Bouchaïb Radi
Abdelkhalak El Hami

MP
MP*

# Maths

## Cours, exercices et problèmes de synthèse corrigés

NOUVEAUX PROGRAMMES



ellipses

Références sciences

# Maths
## MP-MP*

Cours, exercices et problèmes de synthèse corrigés




Bouchaïb Radi
Abdelkhalak El Hami

ellipses

Collection Références sciences

dirigée par Paul de Laboulaye
paul.delaboulaye@editions-ellipses.fr

*Retrouvez tous les livres de la collection et des extraits sur www.editions-ellipses.fr*

ISBN 9782340-073869
©Ellipses Édition Marketing S.A., 2022
8/10 rue la Quintinie 75015 Paris

DANGER LE PHOTOCOPILLAGE TUE LE LIVRE

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5.2° et 3°a), 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 une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

www.editions-ellipses.fr

# Avant-propos

Cet ouvrage satisfait le plus exactement possible aux exigences de la refonte des programmes de mathématiques des classes préparatoires MP et MP* 2ème année et il progresse au rythme de ce programme officiel (mai 2021).

Ce nouveau cours de mathématiques est organisé en douze chapitres qui développent successivement les différents thèmes de ce programme depuis les structures algébriques usuelles et réductions des endomorphismes et des matrices carrées jusqu'aux équations différentielles linéaires, calcul différentiel et optimisation. Le dernier chapitre est dédié aux problèmes de synthèse et de concours d'entrée aux grandes écoles.

Chaque chapitre est divisé en trois parties :

- La première partie est un rappel des définitions et des principaux résultats du cours (propositions et théorèmes sans démonstration) s'appuyant sur des exemples variés choisis avec soin.
- La deuxième partie est un ensemble d'exercices d'application choisis pour faciliter la compréhension et l'assimilation des notions traitées.
- La troisième partie est un ensemble de problèmes englobant les différents sujets abordés.

Plus de 300 exercices et problèmes de synthèse complètement résolus sont proposés. Ils sont de trois types :

- des exercices d'application directe du cours ;
- des exercices pour permettre d'en approfondir la compréhension ;
- des problèmes de synthèse et des problèmes de concours d'entrée aux grandes écoles.

Tous les exercices sont corrigés, le plus souvent en détail, ce qui permettra aux étudiants de ne pas « dépasser » sur un exercice difficile. On les invite cependant à chercher par eux-mêmes avant de regarder les solutions pour ne pas se priver du plaisir de les résoudre.

Pour les élèves des classes préparatoires de MP et MP*, dont il suit exactement le nouveau programme, ou des préparations intégrées des INSA, ENSAM et UT, comme pour les étudiants de deuxième année universitaires, ce livre est un outil de travail pour mieux comprendre ce nouveau programme de mathématiques et il peut devenir un indispensable compagnon d'étude et de préparation aux concours d'entrée aux grandes écoles.

# Table des matières


**1 Structures algébriques usuelles** **1**
- 1.1 Compléments sur les groupes . . . 1
- 1.2 Compléments sur les anneaux . . . 2
- 1.3 Idéaux de $\mathbb{Z}$ . . . 2
- 1.4 Anneaux $\mathbb{Z}/n\mathbb{Z}$ . . . 2
- 1.5 Anneaux $\mathbb{K}[X]$ . . . 4
- 1.6 Algèbres . . . 4
- 1.7 Exercices résolus . . . 5
- 1.8 Problèmes résolus . . . 19

**2 Réduction des endomorphismes et des matrices carrées** **23**
- 2.1 Compléments d'algèbre linéaire . . . 23
- 2.2 Éléments propres d'un endomorphisme, d'une matrice carrée . . . 24
- 2.3 Polynôme caractéristique . . . 24
- 2.4 Endomorphismes et matrices carrées diagonalisables . . . 25
- 2.5 Endomorphismes et matrices carrées trigonalisables . . . 25
- 2.6 Endomorphismes nilpotents, matrices nilpotentes . . . 26
- 2.7 Polynômes d'un endomorphisme, d'une matrice carrée . . . 26
- 2.8 Lemme de décomposition des noyaux . . . 26
- 2.9 Polynômes annulateurs et réduction . . . 27
- 2.10 Théorème de Cayley-Hamilton et sous-espaces caractéristiques . . . 27
- 2.11 Exercices résolus . . . 27
- 2.12 Problèmes résolus . . . 46

**3 Endomorphismes d'un espace euclidien** **49**
- 3.1 Adjoint d'un endomorphisme . . . 49
- 3.2 Matrices orthogonales . . . 50
- 3.3 Isométries vectorielles d'un espace euclidien . . . 50
- 3.4 Isométries vectorielles en dimension 2 . . . 51
- 3.5 Réduction des isométries . . . 52

3.6 Endomorphismes autoadjoints d'un espace euclidien . . . 52
3.7 Endomorphismes autoadjoints positifs, définis positifs . . . 53
3.8 Exercices résolus . . . 53
3.9 Problèmes résolus . . . 68

**4 Topologie des espaces normés 75**
4.1 Normes et espaces vectoriels normés . . . 75
4.2 Suites d'éléments d'un espace vectoriel normé . . . 77
4.3 Comparaison des normes . . . 78
4.4 Topologie d'un espace normé . . . 78
4.5 Étude locale d'une application, continuité . . . 79
4.6 Applications linéaires et multilinéaires continues . . . 81
4.7 Parties compactes d'un espace normé . . . 82
4.8 Applications continues sur une partie compacte . . . 82
4.9 Connexité par arcs . . . 83
4.10 Espaces vectoriels normés de dimension finie . . . 83
4.11 Exercices résolus . . . 84
4.12 Problèmes résolus . . . 106

**5 Séries numériques et vectorielles 111**
5.1 Séries à valeurs dans un espace normé de dimension finie . . . 111
5.2 Compléments sur les séries numériques . . . 112
5.3 Exercices résolus . . . 113
5.4 Problèmes résolus . . . 127

**6 Suites et séries de fonctions, séries entières 131**
6.1 Suites et séries de fonctions . . . 131
6.1.1 Convergence simple, convergence uniforme . . . 131
6.1.2 Continuité, double limite . . . 132
6.1.3 Intégration d'une limite uniforme sur un segment . . . 132
6.1.4 Dérivation d'une suite de fonctions . . . 133
6.1.5 Séries de fonctions . . . 133
6.1.6 Approximation uniforme . . . 133
6.2 Séries entières . . . 133
6.2.1 Généralités . . . 133
6.2.2 Continuité de la somme d'une série entière de la variable complexe . . . 135
6.2.3 Régularité de la somme d'une série entière de la variable réelle . . . 135
6.2.4 Fonctions développables en série entière, développements usuels . . . 135
6.3 Exercices résolus . . . 136

6.4 Problèmes résolus . . . . . 163

**7 Fonctions vectorielles** **167**
7.1 Dérivabilité en un point . . . . . 167
7.2 Opérations sur les fonctions dérivables . . . . . 168
7.3 Intégration sur un segment . . . . . 169
7.4 Intégrale fonction de sa borne supérieure . . . . . 170
7.5 Formules de Taylor . . . . . 170
7.6 Exercices résolus . . . . . 171
7.7 Problèmes résolus . . . . . 188

**8 Intégration sur un intervalle quelconque** **191**
8.1 Intégrale généralisée sur un intervalle de la forme $[a, +\infty[$ . . . . . 191
8.2 Intégrabilité sur un intervalle de la forme $[a, +\infty[$ . . . . . 192
8.3 Intégrales généralisées sur un intervalle quelconque . . . . . 192
8.4 Intégrales absolument convergentes et fonctions intégrables . . . . . 193
8.5 Intégration des relations de comparaison . . . . . 194
8.6 Convergence dominée . . . . . 194
8.7 Intégration terme à terme . . . . . 195
8.8 Régularité d'une fonction définie par une intégrale à paramètre . . . . . 196
8.9 Exercices résolus . . . . . 197
8.10 Problèmes résolus . . . . . 211

