points  $M$  tels que  $\frac{MF}{d(M, \mathcal{D})} = e$  est la conique de foyer  $F$ , de directrice  $\mathcal{D}$  et d'excentricité  $e$ .

C'est une ellipse si  $e < 1$ , une parabole si  $e = 1$ , une hyperbole si  $e > 1$ .

La perpendiculaire à  $\mathcal{D}$  passant par  $F$  est l'axe focal de la conique.

## II Parabole

La parabole  $\mathcal{P}$  et son axe focal ont un point commun unique, le sommet  $S$ .

Dans le repère orthonormal d'origine  $S$  et admettant l'axe focal comme axe des abscisses, l'équation de  $\mathcal{P}$  est :

$$y^2 = 2px$$

où  $p$  est le paramètre de la parabole.

$F$  a pour coordonnées  $\left(\frac{p}{2}, 0\right)$  ;  $\mathcal{D}$  a pour équation  $x = -\frac{p}{2}$ .

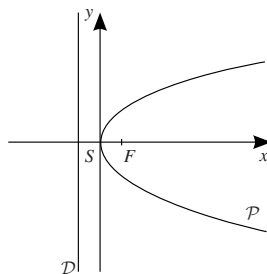


Figure 27.1

## III Ellipse

### • Équation réduite

L'ellipse  $\mathcal{E}$  et son axe focal ont deux points communs,  $A$  et  $A'$ , sommets de l'axe focal.

Le milieu  $O$  de  $[AA']$  est le centre de  $\mathcal{E}$ .

La médiatrice de  $[AA']$  est l'axe non focal.

Elle coupe l'ellipse en  $B$  et  $B'$ , sommets de l'axe non focal.

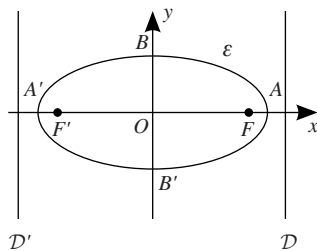


Figure 27.2

Si  $F'$  et  $D'$  sont les symétriques de  $F$  et  $D$  par rapport à  $O$ , l'ellipse de foyer  $F'$ , de directrice  $D'$  et d'excentricité  $e$  est la même ellipse.

On pose  $AA' = 2a$  et  $BB' = 2b$ . Dans le repère orthonormal d'origine  $O$  et admettant l'axe focal comme axe des abscisses et l'axe non focal comme axe des ordonnées, l'équation de  $\mathcal{E}$  est :

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

En posant  $c = \sqrt{a^2 - b^2}$  (possible car  $a \geq b$ ), on a  $FF' = 2c$ ,  $e = \frac{c}{a}$

et  $\mathcal{D}$  a pour équation  $x = \frac{a^2}{c}$ .

- Représentation paramétrique**

$$\begin{cases} x = a \cos \theta \\ y = b \sin \theta \end{cases} \quad \theta \in [0, 2\pi[.$$

- Définition bifocale**

Soit  $F$  et  $F'$  deux points distincts du plan et  $a$  un réel tel que  $FF' < 2a$ .

L'ensemble des points  $M$  du plan tels que  $MF + MF' = 2a$  est une ellipse de foyers  $F$  et  $F'$ .

## IV Hyperbole

- Équation réduite**

L'hyperbole  $\mathcal{H}$  et son axe focal ont deux points communs, les sommets  $A$  et  $A'$ .

Le milieu  $O$  de  $[AA']$  est le centre de  $\mathcal{H}$ .

La médiatrice de  $[AA']$  est l'axe non focal.

Il ne rencontre pas l'hyperbole.

Si  $F'$  et  $D'$  sont les symétriques de  $F$  et  $D$  par rapport à  $O$ , l'hyperbole de foyer  $F'$ , de directrice  $D'$  et d'excentricité  $e$  est la même hyperbole.

On pose  $AA' = 2a$ ,  $FF' = 2c$  et  $b^2 = c^2 - a^2$ .

Dans le repère orthonormal d'origine  $O$  et admettant l'axe focal comme axe des abscisses et l'axe non focal comme axe des ordonnées, l'équation de  $\mathcal{H}$  est :

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1.$$

On a  $e = \frac{c}{a}$  et  $\mathcal{D}$  a pour équation  $x = \frac{a^2}{c}$ .

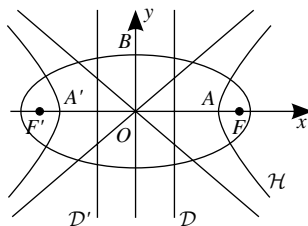


Figure 27.3

- **Équation des asymptotes**

$$y = \frac{b}{a}x \quad ; \quad y = -\frac{b}{a}x.$$

- **Représentation paramétrique**

$$\begin{cases} x = a \operatorname{ch} \theta \\ y = b \operatorname{sh} \theta \end{cases} \quad \theta \in \mathbb{R}.$$

- **Définition bifocale**

Soit  $F$  et  $F'$  deux points distincts du plan et  $a$  un réel tel que  $0 < 2a < FF'$ .

L'ensemble des points  $M$  du plan tels que  $|MF - MF'| = 2a$  est une hyperbole de foyers  $F$  et  $F'$ .

## V Courbes du second degré

Une conique (éventuellement vide ou dégénérée) est l'ensemble des points du plan vérifiant une équation de la forme :

$$\varphi(x, y) = ax^2 + 2bxy + cy^2 + dx + ey + f = 0.$$

- **Recherche des axes de la forme réduite**

La forme quadratique  $q(x, y) = ax^2 + 2bxy + cy^2$  a pour matrice associée

$M = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ . Elle est symétrique et réelle. Elle est donc diagonalisable dans une

base  $(\vec{T}, \vec{J})$  associée aux valeurs propres  $\lambda_1$  et  $\lambda_2$ .