**9 Variables aléatoires discrètes** **215**
9.1 Ensembles dénombrables . . . . . 215
9.2 Espaces probabilisés . . . . . 215
9.3 Probabilités conditionnelles et indépendance . . . . . 216
9.4 Espaces probabilisés discrets . . . . . 217
9.5 Variables aléatoires discrètes . . . . . 217
9.6 Variables aléatoires indépendantes . . . . . 218
9.7 Lois usuelles . . . . . 218
9.8 Espérance d'une variable aléatoire réelle ou complexe . . . . . 219
9.9 Variance d'une variable aléatoire, écart type et covariance . . . . . 220
9.10 Inégalités probabilistes et loi faible des grands nombres . . . . . 221
9.11 Fonctions génératrices . . . . . 221
9.12 Exercices résolus . . . . . 222
9.13 Problèmes résolus . . . . . 242

**10 Équations différentielles linéaires** **249**
10.1 Généralités . . . . . 249
10.2 Solutions d'une équation différentielle linéaire . . . . . 250

10.3 Exponentielle d'un endomorphisme, d'une matrice . . . 250
10.4 Systèmes différentiels linéaires homogènes à coefficients constants . . . 251
10.5 Variation des constantes . . . 252
10.6 Exercices résolus . . . 252
10.7 Problèmes résolus . . . 276

**11 Calcul différentiel et optimisation 283**
11.1 Dérivée selon un vecteur, dérivées partielles . . . 283
11.2 Différentielle . . . 283
11.3 Opérations sur les applications différentiables . . . 285
11.4 Applications de classe $\mathcal{C}^1$ . . . 285
11.5 Vecteurs tangents à une partie d'un espace normé de dimension finie . . . 286
11.6 Optimisation : étude au premier ordre . . . 286
11.7 Applications de classe $\mathcal{C}^k$ . . . 287
11.8 Optimisation : étude au second ordre . . . 288
11.9 Exercices résolus . . . 289
11.10Problèmes résolus . . . 300

**12 Problèmes de synthèse 305**
12.1 Structures algébriques usuelles . . . 305
12.2 Fonctions vectorielles . . . 314
12.3 Intégration sur un intervalle quelconque . . . 317
12.4 Endomorphismes d'un espace euclidien . . . 351
12.5 Séries entières . . . 363
12.6 Topologie des espaces normés . . . 371
12.7 Variables aléatoires discrètes . . . 379
12.8 Réduction des endomorphismes . . . 393
12.9 Suites et séries de fonctions . . . 433

**Index 439**

# Chapitre 1

# Structures algébriques usuelles

## 1.1 Compléments sur les groupes

**Théorème 1.1 (Caractérisation des sous-groupes)** *Soit $G$ un groupe et $H$ une partie de $G$. Les assertions suivantes sont équivalentes :*

*i) $H$ est un sous-groupe de $G$.*

*ii) $e_G \in H$ et $\forall h,h' \in H$, on a : $h^{-1}h' \in H$.*

**Définition 1.1 (Sous-groupe engendré par une partie)** *Soit $G$ un groupe et $S$ une partie de $G$. On appelle le sous-groupe de $G$ engendré par $S$, l'intersection de tous les sous-groupes de $G$ qui contiennent $S$. C'est le plus petit sous-groupe de $G$ contenant $S$, on le note $\langle S \rangle$.*

**Exemple 1.1** $\mathbb{Z} = \{n = n.1 \mid n \in \mathbb{Z}\} = \langle 1 \rangle$.
$U_n = \{z \in \mathbb{C} \mid z^n = 1\} = \langle e^{2i\pi/n} \rangle$.

**Théorème 1.2** *Toute intersection de sous-groupe de $G$ est un sous-groupe de $G$.*

**Définition 1.2** *S'il existe un élément $x$ de $G$ tel que $G = \langle x \rangle$,on dit que $G$ est un groupe monogène.*

**Définition 1.3** *Un groupe cyclique est un groupe monogène fini. Il est engendré par un seul élément.*

**Théorème 1.3** *Les générateurs de $\mathbb{Z}/p\mathbb{Z}$ sont les $\bar{k}$ avec $k \wedge n = 1$.*

**Théorème 1.4** *Si $x$ est d'ordre fini, l'ordre de $x$ est le cardinal du sous-groupe de $G$ engendré par $x$.*

**Théorème 1.5** *Si $x$ est d'ordre fini $d$ et si $e$ désigne l'élément neutre de $G$, alors, pour $n$ dans $\mathbb{Z}$, on a : $x^n = e \Leftrightarrow d \mid n$.*

**Théorème 1.6** *L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.*

## 1.2 Compléments sur les anneaux

**Définition 1.4** *si $(A_i)_{i\in I}$ est une famille d'anneaux, le produit cartésien $\prod_{i\in I} A_i$ peut être muni d'une structure d'anneau en définissant les opérations composante par composante, i.e.*

$$(a_i) + (b_i) = (a_i + b_i)(a_i)\dot{(}b_i) = (a_i\dot{b}_i)1_{\prod i\in I A_i} = (1_{A_i})_{i\in I}$$

*On peut écrire : $\prod_{1\leq i\leq k} A_i$, sous la forme : $A_1 \times A_2 \times \cdot \times A_k$.*

**Définition 1.5 (Idéal d'un anneau commutatif)** *Un idéal d'un anneau commutatif A est un sous-groupe I de (A,+) tel que de plus :*

$$\forall x \in I, \forall a \in A, ax \in I.$$

**Définition 1.6 (Idéal engendré par un élément)** *L'idéal engendré par un élément x est :*

$$xA = \{ax \mid x \in A\}$$

*C'est le plus petit idéal qui contient x.*

**Définition 1.7 (Divisibilité dans un anneau commutatif intègre)** *On dit, pour deux éléments a, b d'un anneau commutatif A, que a divise b (dans A) s'il existe q dans A tel que $aq = b$. Ce qui est particulier pour les anneaux intègres est que dans ce cas, si un élément non nul a divise b, alors l'élément q (le quotient) est toujours unique.*

## 1.3 Idéaux de $\mathbb{Z}$

**Définition 1.8** *Tout idéal I de $\mathbb{Z}$ est de la forme $\mathbb{Z}x$ où x est un élément de $\mathbb{Z}$.*

**Définition 1.9 (PGCD)** *Le PGCD de deux nombres entiers non nuls est le plus grand entier qui les divise simultanément.*

**Théorème 1.7 (Relation de Bézout)** *Soient a et b deux entiers naturels non nuls. a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $au + bv = 1$.*

## 1.4 Anneaux $\mathbb{Z}/n\mathbb{Z}$

**Définition 1.10 ($\mathbb{Z}/\boldsymbol{n}\mathbb{Z}$)** *Pour tout entier $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ possède n éléments et*

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \bar{n-1}\}.$$

**Théorème 1.8 (Anneaux $\mathbb{Z}/\boldsymbol{n}\mathbb{Z}$)** *$(\mathbb{Z}/n\mathbb{Z}, +, \dot{})$ est un anneau commutatif et unitaire.*

**Théorème 1.9** *Pour tout entier naturel $n$, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n$ est premier.*

**Théorème chinois**
*Si $m$ et $n$ sont deux entiers premiers entre eux, les ensembles $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes.*

**Définition 1.11 (Indicatrice d'Euler)** *On appelle indicatrice d'Euler d'un entier $n$ l'entier $\phi(n)$ défini par :*

$$\phi(n) = card\{1 \leq k \leq n;\ k \text{ est premier avec } n\}.$$

*$\phi(n)$ est aussi le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$, l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

**Théorème 1.10** *On a : $\phi(mn) = \phi(m)\phi(n)$ si $m$ et $n$ sont premiers entre eux.*

**Théorème 1.11** *Si $p$ est premier et $k \geq 1$, $\phi(p) = p - 1$ et $\phi(p^k) = p^k - p^{k-1}$.*

Calcul à l'aide de la décomposition en produits de facteurs premiers.