- **Recherche du centre éventuel**

Si la résolution du système :

$$\vec{\operatorname{grad}} \varphi(x, y) = \vec{0} \quad \text{soit} \quad \begin{cases} 2ax + 2by + d = 0 \\ 2bx + 2cy + e = 0 \end{cases}$$

conduit à une solution unique (soit  $\det M \neq 0$ ), il s'agit du centre  $\Omega$  de la conique.

- **Forme réduite**

Si  $\Omega$  existe, dans le repère  $(\Omega; \vec{T}, \vec{J})$ , l'équation devient :

$$\lambda_1 X^2 + \lambda_2 Y^2 + k = 0$$

où  $k = \varphi(\Omega)$ .

## Application

On considère la conique d'équation :

$$2x^2 + 3y^2 - 4x + 18y + 11 = 0.$$

Déterminez sa nature et les éléments géométriques particuliers qui lui sont associés.

## Solution

L'équation de la conique peut s'écrire :

$$\begin{aligned} 2(x^2 - 2x) + 3(y^2 + 6y) + 11 = 0 &\iff 2(x - 1)^2 + 3(y + 3)^2 = 18 \\ &\iff \frac{(x - 1)^2}{9} + \frac{(y + 3)^2}{6} = 1 \end{aligned}$$

Il s'agit donc d'une ellipse de centre  $\Omega(1, -3)$ .

Comme  $9 > 6$ , l'axe focal est parallèle à  $(Ox)$ .

De  $a = 3$  et  $b = \sqrt{6}$ , on déduit les coordonnées des sommets

situés sur l'axe focal :  $(-2, -3)$  et  $(4, -3)$ ,

non situés sur l'axe focal :  $(1, -3 - \sqrt{6})$  et  $(1, -3 + \sqrt{6})$ .

Comme  $c = \sqrt{a^2 - b^2} = \sqrt{3}$ , les foyers ont pour coordonnées :  $(1 - \sqrt{3}, -3)$  et  $(1 + \sqrt{3}, -3)$ .

L'excentricité est  $e = \frac{c}{a} = \frac{\sqrt{3}}{3}$ .

Comme  $\frac{a^2}{c} = 3\sqrt{3}$ , les directrices ont pour équations :  $x = 1 - 3\sqrt{3}$  et  $x = 1 + 3\sqrt{3}$ .

## Application

On considère deux cercles  $\mathcal{C}(O, R)$  et  $\mathcal{C}'(O', R')$  avec  $R > R'$ , qui sont sécants en  $A$  et  $B$ . Montrez que les centres des cercles tangents à  $\mathcal{C}$  et  $\mathcal{C}'$  appartiennent à une hyperbole et à une ellipse à préciser.

## Solution

Considérons un cercle  $\omega$  de centre  $M$  et de rayon  $r$  qui soit tangent à  $\mathcal{C}$  et  $\mathcal{C}'$ . Quatre cas sont à envisager.

**1.  $\omega$  est tangent extérieurement à  $\mathcal{C}$  et  $\mathcal{C}'$**

On a alors  $\begin{cases} MO = R + r \\ MO' = R' + r \end{cases}$  d'où  $MO - MO' = R - R'$ .

## 2. $\omega$ est tangent intérieurement à $\mathcal{C}$ et $\mathcal{C}'$

On a alors  $\begin{cases} MO = R - r \\ MO' = R' - r \end{cases}$  d'où  $MO - MO' = R - R'$ .

Dans les cas 1 et 2,  $M$  appartient à une branche de l'hyperbole de foyers  $O$  et  $O'$  avec  $R - R' = 2a$ . Cette hyperbole passe par  $A$  et  $B$ .

Réciproquement, tout point de cet arc d'hyperbole convient en posant  $r = MO - R$  ou  $r = R - MO$ .

## 3. $\omega$ est tangent extérieurement à $\mathcal{C}$ et intérieurement à $\mathcal{C}'$

On a alors  $\begin{cases} MO = R + r \\ MO' = R' - r \end{cases}$  d'où  $MO + MO' = R + R'$ .

## 4. $\omega$ est tangent intérieurement à $\mathcal{C}$ et extérieurement à $\mathcal{C}'$

On a alors  $\begin{cases} MO = R - r \\ MO' = R' + r \end{cases}$  d'où  $MO + MO' = R + R'$ .

Dans les cas 3 et 4,  $M$  appartient à l'ellipse de foyers  $O$  et  $O'$  avec  $R + R' = 2a$ . Cette ellipse passe par  $A$  et  $B$ .

Réciproquement, tout point de cette ellipse convient en posant  $r = MO - R$  ou  $r = R - MO$ .

## Application

Étudiez la conique d'équation :  $x^2 + xy + y^2 - 4x - 5y + 2 = 0$ .

## Solution

Posons  $f(x, y) = x^2 + xy + y^2 - 4x - 5y + 2$ . Le système :

$$\overrightarrow{\text{grad}} f(x, y) = \overrightarrow{0} \iff \begin{cases} 2x + y - 4 = 0 \\ x + 2y - 5 = 0 \end{cases} \iff \begin{cases} x = 1 \\ y = 2 \end{cases}$$

a une solution unique. La conique a donc un centre  $\Omega(1, 2)$ .

La forme quadratique associée à  $f$  a pour matrice :  $M = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$ .

Ses valeurs propres sont  $\lambda_1 = \frac{1}{2}$  et  $\lambda_2 = \frac{3}{2}$ .

On peut prendre comme vecteurs propres associés  $\vec{V}_1(1, -1)$  et  $\vec{V}_2(1, 1)$ .

Dans le repère  $(\Omega, \vec{V}_1, \vec{V}_2)$ , l'équation de la courbe devient :

$$g(X, Y) = \frac{1}{2} X^2 + \frac{3}{2} Y^2 + k = 0.$$

On obtient  $k$  en écrivant la valeur de la fonction au point  $\Omega$  :

$$g(0, 0) = k = f(1, 2) = -5.$$

On obtient ainsi la forme réduite d'une ellipse :

$$\frac{X^2}{(\sqrt{10})^2} + \frac{Y^2}{\left(\frac{\sqrt{10}}{3}\right)^2} = 1.$$

## I Généralités

## • Courbe paramétrée

Soit  $\vec{F}$  une fonction vectorielle de classe  $C^k$  ( $k$  aussi grand que nécessaire) définie sur une partie non vide  $D$  de  $\mathbb{R}$  et à valeurs dans  $\mathbb{R}^2$  ou  $\mathbb{R}^3$ . L'ensemble  $\Gamma$  des points  $M$  tels que

$$\overrightarrow{OM} = \vec{F}(t) \quad t \in D$$

est une courbe paramétrée.