On peut calculer l'indicateur d'Euler $\phi(n)$ connaissant la décomposition en facteurs premiers de $n$. On a :

$$\begin{aligned} \phi(p_1^{k_1}) - \phi(p_r^{k_r}) &= (p_1^{k_1} - p_1^{k_1-1}) \times \cdots \times (p_r^{k_r} - p_r^{k_r-1}) \\ &= n\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_r}\right). \end{aligned}$$

**Théorème d'Euler**
*Soit un entier $n > 1$. Si $k \in \mathbb{Z}$ vérifie $k \wedge n = 1$, alors*

$$k^{\phi(n)} \equiv 1 \quad [n].$$

Le lien avec le petit théorème de Fermat est le suivant :

**Théorème 1.12** *Soit $p$ un nombre premier, et $a$ un entier premier avec $p$. Alors $a^{p-1}$ a pour reste 1 dans la division par $p$ :*

$$a^{p-1} = 1 \quad mod\ p.$$

## 1.5 Anneaux $\mathbb{K}[X]$

**Définition 1.12** *Soient $n \in \mathbb{N}^*$, $(P_1,\ldots,P_n) \in (\mathbb{K}[X]-\{0\})^n$, il existe un polynôme et un seul $D$, unitaire, non nul, diviseur commun de $P_1,\ldots,P_n$ ; $D$ est appelé le plus grand commun diviseur de $P_1,\ldots,P_n$ et noté* $\mathrm{PGCD}(P_1,\ldots,P_n)$.

**Identité de Bézout**
*Soit $P$ et $Q$ deux polynômes, $P$ et $Q$ sont premiers entre eux si et seulement s'il existe deux polynômes $M$ et $N$ tels que :*

$$PM + QN = 1.$$

**Lemme de Gauss**
*Etant donné trois polynômes $P$, $Q$ et $R$ tels que*

$$P \mid QR \quad P \wedge Q = 1 \text{ alors} \quad P \mid R.$$

**Définition 1.13 (Polynôme irréductible)** *Un polynôme $P$ de $\mathbb{K}[X]$ est dit irréductible sur le corps $\mathbb{K}$ s'il est non inversible et si les seuls diviseurs dans $\mathbb{K}[X]$ sont les polynômes associés à $P$, et les éléments de $\mathbb{K}\backslash\{0\}$.*

**Théorème de décomposition**
*Tout polynôme non-constant $P$ (non-inversible) peut s'écrire d'une manière unique sous la forme :*

$$P = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \ldots P_r^{\alpha_r}$$

*avec $\lambda \in \mathbb{K}^* = \mathbb{K}\backslash\{0\}$ ; $P_1,P_2,\ldots,P_r$ des polynômes irréductibles et $\alpha_1,\ldots,\alpha_r$ des entiers naturels.*

**Corollaire 1.1** *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré un et les polynômes de degré deux de discriminant srictement négatif.*

**Théorème 1.13** *Les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré* 1.

## 1.6 Algèbres

**Définition 1.14** *Soit $E$ un ensemble, muni de deux lois internes $+$, $\times$ et d'une loi externe à opérateurs dans $\mathbb{K}$ . Alors $(E,+,\times,.)$ est un $\mathbb{K}-$algèbre lorsque :*

*1) $(E,+,\times,.)$ est un $\mathbb{K}-$espace vectoriel.*
*2) La loi $\times$ est associative et admet un élément neutre (qu'on note $1_E$).*
*3) La loi $\times$ est distributive sur la loi $+$.*
*4) Pour tous $u,v \in E$, et tout $\lambda \in \mathbb{K}$, $(\lambda u)\times v = u \times (\lambda v) = \lambda(u \times v)$.*

**Définition 1.15 (Sous-algèbre)** *Un sous-algèbre d'un $\mathbb{K}-$algèbre $(E,+,\times,.)$, est une partie $F$ de $E$ qui contient $1_E$ et qui est stable pour chacune des trois lois, c'est-à-dire :*

*1)* $1_E \in F$

*2)* $\forall (u,v) \in F^2$, $u+v \in F$ *et* $u \times v \in F$

*3)* $\forall u \in \mathbb{K}$, $\forall \lambda \in \mathbb{K}$, $\lambda u \in F$.

**Définition 1.16 (Morphisme d'algèbre)** *Soient $(E,+,\times,\dot{})$ et $(F,+,\times,\dot{})$ deux $\mathbb{K}-$algèbres. Soit $\phi$: $E \to F$. On dit que $\phi$ est un morphisme de $\mathbb{K}-$algèbres si les assertions suivantes sont vérifiées :*

*1)* $\forall (u,v) \in E^2$, $\phi(u+v) = \phi(u) + \phi(v)$

*2)* $\forall (u,v) \in E^2$, $\phi(u \times v) = \phi(u) \times \phi(v)$

*3)* $\forall u \in E$, $\forall \lambda \in \mathbb{K}$, $\phi(\lambda u) = \lambda \phi(u)$

*4)* $\phi(1_E) = 1_F$.

## 1.7 Exercices résolus

**Exercice 1.1** *Soit $G = \mathbb{R}^\star \times \mathbb{R}$ et $\star$ la loi de composition interne définie sur $G$ par*

$$(x,y) \star (x',y') = (xx', xy' + y)$$

*1) Montrer que $(G,\star)$ est un groupe non commutatif.*

*2) Montrer que $\mathbb{R}_+^\star \times \mathbb{R}$ est un sous-groupe de $(G,\star)$.*

**Solution.**

1) La loi $\star$ est bien définie, on montre que $*$ est associative, (1,0) est l'élément neutre et $(\frac{1}{x}, -\frac{y}{x})$ est le symétrique de $(x,y)$. Soient $(x,y), (x',y'), (x'',y'') \in G$

   a) Associativité :

$$\begin{aligned}(x,y) \star (x',y') \star (x'',y'') &= (xx', xy' + y) \star (x'',y'') \\ &= (xx'x'', xx'y'' + xy' + y)\end{aligned}$$

   et

$$\begin{aligned}(x,y) \star ((x',y') \star (x'',y'')) &= (x,y) \star (x'x'', x'y'' + y') \\ &= (xx'x'', xx'y'' + xy' + y)\end{aligned}$$

   donc $\star$ est associative.

   b) Elément neutre :

$$(x,y) \star (1,0) = (x,y) \quad \text{et} \quad (1,0) \star (x,y) = (x,y)$$

   donc (1,0) est élément neutre.

c) Symétrie :

$$(x,y) \star (1/x, -y/x) = (1,0) \quad \text{et} \quad (1/x, -y/x) \star (x,y) = (1,0)$$

donc tout élément est symétrisable.

Finalement d'après a), b) et c), on a : $(G,\star)$ est un groupe.

$(1,2)\star(3,4) = (3,6)$ et $(3,4)\star(1,2) = (3,10)$ donc le groupe n'est pas commutatif.

2) $H = \mathbb{R}_+^\star \times \mathbb{R}$ est inclus dans $G$.

$(1,0) \in H$.

$$\forall\, (x,y)\,,\ (x',y') \in H,\ (x,y) \star (x',y') \in H$$

car $xx' > 0$

$$\forall\, (x,y) \in H,\ (x,y)^{-1} = (1/x, -y/x) \in H$$

car $1/x > 0$.

D'où $H$ est un sous groupe de $(G,\star)$.

**Exercice 1.2** *1) Montrer que $\mathbb{Z}^2$ n'est pas monogène.*

*2) Est-ce que $(\mathbb{Z}/10\mathbb{Z}) \times (\mathbb{Z}/21\mathbb{Z})$ est monogène ?*

**Solution.**

1) Soit $(a,b) \in \mathbb{Z}^2$. Le sous-groupe de $\mathbb{Z}^2$ engendré par $(a,b)$ est l'ensemble $A = \{(na,nb)\ ;\ n \in \mathbb{Z}\}$.

*bullet* Si $(a,b) = (0,0)$, il est clair que $A \neq \mathbb{Z}^2$.

• Sinon, on suppose par exemple $b \neq 0$. Alors $(1,0) \notin A$ puisque

$$nb = 0 \Rightarrow n = 0.$$

Dans tous les cas $A \neq \mathbb{Z}^2$, donc $\mathbb{Z}^2$ n'est pas monogène.

2) Le groupe $(\mathbb{Z}/10\mathbb{Z}) \times (\mathbb{Z}/21\mathbb{Z})$ est isomorphe à $\mathbb{Z}/210\mathbb{Z}$ puisque 10 et 21 sont premiers entre eux $(21 - 2 \times 10 = 1)$.

**Exercice 1.3** *1) L'ensemble des matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ avec $a,b,c,d \in \mathbb{R}$ tels que $ad - bc \neq 0$ et $a^2 - b^2 - c^2 - d^2 \leq 1$ est-il un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$ ?*

*2) L'ensemble des matrices $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ avec $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$ est-il un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$ ?*

*3) Existe-t-il une valeur $M \in \mathbb{R}$ telle que l'ensemble des matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ avec $a,b,c,d \in \mathbb{R}$ tels que $ad - bc \neq 0$ et $a \leq M$ forme un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$ ?*

**Solution.**

1) L'ensemble $G$ des matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ avec $a,b,c,d \in \mathbb{R}$ tels que $ad - bc \neq 0$ et $a^2 - b^2 - c^2 - d^2 \leq 1$ n'est pas un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$. En effet, les deux matrices $\begin{pmatrix} 1 & 1 \\ 0 & \frac{1}{2} \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 1 & \frac{1}{2} \end{pmatrix}$ appartiennent à $G$ et leur produit $\begin{pmatrix} 2 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{4} \end{pmatrix}$ n'appartient pas à $G$.

2) L'ensemble $H$ des matrices $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ avec $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$ est un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$. En effet,
   - $I_2$ élément neutre de $\mathcal{G}l_2(\mathbb{R})$ appartient à $H$.
   - Soient $M = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ et $M' = \begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix}$ deux éléments de $H$ alors $MM' = \begin{pmatrix} ac & ad + bc^{-1} \\ 0 & (ac)^{-1} \end{pmatrix}$ donc le produit de deux éléments de $H$ appartient à $H$.
   - Soit $M = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$. Alors $M^{-1} = \begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix}$ appartient à $H$.

3) Soit $K_M$ l'ensemble des matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ avec $a$,$b$,$c$,$d \in \mathbb{R}$ tels que $ad - bc \neq 0$ et $a \leq M$. On montre, en raisonnant par l'absurde, qu'il n'existe pas de valeur $M \in \mathbb{R}$ telle que $K_M$ forme un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$.
   Soit $M \in \mathbb{R}$ tel que $K_M$ forme un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$. Alors $I_2$ appartient à $K_M$ donc $M \geq 1$. Ainsi, les matrices $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et, pour tout $n \in \mathbb{N}$, $A_n = \begin{pmatrix} 1 & 1 \\ n & 1 \end{pmatrix}$ appartiennent à $K_n$ donc le produit $AA_n = \begin{pmatrix} 1+n & 0 \\ 0 & 1 \end{pmatrix}$ appartient à $K_n$. En conséquence, pour tout $n \in \mathbb{N}$, on a : $1 + n \leq M$, ce qui est absurde.

**Exercice 1.4** *Soit $G$ un groupe, $H$ et $K$ deux sous-groupes de $G$. Montrer que $H \cup K$ est un sous-groupe de $G$ si et seulement si $H \subset K$ ou $K \subset H$.*

**Solution.**

- Si $H \subset K$ alors $H \cup K = K$, qui est un sous-groupe de $H$. Même chose si $K \subset H$.
- Réciproquement, supposons que $H \cup K$ est un sous-groupe de $G$. Par l'absurde supposons que $H \not\subset K$ et $K \not\subset H$. Alors il existe $x \in H \setminus K$ et $y \in K \setminus H$. Comme $x$,$y \in H \cup K$ et que $H \cup K$ est un groupe alors $x.y \in H \cup K$. Donc $x.y \in H$ ou $x.y \in K$. Par exemple supposons $x.y \in H$ alors comme $x \in H$, $x^{-1} \in H$ et donc comme $H$ est un groupe $x^{-1}.x.y \in H$ et donc $y \in H$. Ce qui est en contradiction avec l'hypothèse $y \in K \setminus H$. En conclusion, parmi les sous-groupes $H$ et $K$ l'un est inclus dans l'autre.

**Exercice 1.5** *Soit $H$ un groupe abélien. Un élément $x \in H$ est dit d'ordre fini lorsqu'il existe $n \in \mathbb{N}$ tel que la somme $x + \cdots + x$ ($n$-fois) soit égale à 0. Montrer que l'ensemble des éléments d'ordre fini de $H$ est un sous-groupe abélien de $H$.*

**Solution.** On note $G$ l'ensemble des éléments d'ordre fini de $H$. On montre que $G$ est un sous-groupe de $H$.
- $G \subset H$ et $0 \in G$.
- Si $x \in G$ alors $(-x)+(-x)+\cdots+(-x) = -(x+x+\cdots+x) = 0$. Donc $-x \in G$.

– Si $x$,$y \in G$ alors $(x+y)+\cdots+(x+y) = (x+\cdots+x)+(y+\cdots+y) = 0+0 = 0$. Donc $x+y \in G$.

On a montré que $G$ est un sous-groupe de $H$. De plus, comme $H$ est commutatif alors $G$ l'est aussi.

**Exercice 1.6** *Soient $G$ un groupe et $x \in G$ un élément d'ordre $n$. Quel est l'ordre de $x^2$ ?*

**Solution.** On rappelle d'abord que pour $x$ un élément d'ordre $n$, alors

$$x^q = e \Rightarrow n|q.$$

– Si $n$ est pair alors $\text{ord}(x^2) = n/2$ : en effet $(x^2)^{\frac{n}{2}} = x^n = e$ et pour $p \geq 1$ tel que $(x^2)^p = e$ alors $x^{2p} = e$ et $n|2p$ donc $p \geq \frac{n}{2}$. Donc $n/2$ est le plus petit des entiers $q$ (non nul) tel que $x^q = e$ et par conséquent $n/2$ est l'ordre de $x$.
– Si $n$ est impair alors $\text{ord}(x) = n$. Tout d'abord $(x^2)^n = (x^n)^2 = e$ et pour $p$ tel que $(x^2)^p = e$ alors $n|2p$ mais 2 et $n$ sont premiers entre eux donc d'après le théorème de Gauss, $n|p$ et en particulier $p \geq n$.

**Exercice 1.7** *1) Soient $G$ un groupe et $x$,$y \in G$ des éléments qui commutent et d'ordres respectifs $m$ et $n$ premiers entre eux. Montrer que $xy$ est d'ordre $mn$. Montrer que l'hypothèse $m$ et $n$ premiers entre eux est indispensable.*

*2) Montrer que $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ sont des éléments d'ordres finis et que $AB$ n'est pas d'ordre fini.*

**Solution.**

1) On a $(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n(y^n)^m = e.e = e$. Soit $p$ tel que $(xy)^p = e$, alors $e = (xy)^{mp} = x^{mp}y^{mp} = y^{mp}$, et donc $mp$ est divisible par l'ordre de $y$, c'est-à-dire $n$. Comme $m$ et $n$ sont premiers entre eux alors d'après le théorème de Gauss $n$ divise $p$. Un raisonnement semblable à partir de $(xy)^{np} = e$ conduit à : $m$ divise $p$. Finalement $m|p$ et $n|p$ donc $mn|p$ car $m$ et $n$ sont premiers entre eux.
   On propose un contre-exemple dans le cas où $m$ et $n$ ne sont pas premiers entre eux : dans le groupe $\mathbb{Z}/12\mathbb{Z}$ : $\bar{2}$ est d'ordre 6, $\bar{4}$ est d'ordre 3, mais $\bar{2}+\bar{4} = \bar{6}$ est d'ordre $2 \neq 3 \times 6$.
2) $A$ est d'ordre 4, $B$ est d'ordre 3, $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ n'est jamais la matrice identité pout $n \geq 1$.