Si  $D$  est un intervalle, il s'agit d'un arc de courbe.

On dit que  $\vec{F}(t)$  est une représentation paramétrique de  $\Gamma$ , ou encore que  $\Gamma$  a pour équations paramétriques :

$$x = x(t) ; y = y(t) \quad t \in D.$$

Une même courbe  $\Gamma$  (ensemble de points) a plusieurs paramétrages.

## • Représentation propre

Pour construire  $\Gamma$ , on détermine d'abord un domaine de représentation propre, c'est-à-dire une partie  $D_1$  de  $D$  telle que la courbe géométrique  $\Gamma$  soit entièrement décrite, et une seule fois, lorsque  $t$  décrit  $D_1$ .

## • Domaine d'étude

Si  $x$  et  $y$  sont deux fonctions impaires,  $\Gamma$  est symétrique par rapport au point  $O$  et il suffit de faire l'étude sur  $D_1 \cap \mathbb{R}_+$ .

Si  $x$  est paire et  $y$  impaire,  $\Gamma$  est symétrique par rapport à l'axe des abscisses et il suffit de faire l'étude sur  $D_1 \cap \mathbb{R}_+$ .

Si  $x$  est impaire et  $y$  paire,  $\Gamma$  est symétrique par rapport à l'axe des ordonnées et il suffit de faire l'étude sur  $D_1 \cap \mathbb{R}_+$ .

## II Étude locale

Soit  $p$  le plus petit entier tel que  $\vec{F}^{(p)}(t_0) \neq \vec{0}$  et  $q$  ( $p < q$ ) l'ordre de la première dérivée telle que  $(\vec{F}^{(p)}(t_0), \vec{F}^{(q)}(t_0))$  forme une base du plan vectoriel.

$\vec{F}^{(p)}(t_0)$  est un vecteur directeur de la tangente en  $M(t_0)$  à  $\Gamma$ .

Si  $p \neq 1$ , le point  $M(t_0)$  est stationnaire (ou singulier). Si  $p = 1$ , c'est un point régulier. Si  $p = 1$  et  $q = 2$ , c'est un point birégulier.

Si  $p$  impair et  $q$  pair,  $M(t_0)$  est un point ordinaire (cf. fig. 28.1).

Si  $p$  impair et  $q$  impair,  $M(t_0)$  est un point d'inflexion (cf. fig. 28.2).

Si  $p$  pair et  $q$  impair,  $M(t_0)$  est un point de rebroussement de première espèce (cf. fig. 28.3).

Si  $p$  pair et  $q$  pair,  $M(t_0)$  est un point de rebroussement de deuxième espèce (cf. fig. 28.4).

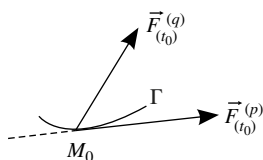


Figure 28.1

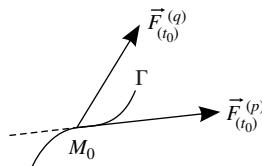


Figure 28.2

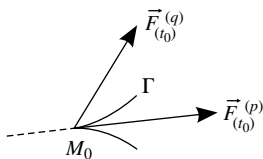


Figure 28.3

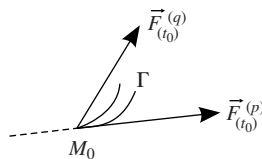


Figure 28.4

## III Branches infinies

La courbe  $\Gamma$  présente une branche infinie pour  $t$  tendant vers  $t_0$  ( $t_0$  fini ou non) si au moins une des coordonnées  $x(t)$  et  $y(t)$  de  $M$  tend vers l'infini lorsque  $t$  tend vers  $t_0$ .

- Si  $x(t) \rightarrow x_0 \in \mathbb{R}$  et  $y(t) \rightarrow \pm\infty$ , alors la droite  $x = x_0$  est asymptote à  $\Gamma$ .
- Si  $x(t) \rightarrow \pm\infty$  et  $y(t) \rightarrow y_0 \in \mathbb{R}$ , alors la droite  $y = y_0$  est asymptote à  $\Gamma$ .

- Si  $x(t) \rightarrow \pm\infty$  et  $y(t) \rightarrow \pm\infty$ , on cherche la limite éventuelle de  $\frac{y(t)}{x(t)}$  lorsque  $t$  tend vers  $t_0$ .
- Si  $\lim_{t \rightarrow t_0} \frac{y(t)}{x(t)} = 0$ ,  $\Gamma$  présente une branche parabolique de direction  $(Ox)$ .
- Si  $\lim_{t \rightarrow t_0} \frac{y(t)}{x(t)} = \pm\infty$ ,  $\Gamma$  présente une branche parabolique de direction  $(Oy)$ .
- Si  $\lim_{t \rightarrow t_0} \frac{y(t)}{x(t)} = a$ , limite finie non nulle, on étudie  $y(t) - ax(t)$ .
  - \* Si  $\lim_{t \rightarrow t_0} [y(t) - ax(t)] = \pm\infty$ ,  $\Gamma$  présente une branche parabolique de coefficient directeur  $a$ .
  - \* Si  $\lim_{t \rightarrow t_0} [y(t) - ax(t)] = b$ , la droite  $y = ax + b$  est asymptote à  $\Gamma$  et la position de la courbe par rapport à l'asymptote est donnée par le signe de  $y(t) - ax(t) - b$ .