**Exercice 1.8** *Le groupe $(\mathbb{Q},+)$ est-il monogène ?*

**Solution.** On propose une démonstration par l'absurde. Supposons que $(\mathbb{Q},+)$ est engendré par un seul élément $\frac{p}{q}$ ($p$ et $q$ premiers entre eux) alors tout élément de $\mathbb{Q}$ s'écrit $n\frac{p}{q}$ avec $n \in \mathbb{Z}$. Il s'ensuit que $\frac{p}{2q}$ (qui appartient à $\mathbb{Q}$) doit s'écrire $n\frac{p}{q}$, mais alors $2n = 1$ avec $n \in \mathbb{Z}$ ce qui est impossible. Par conséquent, $(\mathbb{Q},+)$ n'est pas monogène.

**Exercice 1.9** *Montrer que les groupes multiplicatifs $\mathbb{R} \setminus \{0\}$ et $\mathbb{C} \setminus \{0\}$ ne sont pas isomorphes.*

**Solution.** Soit $\phi : \mathbb{C}^* \longrightarrow \mathbb{R}^*$ un morphisme entre les deux groupes multiplicatifs $\mathbb{C}^*$ et $\mathbb{R}^*$. Notons $a = \phi(i) \in \mathbb{R}^*$. Alors $\phi(-1) = \phi(i^2) = \phi(i)^2 = a^2$, de même $1 = \phi(1) = \phi((-1)^2) = \phi(-1)^2 = a^4$ ; donc $a^4 = 1$ et nécessairement $a^2 = 1$. Le morphisme $\phi$ n'est pas injectif car $\phi(1) = \phi(-1) = 1$, a fortiori $\phi$ n'est pas un isomorphisme.

**Exercice 1.10** *Soient $p$ un nombre premier et $G$ un groupe d'ordre $p$. Montrer que $G$ est cyclique et donner la liste des générateurs de $G$.*

**Solution.** Soit $x \neq e$ un élément de $G$, soit $H = \{e,x,x^2,\ldots\}$ le sous-groupe engendré par $x$. $H$ est un sous-groupe de $G$ donc $\operatorname{Card} H$ divise $\operatorname{Card} G = p$ qui un nombre premier. En conséquent $\operatorname{Card} H = 1$ ou $p$ mais $H \neq \{e\}$ donc $\operatorname{Card} H = p$ et $H = G$.

On a montré que $G$ est engendré par $x$ donc $G$ est un groupe cyclique. De plus le raisonnement est valide quelque soit $x \neq e$ alors tout élément de $G \setminus \{e\}$ est un générateur de $G$.

**Exercice 1.11** *Soit $G$ un groupe d'ordre $pn$ avec $p$ premier.*

*1) On considère deux sous-groupes $H$ et $H'$ de $G$ d'ordre $p$ avec $H \neq H'$. Montrer que $H \cap H' = \{e\}$.*

*2) En déduire que le nombre d'éléments d'ordre $p$ dans $G$ est un multiple de $p-1$.*

**Solution.**

1) $H \cap H'$ est un sous-groupe de $H$ donc $\operatorname{Card}(H \cap H')$ divise $\operatorname{Card} H = p$. Or $p$ est premier donc $\operatorname{Card}(H \cap H') = 1$ ou $p$. Mais $H \cap H' \neq H$ donc $\operatorname{Card}(H \cap H') \neq p$ et donc $H \cap H' = \{e\}$.
2) Soit $E$ l'ensemble des éléments d'ordre $p$ que l'on suppose non vide. On note que pour $x \in E$ le sous-groupe $H_x$ engendré par $x$ est d'ordre $p$ et de plus tout $z \in H_x \setminus \{e\}$ est d'ordre $p$ car $H_x$ est cyclique et $p$ est premier. Donc $H_x$ contient $p-1$ élément d'ordre $p$.
   Si $E$ ne contient qu'un seul élément $x$, alors $E = H_x \setminus \{e\}$ et donc $E$ contient $p-1$ éléments.
   Sinon, soit $x,y \in E$ avec $x \neq y$. Alors d'après la première question $H_x \cap H_y = \{e\}$. Donc $E$ se décompose en une union disjointe de $H_x \setminus \{e\}$. Donc $\operatorname{Card} E$ est multiple de $p-1$.

**Exercice 1.12** *1) Soit $G$ un groupe dans lequel tout élément (distinct de l'élément neutre) est d'ordre 2. Montrer que $G$ est commutatif.*

*2) Soit $G$ un groupe d'ordre pair. Montrer que $G$ contient au moins un élément d'ordre 2.*

**Solution.**

1) On note d'abord que pour $x \in G$ ; $x^2 = e$ et donc $x^{-1} = x$. Soit $x,y \in G$. Alors $xy \in G$ et $(xy)^2 = e$ donc $xy = (xy)^{-1}$ et par suite $xy = y^{-1}x^{-1} = yx$ car $x$ et $y$ sont d'ordre 2. Le produit de deux éléments quelconques de $G$ commute donc $G$ est un groupe commutatif.

2) On note $E$ l'ensemble des éléments d'ordre 2.

$$E = \{x \in G \ / \ x^2 = e \text{ et } x \neq e\} = \{x \in G \ / \ x = x^{-1} \text{ et } x \neq e\}.$$

On démontre l'assertion par l'absurde, on suppose que $H$ est l'ensemble vide. Alors quelque soit $x \neq e$ dans $G$ ; $x \neq x^{-1}$. Donc nous pouvons décomposer $G \setminus \{e\}$ en deux ensembles disjoints $F = \{x_1, \ldots, x_n\}$ et $F' = \{{x_1}^{-1}, \ldots, {x_n}^{-1}\}$ qui sont de même cardinal $n$. Donc le cardinal de $G$ est $2n+1$. Ce qui contredit l'hypothèse « $G$ d'orde pair ».

**Exercice 1.13** *1) Rappeler $|S_3|$. Montrer que $S_3$ ne contient pas d'élément d'ordre* 6.

*2) Montrer que $S_3$ contient un unique sous-groupe d'ordre* 3. *Déterminer tous les sous-groupes d'ordre* 2 *de $S_3$.*

*3) Déduire de ce qui précède tous les sous-groupes de $S_3$.*

**Solution.**

1) $|S_n| = n!$ donc $|S_3| = 3! = 6$. Montrons plus généralement qu'il n'existe pas d'élément d'ordre $n!$ dans $S_n$ ($n \geq 3$). Par l'absurde soit $\alpha$ un tel élément. Alors par hypothèse $S_n$ est engendré par $\alpha$ et donc $S_n$ est un groupe commutatif. Mais (1,2)(2,3) $\neq$ (2,3)(1,2) ce qui est absurde. En conclusion il n'existe pas d'éléments d'ordre 6.

2) $S_3$ est définie par :

$$S_3 = \left\{\mathrm{id}; \tau_1 = (1,2); \tau_2 = (2,3); \tau_3 = (1,3); \sigma_1 = (1,2,3); \sigma_2 = \sigma_1^{-1} = (3,2,1)\right\}.$$

Les sous-groupes d'ordre 2 sont de la forme $\{\mathrm{id}; \tau\}$ avec $\tau^2 = id$. Les seuls éléments d'ordre 2 sont les transpositions et donc se sont les groupes $\{\mathrm{id}; (1,2)\}$, $\{\mathrm{id}; (1,3)\}$ et $\{\mathrm{id}; (2,3)\}$.
Les sous-groupes d'ordre trois sont de la forme $\{\mathrm{id}, \sigma, \sigma^2\}$ avec $\sigma^2 = \sigma^{-1}$. Et donc le seul sous-groupe d'ordre 3 est $\{\mathrm{id}; (1,2,3); (3,2,1)\}$.

3) Les sous-groupes de $S_3$ ont un ordre qui divise $|S_3| = 6$. Donc un sous-groupe peut-être d'ordre 1,2,3 ou 6. L'unique sous-groupe d'ordre 1 est $\{id\}$, et l'unique sous-groupe d'ordre 6 est $S_3$. Les sous-groupes d'ordre 2 et 3 sont donnés dans la question 2.

**Exercice 1.14** *Trouver la décomposition en produit de cycles à supports disjoints, la signature, l'ordre et une décomposition en produit de transpositions des permutations suivantes de $\mathcal{S}_{10}$ :*

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

$$\varphi = (10,3,4,1)\,(8,7)\,(4,7)\,(5,6)\,(2,6)\,(2,9)\,.$$

*Calculer $\sigma^{1998}$ et $\varphi^{1998}$.*

**Solution.**

1) $\sigma = (1,3)(2,7,9,5) = (2,7,9,5)(1,3)$ et $\sigma^k = (1,3)^k(2,7,9,5)^k$. Les transpositions sont d'ordre 2 donc $(1,3)^k = \mathrm{id}$ si $k \equiv 0\,[2]$ et $(1,3)^k = (1,3)$ si $k \equiv 1\,[2]$.
Le cycle (2,7,9,5) est d'ordre 4, et $(2,7,9,5)^k$ est respectivement égale à id,(2,7,9,5),(2,9)(7,5),(5,9,7,2) si $k$ est respectivement congru à 0,1,2,3 modulo 4.
Le calcul de $\sigma^k$ donne donc id,(1,3)(2,7,9,5),(2,9)(7,5) ou (1,3)(5,9,7,2) selon que $k$ est congru à 0,1,2 ou 3 modulo 4.
2) L'écriture de $\varphi = (10,3,4,1)(8,7)(4,7)(5,6)(2,6)(2,9)$ est une décomposition en produit de cycles mais ils ne sont pas à supports disjoints. On écrit $\varphi$ sous la forme :
$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 9 & 4 & 8 & 6 & 2 & 1 & 7 & 5 & 3 \end{pmatrix}$$
Ce qui se décompose de la façon suivante
$$\varphi = (1,10,3,4,8,7)(2,9,5,6) = (2,9,5,6)(1,10,3,4,8,7).$$
Le calcul de $\varphi^k = (1,10,3,4,8,7)^k(2,9,5,6)^k$ est similaire au calcul précédent (selon $k(\mod 12)$ ).

**Exercice 1.15** *1) Montrer que $\mathcal{S}_n$ est isomorphe à un sous-groupe de $\mathcal{A}_{n+2}$.*
*2) Montrer que $\mathcal{S}_4$ n'est pas isomorphe à un sous-groupe de $\mathcal{A}_5$.*
*3) Montrer que $\mathcal{S}_5$ n'est pas isomorphe à un sous-groupe de $\mathcal{A}_6$.*

**Solution.**

1) $\mathcal{S}_N$ est l'ensemble des permutations de l'ensemble $\{1,2,\ldots,N\}$. Dans $\mathcal{S}_{n+2}$, notons $\tau$ la permutation $(n+1,n+2)$. Nous définissons une application $\phi : \mathcal{S}_n \longrightarrow \mathcal{S}_{n+2}$ par les relations
$$\phi(\sigma) = \sigma \text{ si } \epsilon(\sigma) = +1 \quad ; \quad \phi(\sigma) = \sigma \circ \tau \text{ sinon} ;$$
où $\epsilon$ désigne la signature. Alors $\phi$ est un morphisme de groupe, de plus $\forall \sigma \in \mathcal{S}_n$ alors $\epsilon(\phi(\sigma)) = +1$ (si $\epsilon(\sigma) = +1$ c'est clair, sinon $\epsilon(\phi(\sigma)) = \epsilon(\sigma) \times \epsilon(\tau) = (-1) \times (-1) = +1$). Donc $\phi(\mathcal{S}_n)$ est un sous-groupe de $\mathcal{A}_{n+2}$.
Enfin $\phi$ est injective : en effet soit $\sigma$ tel que $\phi(\sigma) = \mathrm{id}$. Soit $\epsilon(\sigma) = +1$ et alors $\phi(\sigma) = \sigma = \mathrm{id}$ ; soit $\epsilon(\sigma) = -1$ et alors $\phi(\sigma) = \sigma \circ \tau$, pour $j \in \{1,2,\ldots,n\}$ $j = \phi(\sigma)(j) = \sigma \circ \tau(j) = \sigma(j)$, et donc quelque soit $j \in \{1,2,\ldots,n\}$ $\sigma(j) = j$ et donc $\sigma = \mathrm{id}$.
On vient de démontrer que la composée de deux permutations à supports disjoint est l'identité si et seulement si les permutations sont déjà l'identité.
On note encore $\phi$: $\mathcal{S}_n \to \phi(\mathcal{S}_n)$ le morphisme induit par $\phi$. Il est injectif et surjectif, donc $\mathcal{S}_n$ est isomorphe $\phi(\mathcal{S}_n)$ qui est un sous-groupe de $\mathcal{A}_{n+2}$.
2) $\mathcal{A}_5$ est de cardinal $5!/2 = 60$, et comme $24 = \mathrm{Card}\,\mathcal{S}_4$ ne divise pas 60 alors $\mathcal{A}_5$ n'a pas de sous-groupe d'ordre 24.

3) Comme $\operatorname{Card}\mathcal{S}_5 = 5! = 120$ divise $\operatorname{Card}\mathcal{A}_6 = 6!/2 = 360$ donc l'argument ci-dessus n'est pas valide. Cependant s'il existe un isomorphisme entre $\mathcal{S}_5$ et un sous-groupe de $\mathcal{A}_6$ alors un cycle d'ordre 5 de $\mathcal{S}_5$ est envoyé sur une permutation $\sigma \in \mathcal{A}_6$ d'ordre 5.
On décompose $\sigma$ en produit de cycles à supports disjoints,
$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots$ Comme les cycles $\sigma_i$ sont à supports disjoints, il y a au plus trois cycles (de longueur $\geq 2$) dans la décomposition (car dans $\mathcal{A}_6$ on peut permuter au plus 6 éléments).
   - Le cas $\sigma = \sigma_1$ n'est pas possible car alors $\sigma_1$ serait un cycle d'ordre 5 et donc de signature $-1$ dans $\mathcal{A}_6$.
   - Si $\sigma = \sigma_1 \circ \sigma_2$ alors les longueurs de $\sigma_1$ et $\sigma_2$ sont (4,2) ou (2,2), et l'ordre de leur composée $\sigma_1 \circ \sigma_2$ est donc 4 ou 2 mais pas 5.
   - Si $\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3$ alors les $\sigma_i$ sont des transpositions, et la signature de $\sigma$ est alors $-1$ ce qui contredit $\sigma \in \mathcal{A}_6$.

   Donc $S_5$ n'est pas isomorphe à un sous-groupe de $\mathcal{A}_6$.

**Exercice 1.16** *On considère un entier $n > 0$ et deux suites finies $(a_k)_{1\leqslant k\leqslant n}$ et $(b_k)_{1\leqslant k\leqslant n}$ de réels telles que $a_k + b_l \neq 0$ pour tout $(k,l) \in \{1,2,\ldots,n\}^2$. Pour tout entier $m$ tel que $0 < m \leqslant n$, le déterminant de Cauchy d'ordre $m$ est défini par :*

$$D_m = \begin{vmatrix} \frac{1}{a_1+b_1} & \frac{1}{a_1+b_2} & \cdots & \frac{1}{a_1+b_m} \\ \frac{1}{a_2+b_1} & \frac{1}{a_2+b_2} & \cdots & \frac{1}{a_2+b_m} \\ \frac{1}{a_m+b_1} & \frac{1}{a_m+b_2} & \cdots & \frac{1}{a_m+b_m} \end{vmatrix}$$

*On définit la fraction rationnelle :*

$$R(X) = \frac{\prod_{k=1}^{n-1}(X-a_k)}{\prod_{k=1}^{n}(X-b_k)}.$$

*1) Montrer que si $R(X)$ est de la forme $R(X) = \sum_{k=1}^{n} \frac{A_k}{X+b_k}$ alors*

$$A_n D_n = R(a_n) D_{n-1}.$$

*2) En déduire que*

$$D_n = \frac{\prod_{1\leqslant i,j\leqslant n}(a_j - a_i)(b_j - b_i)}{\prod_{1\leqslant i,j\leqslant n}(b_j + a_i)}$$