## IV Points multiples

$A$  est un point multiple de  $\Gamma$  s'il existe au moins deux valeurs  $t_1 \neq t_2$  de  $D_1$  telles que  $M(t_1) = M(t_2) = A$ . On le détermine en résolvant :

$$x(t_1) = x(t_2) ; y(t_1) = y(t_2) ; t_1 \neq t_2 .$$

## Application

Soit  $\Gamma$  l'arc paramétré :

$$x(t) = \frac{t^2 + 2t^3}{1-t} \quad ; \quad y(t) = \frac{t^3}{1-t} \quad ; \quad t \in \mathbb{R} \setminus \{1\}$$

Étudiez :

1. les variations de  $x(t)$  et de  $y(t)$  ;
2. les points singuliers de  $\Gamma$  ;
3. les branches infinies de  $\Gamma$ .
4. Construisez la courbe représentative de  $\Gamma$ .

## Solution

### 1. Variations de $x$ et de $y$

Les fonctions  $x$  et  $y$  sont définies et indéfiniment dérivables sur  $\mathbb{R} \setminus \{1\}$ .

$x'(t) = \frac{-4t^3 + 5t^2 + 2t}{(1-t)^2}$  est du signe de  $t(-4t^2 + 5t + 2)$  et le trinôme

$-4t^2 + 5t + 2$  a pour racines  $t_1 = \frac{5 - \sqrt{57}}{8} \approx -0,32$  et  $t_2 = \frac{5 + \sqrt{57}}{8} \approx 1,57$

$y'(t) = \frac{-2t^3 + 3t^2}{(1-t)^2}$  est du signe de  $3 - 2t$ .

On en déduit le tableau de variation :

| $t$     | $-\infty$ | $t_1$      | 0          | 1          | 1,5       | $t_2$     | $+\infty$ |
|---------|-----------|------------|------------|------------|-----------|-----------|-----------|
| $x'(t)$ | +         | 0          | -          | 0          | +         | 0         | -         |
| $x(t)$  | $-\infty$ | $\nearrow$ | $\searrow$ | $\nearrow$ | $+\infty$ | $-\infty$ | $-\infty$ |
| $y'(t)$ | +         | +          | 0          | +          | +         | 0         | -         |
| $y(t)$  | $-\infty$ | $\nearrow$ | $\nearrow$ | $\nearrow$ | $+\infty$ | $-\infty$ | $-\infty$ |

Figure 28.5

## 2. Points singuliers

$\Gamma$  présente un point singulier pour  $t = 0$  car  $x'(0) = y'(0) = 0$ . Il s'agit du point  $O$ . On peut déterminer la nature de ce point singulier à l'aide de développements limités de  $x(t)$  et de  $y(t)$  au voisinage de  $t = 0$  :

$$x(t) = t^2 + 3t^3 + o(t^3), \quad y(t) = t^3 + o(t^3).$$

Donc  $\overrightarrow{OM} = t^2 \overrightarrow{i} + t^3(3 \overrightarrow{i} + \overrightarrow{j}) + t^3 \overrightarrow{\varepsilon}(t)$  avec  $\lim_{t \rightarrow 0} \overrightarrow{\varepsilon}(t) = \overrightarrow{0}$ .

Par identification avec la formule de Taylor-Young, on en déduit :

$$\overrightarrow{F}''(0) = 2 \overrightarrow{i}, \quad \overrightarrow{F}^{(3)}(0) = 6(3 \overrightarrow{i} + \overrightarrow{j}).$$

La courbe  $\Gamma$  admet donc au point  $O$  une tangente dirigée par  $\overrightarrow{i}$ . Et il s'agit d'un point de rebroussement de première espèce car  $p = 2$  et  $q = 3$ .

## 3. Branches infinies

- $\lim_{t \rightarrow \pm\infty} \frac{y(t)}{x(t)} = 0,5$  ;  $\lim_{t \rightarrow \pm\infty} [y(t) - 0,5x(t)] = \pm\infty$

Donc, lorsque  $t$  tend vers  $-\infty$  ou  $+\infty$ , la courbe  $\Gamma$  a une direction asymptotique de coefficient directeur 0,5, mais n'a pas d'asymptote.

- $\lim_{t \rightarrow 1} \frac{y(t)}{x(t)} = \frac{1}{3}$  ;  $\lim_{t \rightarrow 1} [y(t) - \frac{1}{3}x(t)] = -\frac{1}{3}$ .

Lorsque  $t$  tend vers 1, la courbe  $\Gamma$  admet donc pour asymptote la droite d'équation  $y = \frac{1}{3}x - \frac{1}{3}$ .

## 4. Courbe représentative

Pour voir l'allure locale de la courbe au voisinage du point singulier, il faut faire un zoom.

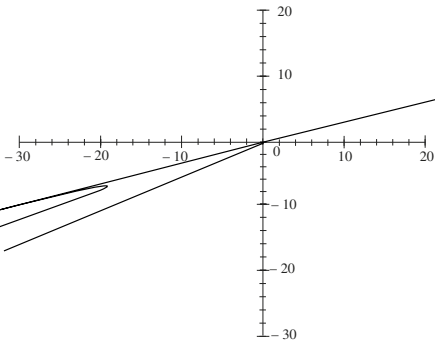


Figure 28.6

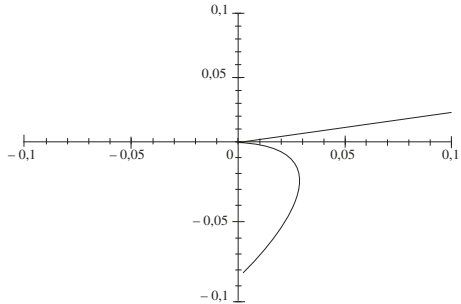


Figure 28.7

## Application

Dans le plan euclidien rapporté à un repère orthonormal, on considère la courbe paramétrée  $\mathcal{C}$  :

$$\begin{cases} x(t) = 3t^2 \\ y(t) = 2t^3 \end{cases} \quad t \in \mathbb{R}$$

Déterminez les droites qui sont à la fois tangentes et normales à  $\mathcal{C}$ .

## Solution

Comme  $x'(t) = 6t$  et  $y'(t) = 6t^2$ , tout point de  $\mathcal{C}$  tel que  $t \neq 0$  est régulier et la tangente en  $M(t)$

a pour vecteur directeur  $\begin{pmatrix} 1 \\ t \end{pmatrix}$ .

La tangente  $D_t$  en  $M(t)$  admet donc pour équation :

$$tx - y - t^3 = 0.$$

Si  $D_t$  recoupe  $\mathcal{C}$  en  $N(u)$ , le paramètre  $u$  vérifie l'équation :

$$3tu^2 - 2u^3 - t^3 = 0.$$

Le polynôme en  $u$  du premier membre est de degré 3 et il admet  $t$  comme racine double puisque la droite est tangente en  $M(t)$ .

On peut donc le factoriser et l'équation précédente s'écrit :

$$(u - t)^2(2u + t) = 0.$$

La droite  $D_t$  recoupe donc  $\mathcal{C}$  en  $N\left(-\frac{t}{2}\right)$ . Elle est normale à  $\mathcal{C}$  en ce point si, et seulement si, les vecteurs  $\begin{pmatrix} 1 \\ t \end{pmatrix}$  et  $\begin{pmatrix} 1 \\ -\frac{t}{2} \end{pmatrix}$

sont orthogonaux, donc si  $t^2 = 2$ .

Les droites qui sont à la fois normales et tangentes à  $\mathcal{C}$  admettent donc pour équations :

$$y = \sqrt{2}(x - 2) ; y = -\sqrt{2}(x - 2).$$

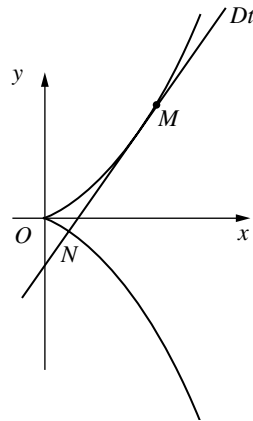


Figure 28.8

# Courbes en coordonnées polaires

## I Généralités

### • Représentation polaire

Soit  $(O, \vec{e}_1, \vec{e}_2)$  un repère orthonormal du plan. À tout point  $M$ , distinct de  $O$ , on peut associer des coordonnées polaires  $(\rho, \theta)$  telles que  $\overrightarrow{OM} = \rho \vec{u}$ .

$(O, \vec{u}, \vec{v})$  est le repère polaire orthormal lié à  $M$  et défini par :

$$(\vec{e}_1, \vec{u}) = \theta \quad ; \quad (\vec{u}, \vec{v}) = \frac{\pi}{2}.$$

Il n'y a pas unicité des coordonnées polaires d'un point. Si  $k \in \mathbb{Z}$ , alors  $(\rho, \theta + 2k\pi)$  et  $(-\rho, \theta + \pi + 2k\pi)$  repèrent le même point  $M$ .

Le point  $O$  est repéré par  $\rho = 0$  et  $\theta$  quelconque.

Une courbe en coordonnées polaires est l'ensemble des points  $M$  du plan dont les coordonnées polaires sont liées par une relation du type  $\rho = f(\theta)$  où  $f$  est une fonction de  $\mathbb{R}$  dans  $\mathbb{R}$  dérivable autant de fois qu'il sera nécessaire.

### • Domaine d'étude

Soit  $\Gamma$  la courbe d'équation polaire  $\rho = f(\theta)$  et  $D$  l'ensemble de définition de  $f$ . On détermine d'abord un domaine de représentation propre, c'est-à-dire une partie  $D_1$  de  $D$  telle que la courbe géométrique  $\Gamma$  soit entièrement décrite, une fois et une seule, lorsque  $\theta$  décrit  $D_1$ .

Si  $f$  est paire,  $\Gamma$  est symétrique par rapport à l'axe des abscisses et il suffit de faire l'étude sur  $D_1 \cap \mathbb{R}_+$ .

Si  $f$  est impaire,  $\Gamma$  est symétrique par rapport à l'axe des ordonnées et il suffit de faire l'étude sur  $D_1 \cap \mathbb{R}_+$ .

## II Étude locale

### • Tangente en un point

En  $M(\theta) \neq O$ ,  $\Gamma$  admet une tangente dirigée par le vecteur

$$\vec{T} = \rho'(\theta) \vec{u} + \rho(\theta) \vec{v}.$$

En  $M(\theta_0) = O$ ,  $\Gamma$  admet une tangente d'angle polaire  $\theta_0$ .

### • Points d'inflexion

Les points d'inflexion de  $\Gamma$  correspondent aux valeurs de  $\theta$  pour lesquelles l'une des deux expressions suivantes s'annule en changeant de signe, avec  $\rho \neq 0$  :

$$\rho^2 + 2\rho'^2 - \rho\rho'' \quad ; \quad \frac{1}{\rho} + \left(\frac{1}{\rho}\right)''.$$

## III Branches infinies

- Si  $\theta \rightarrow \pm\infty$  et  $\rho = f(\theta) \rightarrow \pm\infty$ , la courbe  $\Gamma$  présente une spirale.
- Si  $\theta \rightarrow \pm\infty$  et  $\rho = f(\theta) \rightarrow a$  (avec  $a \in \mathbb{R}$ ), alors le cercle de centre  $O$  et de rayon  $|a|$  est asymptote à la courbe  $\Gamma$ .
- Si  $\theta \rightarrow \theta_0$  et  $\rho = f(\theta) \rightarrow \pm\infty$ , alors l'axe  $OX$  d'angle  $\theta_0$  est une direction asymptotique de  $\Gamma$ .

Dans le repère orthonormal direct  $(OX, OY)$ , l'ordonnée de  $M$  s'écrit  $Y = \rho(\theta) \sin(\theta - \theta_0)$  et on étudie sa limite lorsque  $\theta$  tend vers  $\theta_0$ .

- Si  $\lim_{\theta \rightarrow \theta_0} \rho(\theta) \sin(\theta - \theta_0) = l$  (limite finie), alors  $\Gamma$  admet pour asymptote la droite  $Y = l$ .