**Solution.**

1) Comme la fraction rationnelle $R(X)$ est de degré égal à $-1$ si les pôles $b_k$ sont distincts (ce qu'on suppose puisque sinon $D_m = 0$), elle admet une décompsition

en éléments simples de la forme $R(X) = \sum_{k=1}^{n} \frac{A_k}{X + b_k}$ où les $A_k$ sont déterminés classiquement par la méthode dite des pôles ou des résidus

$$A_k = \frac{\prod_{j=1}^{n-1} (-b_k - \alpha_k)}{\prod_{\substack{j=1 \\ j \neq k}}^{n} (b_j - b_k)}$$

comme le déterminant d'une matrice est linéaire par rapport à chacune de ses colonnes, $A_n D_n$ est le déterminant obtenu à partir de $D_n$ en remplaçant la dernière colonne par elle-même multipliée par $A_n$ dans le déterminant obtenu. On effectue l'opération élémentaire suivante : $C_n \leftarrow C_n + \sum_{j=1}^{n-1} A_j C_j$ et on obtient le déterminant $\Delta_n$ à partir de $D_n$ en remplaçant la dernière colonne par la transposée de la ligne $(R(a_1), R(a_2), \ldots, R(a_n))$ i.e $(0\,0 \ldots 0\, R(a_n))$ puisque $a_1, a_2, \ldots, a_{n-1}$ sont racines de $R$. Le développement du déterminant $A_n D_n = \Delta_n$ par rapport à sa dernière colonne donne $A_n D_n = R(a_n) D_{n-1}$.

2) Donc

$$D_n = \frac{R(a_n)}{A_n} D_{n-1} = \frac{\prod_{k=1}^{n-1} (a_n - a_k) \prod_{k=1}^{n-1} (b_n - b_k)}{\prod_{k=1}^{n} (a_n + b_k) \prod_{k=1}^{n-1} (a_k + b_n)} D_{n-1}$$

Comme $D_1 = \frac{1}{a_1 + b_1}$, le résultat est obtenu par récurrence.

**Exercice 1.17** *Soient $A$ un anneau commutatif et $I$ un idéal de $A$. On appelle radical de $I$ et on note $\sqrt{I}$, l'ensemble des éléments $x$ de $A$ pour lesquels il existe un entier $n$ tel que $x^n$ appartienne à $I$.*

*1) Démontrer que $\sqrt{I}$ contient $I$ et que $\sqrt{I}$ est un idéal de $A$.*

*2) Soient $I$ et $J$ deux idéaux de $A$ tels que $I \subset J$ ; démontrer que $\sqrt{I} \subset \sqrt{J}$. Démontrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.*

*3) Démontrer que $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.*

**Solution.**

1) On remarque d'abord que $\sqrt{I}$ est non vide car il contient l'idéal $I$ ; en effet, si $x$ est un élément de $I$, $x^1 = x$ appartient à $I$ donc $x$ est un élément de $\sqrt{I}$.
Soient $x$ et $y$ deux éléments de $\sqrt{I}$ ; il existe alors deux entiers $m$ et $n$ tels que $x^n$ et $y^m$ appartiennent à $I$. On calcule $(x - y)^{m+n}$ ; puisque l'anneau $A$ est

commutatif, on peut utiliser la formule du binôme ; on obtient

$$\begin{aligned}(x-y)^{m+n} &= \sum_{p=0}^{p=m+n}(-1)^{m+n-p}\ \mathrm{C}_{m+n}^{p}\ x^p\ y^{m+n-p}\\ &= \sum_{p=0}^{p=n}(-1)^{m+n-p}\ \mathrm{C}_{m+n}^{p}\ x^p\ y^{m+n-p}+\\ &\quad \sum_{p=n+1}^{p=m+n}(-1)^{m+n-p}\ \mathrm{C}_{m+n}^{p}\ x^p\ y^{m+n-p}\end{aligned}$$

Si $0 \leq p \leq n$, $m+n-p \geq m$ donc

$$x^p\ y^{m+n-p} = y^m(x^p\ y^{n-p})$$

Si $n+1 \leq p \leq m+n$,

$$x^p\ y^{m+n-p} = x^n(x^{p-n}\ y^{m+n-p}),$$

donc

$$\begin{aligned}(x-y)^{m+n} &= y^m\left(\sum_{p=0}^{p=n}(-1)^{m+n-p}\ \mathrm{C}_{m+n}^{p}\ x^p\ y^{n-p}\right)\\ &\quad +x^n\left(\sum_{p=n+1}^{p=m+n}(-1)^{m+n-p}\ \mathrm{C}_{m+n}^{p}\ x^{p-n}\ y^{m+n-p}\right)\end{aligned}$$

mais $y^m$ appartient à l'idéal $I$ donc

$$y^m\left(\sum_{p=0}^{p=n}(-1)^{m+n-p}\ \mathrm{C}_{m+n}^{p}\ x^p\ y^{n-p}\right)$$

est un élément de $I$, de même $x^n$ appartient à $I$, donc

$$x^n\left(\sum_{p=n+1}^{p=m+n}(-1)^{m+n-p}\ C_{m+n}^{p}\ x^{p-n}\ y^{m+n-p}\right)$$

est un élément de $I$, par suite $(x-y)^{m+n}$ appartient à $I$ donc $x-y$ est élément de $\sqrt{I}$.

Soit $a$ un élément de $A$, alors $(ax)^n = a^n x^n$ car l'anneau $A$ est commutatif, mais $x^n$ appartient à $I$ donc $a^n x^n$ est élément de $I$, par suite $ax$ appartient à $\sqrt{I}$, ce qui montre que $\sqrt{I}$ est un idéal de $A$.

2) Soit $x$ un élément de $\sqrt{I}$, alors il existe un entier $n$ tel que $x^n$ appartienne à $I$ ; comme $I \subset J$, $x^n$ appartient à $J$ donc $x$ est élément de $\sqrt{J}$ ce qui montre que $\sqrt{I} \subset \sqrt{J}$. Nous avons vu que $I \subset \sqrt{I}$, donc $\sqrt{I} \subset \sqrt{\sqrt{I}}$. Soit $y$ un élément de $\sqrt{\sqrt{I}}$ alors il existe un entier $p$ tel que $y^p$ appartienne à $\sqrt{I}$, mais comme $y^p$ est un élément de $\sqrt{I}$, il existe un entier $q$ tel que $(y^p)^q$ appartienne à $I$, donc $y^{pq}$ est élément de $I$ c'est-à-dire que $y$ appartient à $\sqrt{I}$ donc $\sqrt{\sqrt{I}} \subset \sqrt{I}$ d'où $\sqrt{\sqrt{I}} = \sqrt{I}$.

3) On a $I \cap J \subset I$ et $I \cap J \subset J$ donc $\sqrt{I \cap J} \subset \sqrt{I}$ et $\sqrt{I \cap J} \subset \sqrt{J}$, soit $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$. A présent soit $x$ un élément de $\sqrt{I} \cap \sqrt{J}$ ; alors il existe deux entiers $m$ et $n$ tels que $x^n$ appartienne à $I$ et $x^m$ à $J$. Puisque $x^n$ appartient à $I$, il en est de même de $x^m \cdot x^n$ ; puisque $x^m$ appartient à $J$, il en est de même de $x^m \cdot x^n$, par suite $x^{m+n}$ appartient à $I \cap J$ donc $x$ est élément de $\sqrt{I \cap J}$, donc $\sqrt{I} \cap \sqrt{J} \subset \sqrt{I \cap J}$ d'où $\sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J}$.

Soient $p$ et $q$ deux nombres entiers premiers entre eux.