Attention en traçant la droite  $Y = l$  à bien utiliser le nouveau repère  $(OX, OY)$ .

- Si  $\lim_{\theta \rightarrow \theta_0} \rho(\theta) \sin(\theta - \theta_0) = \pm\infty$ , alors la droite d'équation polaire  $\theta = \theta_0$  est une branche parabolique de  $\Gamma$ .

## Application

Étudiez et construisez la courbe  $\mathcal{C}$  définie en coordonnées polaires par :

$$\rho = \frac{\theta}{\theta - \frac{\pi}{4}}.$$

Étudiez en particulier les branches infinies et les points doubles.

## Solution

- Pour obtenir la courbe,  $\theta$  doit décrire  $\mathbb{R} \setminus \{\frac{\pi}{4}\}$ .

Comme  $\rho'(\theta) = \frac{-\frac{\pi}{4}}{\left(\theta - \frac{\pi}{4}\right)^2} < 0$ , on a le tableau de variations :

| $\theta$        | $-\infty$ | $\frac{\pi}{4}$ | $+\infty$ |
|-----------------|-----------|-----------------|-----------|
| $\rho'(\theta)$ | -         |                 | -         |
| $\rho(\theta)$  | 1         | $+\infty$       | 1         |

Figure 29.1

- Pour étudier la branche infinie au voisinage de  $\frac{\pi}{4}$  posons  $h = \theta - \frac{\pi}{4}$ .

$$\rho \sin h = \frac{h + \frac{\pi}{4}}{h} \sin h = \frac{\pi}{4} + h + o(h).$$

La courbe  $\mathcal{C}$  admet donc pour asymptote la droite d'équation  $Y = \frac{\pi}{4}$  dans le repère  $(O, \overrightarrow{Ox}, \overrightarrow{OY})$  tel que  $(\overrightarrow{Ox}, \overrightarrow{OX}) = \frac{\pi}{4}$  et  $(\overrightarrow{OX}, \overrightarrow{OY}) = \frac{\pi}{2}$ .

- Lorsque  $\theta$  tend vers  $\pm\infty$ , comme  $\lim_{\theta \rightarrow -\infty} \rho(\theta) = 1^-$  et  $\lim_{\theta \rightarrow +\infty} \rho(\theta) = 1^+$ , la courbe  $\mathcal{C}$  admet pour cercle asymptote le cercle de centre  $O$  et de rayon 1.
- Les points doubles peuvent s'obtenir à partir des deux égalités :  
 $\rho(\theta + 2k\pi) = \rho(\theta)$  avec  $k \in \mathbb{Z}^*$ , ce qui est impossible ici ;

$$\rho(\theta + (2k + 1)\pi) = -\rho(\theta) \text{ avec } k \in \mathbb{Z}$$

$$\Leftrightarrow 2\theta^2 + 2\left(2k + \frac{3}{4}\right)\pi\theta - \frac{\pi}{4}(2k + 1)\pi = 0$$

$$\Leftrightarrow \theta = \left(-2k - \frac{3}{4} \pm \sqrt{4k^2 + 4k + \frac{17}{16}}\right)\frac{\pi}{2}$$

• Graphique :

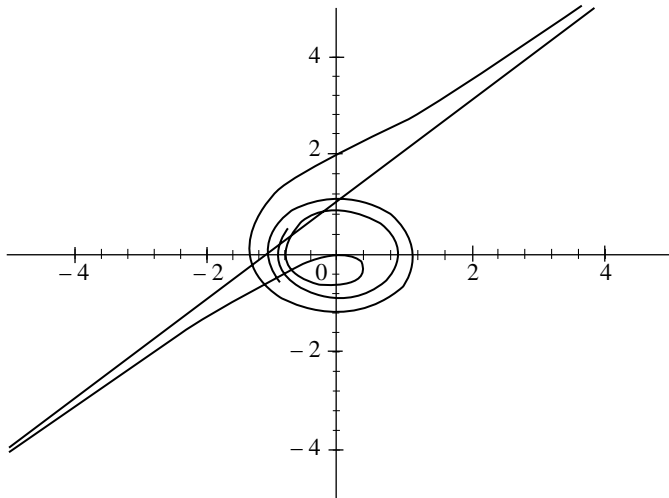


Figure 29.2

## I Longueur d'un arc de courbe

Soit  $\Gamma$  un arc de courbe de classe  $\mathcal{C}^2$  admettant une représentation paramétrique  $M(t) = (x(t), y(t), z(t))$ , avec  $t \in [a, b]$ , dans un repère orthormal  $(O, \vec{i}, \vec{j}, \vec{k})$  de l'espace.

En un point régulier,  $\vec{T} = \frac{\overrightarrow{OM'}(t)}{\|\overrightarrow{OM'}(t)\|}$  est un vecteur unitaire qui dirige la tangente en  $M$  à  $\Gamma$ .

L'arc est orienté par le choix de l'un des deux sens de parcours possibles, ce qui revient à distinguer les vecteurs unitaires tangents (opposés)  $\vec{T}_+$  et  $\vec{T}_-$ .

L'abscisse curviligne  $s$  est un paramétrage de  $\Gamma$  tel que  $\frac{d\overrightarrow{OM}}{ds}$  soit unitaire.

La longueur de  $\Gamma$  est :

$$L = \int_a^b \sqrt{x'^2(t) + y'^2(t) + z'^2(t)} dt.$$

Elle est indépendante du paramétrage choisi.

On note souvent  $ds = \sqrt{x'^2(t) + y'^2(t) + z'^2(t)} dt$  où  $s$  est l'abscisse curviligne.

## II Courbure d'une courbe plane

### • Repère de Frenet

Soit  $\vec{N}$  tel que  $(M, \vec{T}, \vec{N})$  soit orthonormal direct. Ce repère est appelé repère de Frenet au point  $M$ .

- **Formules de Frenet**

En un point birégulier, on a :

$$\frac{d\vec{T}}{ds} = \gamma \vec{N} ; \quad \frac{d\vec{N}}{ds} = -\gamma \vec{T}$$

où  $\gamma$  est la courbure de  $\Gamma$  au point  $M$ .

- **Repérage angulaire**

Si  $\alpha$  est l'angle  $(\vec{i}, \vec{T})$ , on a  $\gamma = \frac{d\alpha}{ds}$ .

- **Rayon de courbure**

En un point birégulier  $M$ , la courbure est non nulle et  $R = \frac{1}{\gamma}$  s'appelle rayon de courbure de  $\Gamma$  en  $M$ . On a :

en coordonnées paramétriques : 
$$R = \frac{(x'^2 + y'^2)^{\frac{3}{2}}}{x'y'' - y'x''}$$

en coordonnées polaires : 
$$R = \frac{(\rho^2 + \rho'^2)^{\frac{3}{2}}}{\rho^2 + 2\rho'^2 - \rho\rho''}$$

En un point birégulier, ces dénominateurs sont non nuls.

Le centre de courbure en  $M$  est le point  $I$  défini par  $\vec{MI} = R\vec{N}$ .

## Application

1. Calculez la longueur de l'arche de cycloïde :

$$\begin{cases} x = t - \sin t \\ y = 1 - \cos t \end{cases} \quad 0 \leq t \leq 2\pi$$

2. Pour un point  $M$  de la courbe, déterminez le repère de Frenet, le rayon de courbure et le centre de courbure.

## Solution

1. De  $x'(t) = 1 - \cos t$  et  $y'(t) = \sin t$ , on déduit :

$$x'^2(t) + y'^2(t) = 2(1 - \cos t) = 4 \sin^2 \frac{t}{2}.$$

Pour  $t \in [0, 2\pi]$ , on a  $\frac{t}{2} \in [0, \pi]$ , d'où  $\sin \frac{t}{2} \geq 0$ . La longueur cherchée est donc :

$$L = \int_0^{2\pi} 2 \sin \frac{t}{2} dt = \left[ -4 \cos \frac{t}{2} \right]_0^{2\pi} = 8.$$

L'arc étudié a pour allure :

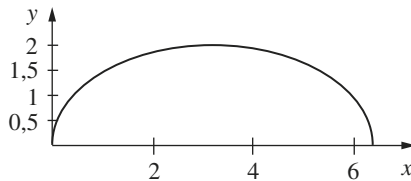


Figure 30.1

2. Pour  $t \in ]0, 2\pi[$ , la tangente en  $M(t)$  est dirigée par le vecteur

$$x' \vec{i} + y' \vec{j} = 2 \sin \frac{t}{2} \left[ \sin \frac{t}{2} \vec{i} + \cos \frac{t}{2} \vec{j} \right]$$

On a donc  $\frac{ds}{dt} = 2 \sin \frac{t}{2}$  et, le repère de Frenet étant orthonormal direct :

$$\vec{T} = \sin \frac{t}{2} \vec{i} + \cos \frac{t}{2} \vec{j} \quad ; \quad \vec{N} = -\cos \frac{t}{2} \vec{i} + \sin \frac{t}{2} \vec{j}$$

et l'angle polaire de la tangente est :

$$\alpha = (\vec{i}, \vec{T}) = \frac{\pi}{2} - \frac{t}{2}.$$

Dans ce cas, le rayon de courbure en  $M(t)$  se calcule facilement :

$$R = \frac{ds}{d\alpha} = \frac{ds}{dt} \frac{dt}{d\alpha} = -4 \sin \frac{t}{2}.$$

Le centre de courbure en  $M$  est le point  $I$  défini par  $\overrightarrow{MI} = R \vec{N}$ .

Il a donc pour coordonnées dans le repère  $(O, \vec{i}, \vec{j})$  :

$$\begin{cases} x = t - \sin t + 4 \sin \frac{t}{2} \cos \frac{t}{2} = t + \sin t \\ y = 1 - \cos t - 4 \sin \frac{t}{2} \sin \frac{t}{2} = -1 + \cos t \end{cases}$$

L'ensemble des centres de courbure s'appelle la développée de la courbe  $\mathcal{C}$ . Ici on obtient une autre cycloïde (deux demi-arches).

## Application

La courbe d'équation polaire  $\rho = \cos^3\left(\frac{\theta}{3}\right)$  a l'allure qui suit. On obtient toute la courbe avec  $\theta \in [0, 3\pi]$ . Calculez la longueur de la courbe.

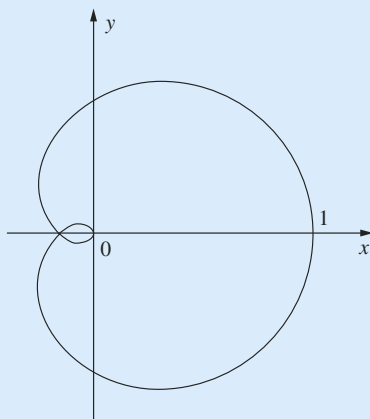


Figure 30.2

## Solution

Avec le repère mobile associé aux coordonnées polaires, on a :

$$\overrightarrow{OM} = \cos^3\left(\frac{\theta}{3}\right) \vec{u}(\theta).$$

La dérivation par rapport au paramètre  $\theta$  donne :

$$\frac{d\overrightarrow{OM}}{d\theta} = -\cos^2\left(\frac{\theta}{3}\right) \sin\left(\frac{\theta}{3}\right) \vec{u}(\theta) + \cos^3\left(\frac{\theta}{3}\right) \vec{v}(\theta)$$

d'où :

$$\left\| \frac{d\overrightarrow{OM}}{d\theta} \right\| = \cos^2\left(\frac{\theta}{3}\right) = \frac{ds}{d\theta}$$

puis :

$$L = \int_0^{3\pi} \cos^2\left(\frac{\theta}{3}\right) d\theta = \int_0^{3\pi} \frac{1}{2} \left[ 1 + \cos\left(\frac{2\theta}{3}\right) \right] d\theta = \frac{3\pi}{2}.$$

On peut aussi obtenir ce résultat en partant de  $ds = \sqrt{\rho'^2 + \rho^2} d\theta$

# Index

## A

absurde, 8  
algorithme d'Euclide, 37  
anneau intègre, 33  
anneaux, 32  
antisymétrique, 20  
application linéaire, 78  
applications, 16  
argument, 43  
associative, 26

## B

bases, 72  
bijections, 16  
borne  
inférieure, 21  
supérieure 21

## C

Cauchy-Schwarz, 116  
cofacteur, 104  
commutative, 26  
complémentaire, 12  
congruences, 38  
conjugué, 42  
connecteurs logiques, 6  
corps, 33  
courbe en coordonnées  
polaires, 150  
courbe paramétrée, 144  
courbure, 154  
cycle, 28

## D

déduction, 8  
déterminants, 102  
diagonalisation, 109  
différence, 12

différence symétrique, 12  
directrice, 138  
disjonction des cas, 8  
distance, 122, 134  
distributive, 26  
diviseurs de zéro, 33  
divisibilité, 36, 53  
division euclidienne, 36, 53

## E

élément(s)  
neutre, 26  
simples, 58  
ellipse, 138  
endomorphisme(s)  
symétrique, 132  
orthogonaux, 126  
ensembles, 12  
finis, 24  
équivalentes, 97  
espace(s)  
vectoriel, 66  
euclidiens, 116  
préhilbertiens réels, 115  
Euler, 43  
excentricité, 138  
exponentielle complexe, 43

## F

famille  
liée, 72  
libre, 72  
forme  
algébrique, 42  
bilinéaire symétrique,  
114  
linéaire, 80  
quadratique, 114  
trigonométrique, 42  
formule du binôme, 32

de Newton, 91  
foyer, 138

## G

groupe(s) orthogonal, 26,  
126  
spécial orthogonal, 127  
symétrique, 28

## H

homothéties, 86  
hyperbole, 139  
hyperplan, 80

## I

image, 27, 78  
directe, 17  
réciproque, 17  
injections, 16  
intersection, 12  
invertible, 26

## L

logique binaire, 6  
longueur, 154

## M

majorant, 21  
matrice(s) de passage, 90,  
97  
invertibles, 91  
orthogonales, 127  
méthode  
d'orthogonalisation de  
Schmidt, 121  
du pivot de Gauss, 63  
mineur, 104

minorée, 21  
module, 42  
Moivre (formule de), 43  
morphismes  
  d'anneaux, 33  
morphismes de groupes, 27

## N

nombres premiers, 36  
norme euclidienne, 116  
noyau, 27, 78

## O

ordre, 21  
ordre  
  partiel, 21  
  total, 21  
orientation, 116

## P

parabole, 138  
partie entière, 58  
partie fractionnaire, 58  
partie polaire, 58  
partition, 12  
permutations, 28  
perpendiculaire commune, 135  
pgcd, 36  
plus grand élément, 21  
plus petit élément, 21  
polynôme(s), 52  
  caractéristique, 108  
  irréductible, 54  
  scindé, 54  
  annulateurs, 110

ppcm, 37  
produit  
  cartésien, 13  
  mixte, 134  
  scalaire, 115, 134  
  vectoriel, 134  
projecteurs, 87  
prolongement, 16  
proposition logique, 6  
Pythagore, 120

## Q, R

quantificateurs 7  
racines, 53  
   $n$ -ièmes 44  
rang, 74  
  d'un système, 63  
  d'une matrice, 98  
recouvrement, 12  
récurrence, 8, 24  
réflexions, 128  
réflexive, 20  
relations d'équivalence, 20  
relations d'ordre, 21  
repère de Frenet, 154  
restriction, 16  
réunion, 12  
rotations, 127

## S

semblables, 97  
signature d'une permutation, 28  
similitude directe, 48  
somme directe, 68  
sous-anneau, 32

sous-corps, 33  
sous-espaces  
  vectoriels orthogonaux, 120  
  vectoriels 67  
sous-groupes, 27  
spectre, 108  
supplémentaire(s)  
  orthogonal, 68, 121  
surjections, 16  
symbole de Kronecker, 81  
symétrique, 20  
  vectorielles, 87  
systèmes  
  en escalier, 62  
  linéaires, 62

## T

Théorème  
  d'Alembert-Gauss, 54  
  de Bézout, 37  
  de Cayley-Hamilton, 110  
  de Gauss, 37  
  du rang, 80  
trace, 98  
transitive, 20  
translation, 48  
transposition 28, 92

## V

valeur propre, 108  
vecteur(s)  
  propre, 108  
  orthogonaux, 120



**Daniel FREDON**  
**Myriam MAUMY-BERTRAND**  
**Frédéric BERTRAND**

## Mathématiques

### Algèbre et géométrie en 30 fiches

#### Des principes aux applications

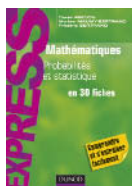
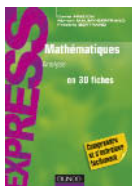
Comment aller à l'essentiel, comprendre les méthodes et les démarches avant de les mettre en application ?

Conçue pour faciliter aussi bien l'apprentissage que la révision, la collection « **EXPRESS** » vous propose une présentation simple et concise en **30 fiches pédagogiques** des notions d'algèbre et géométrie.

Chaque fiche comporte :

- les **idées** clés à connaître,
- la **méthode** à mettre en œuvre,
- des **applications** sous forme d'exercices corrigés.

#### Des mêmes auteurs :



#### Daniel Fredon

Ancien maître de conférences à l'université de Limoges.

#### Myriam Maumy-Bertrand

Maître de conférences à l'université Louis Pasteur de Strasbourg.

#### Frédéric Bertrand

Maître de conférences à l'université Louis Pasteur de Strasbourg.

#### L1/ L2

**Mathématiques,  
Informatique,  
Sciences physiques,  
Cycles  
préparatoires  
intégrés**