1) Montrer que, quels que soient les entiers $y$, $z$, il existe un entier $x$ tel que $x \equiv y(\mod p)$ et $x \equiv z(\mod q)$.
   Démontrer que toutes les solutions sont congrues modulo $n = p\dot{q}$.
2) Soit $(\dot{y},\dot{z})$ un élément de $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$. Démontrer qu'il existez élément unique $\dot{x}$ de $\mathbb{Z}/n\mathbb{Z}$ tel que, si $x$ (resp. $y$,$z$) est un représentant $\dot{x}$ (resp. $\dot{y}$,$\dot{z}$) alors

$$x \equiv y(\mod p) \quad \text{et} \quad x \equiv z(\mod q).$$

3) Démontrer que l'application $f$ de $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ dans $\mathbb{Z}/n\mathbb{Z}$, qui à $(\dot{y},\dot{z})$ fait correspondre l'élément $\dot{x}$ défini ci-dessus, est un isomorphisme de l'anneau produit $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/qZ)$ sur l'anneau $\mathbb{Z}/n\mathbb{Z}$.
4) Soit $x$ un entier ; démontrer que la classe de $x$ modulo $p$ (resp. $q$) ne dépend que de la classe de $x$ modulo $n$. En déduire l'isomorphisme réciproque de $f$.

**Solution.**

1) Puisque les nombres $p$ et $q$ sont premiers entre eux, il existe des entiers $u$ et $v$ tels que :

$$pu + qv = 1. \tag{1.1}$$

   $x$ doit vérifier $y - x = kp$, $z - x = k'q$ où $k$ et $k'$ sont des entiers, soit $y - z = kp - k'q$, mais d'après (1.1), on a

$$y - z = (y - z)pu + (y - z)qv$$

   donc $k = (y - z)u$ et $k' = (y - z)v$, d'où

$$x = y - (y - z)up = z - (z - y)vq$$

   donc $x \equiv y(\mod p)$ et $x \equiv z(\mod q)$. Soit $x'$ une autre solution, on a : $y - x' = k_1 p$ et $z - x' = k_1' q$ où $k_1$ et $k_1'$ sont des entiers rationnels, alors

$$x - x' = (k_1 - k)\, p \quad \text{et} \quad x - x' = \left(k_1' - k'\right) q$$

   donc $x - x'$ est divisible par $p$ et par $q$. Comme $p$ et $q$ sont premiers entre eux, $x - x'$ est divisible par $p\dot{q} = n$ donc $x \equiv x'(\mod n)$.
2) Soit $y$ (resp. $z$) un représentant de $\dot{y}$ (resp. $\dot{z}$ ). On sait qu'il existe un élément $x$ de $\mathbb{Z}$ tel que $x \equiv y(\mod p)$ et $x \equiv z(\mod q)$ et toute autre solution est congrue à $x$ modulo $n$ ; donc $\dot{y}$ et $\dot{z}$ on donne un élément $\dot{x}$ de $\mathbb{Z}/n\mathbb{Z}$ et un seul, vérifiant la condition de l'énoncé ; en effet, si $y'$, $z'$ sont d'autres représentants de $\dot{y}$ et $\dot{z}$, on a $y' \equiv y(\mod p)$,$z' \equiv z(\mod q)$ donc $x \equiv y'(\mod p)$ et $x \equiv z'(\mod q)$, on retrouve donc les mêmes solutions.
3) On démontre d'abord que $f$ est un homomorphisme d'anneaux. Soient $(\dot{y},\dot{z})$ et $\left(\dot{y}',\dot{z}'\right)$ deux éléments de $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ et soient $y$,$z$,$y'$,$z'$ de représentants de $\dot{y}$,$\dot{z}$,$\dot{y}'$,$\dot{z}'$ respectivement. Soit $x$ (resp. $x'$) un entier tel que $x \equiv y(\mod p)$ et $x \equiv z(\mod q)$ ( resp. $x' \equiv y'(\mod p)$ et $\left(x' \equiv z'(\mod q)\right)$ alors on a

$$f\left[(\dot{y},\dot{z}) + \left(\dot{y}',\dot{z}'\right)\right] = f\left[\dot{y} + \dot{y}',\dot{z} + \dot{z}'\right],$$

or les quatre congruences précédentes montrent que

$$x+x^{'}\equiv y+y^{'}(\mod p),\quad x+x^{'}\equiv z+z^{'}(\mod q)$$

donc

$$f\left[\dot{y}+\dot{y}^{'},\dot{z}+\dot{z}^{'}\right]=x\dot{\frown}x'=\dot{x}+\dot{x}^{'}$$

d'où

$$f\left[(\dot{y},\dot{z})+\left(\dot{y}^{'},\dot{z}^{'}\right)\right]=f(\dot{y},\dot{z})+f\left(\dot{y}^{'},\dot{z}^{'}\right).$$

On a de même $xx^{'}\equiv yy^{'}(\mod p)$ et $xx^{'}\equiv zz^{'}(\mod q)$ donc

$$f\left[(\dot{y},\dot{z})\cdot\left(\dot{y}^{'},\dot{z}^{'}\right)\right]=f\left[\dot{y}\dot{y}^{'},\dot{z}^{'}\dot{z}^{'}\right]=\dot{\dot{x}}\dot{x}^{'}=\dot{x}\dot{x}^{'}=f(\dot{y},\dot{z})f\left(\dot{y}^{'},\dot{z}^{'}\right)$$

et $f$ est bien un homomorphisme d'anneaux.
Cet isomorphisme est injectif car si $(\dot{y},\dot{z})$ et $\left(\dot{y}^{'},\dot{z}^{'}\right)$ sont deux éléments de $(\mathbb{Z}/p\mathbb{Z})\times(\mathbb{Z}/q\mathbb{Z})$ tels que

$$f(\dot{y},\dot{z})=f\left(\dot{y}^{'},\dot{z}^{'}\right)$$

alors en posant $\dot{x}=f(\dot{y},\dot{z})$ et en choisissant des représentants $x,y,z,y^{'},z$ de $\dot{x},\dot{y},\dot{z},\dot{y}^{'},\dot{z}^{'}$ respectivement, on a $x\equiv y(\mod p),x\equiv z(\mod q),x\equiv y^{'}(\mod p)$ et $x\equiv z^{'}(\mod q)$ donc $y\equiv y^{'}(\mod p)$ et $z\equiv z^{'}(\mod q)$ soit $\dot{y}=\dot{y^{'}}$ et $\dot{z}=\dot{z}'$. Par ailleurs, on a card $(\mathbb{Z}/n\mathbb{Z})=n=\text{card}[(\mathbb{Z}/p\mathbb{Z})\times(\mathbb{Z}/q\mathbb{Z})]$ donc $(\mathbb{Z}/p\mathbb{Z})\times(\mathbb{Z}/q\mathbb{Z})$ sur $\mathbb{Z}/n\mathbb{Z}$.

4) Soient $x$ et $x^{'}$ deux entiers congrus modulo $n$ ; alors il existe un entier $k$ tel que $x=x^{'}+kn$, mais $n=p\dot{q}$ donc $x=x^{'}+(kq)p$ d'où $x\equiv x^{'}(\mod p)$ ; de même $x=x^{'}+(kp)q$ d'où $x\equiv x^{'}(\mod q)$. Soit $\dot{x}$ un élément de $\mathbb{Z}\ln Z_t$ soit $x$ un représentant de $\dot{x}$ ; on désigne par $(\dot{x})_p$ ( resp. $((\dot{x})_q)$ la classe de modulo $p$( resp. $q$). On vient de voir que ces classes ne dépendent que de $(\mathbb{Z}/p\mathbb{Z})\times(\mathbb{Z}/q\mathbb{Z})$ définie en posant pour tout élément $\dot{x}$ de $\mathbb{Z}/n\mathbb{Z}$ :

$$g(\dot{x})=((\dot{x})_p,(\dot{x})_q).$$

On calcule $f(g(\dot{x}))$ pour un élément $\dot{x}$ de $\mathbb{Z}/n\mathbb{Z}$ ; on a

$$f(g(\dot{x}))=f\left((\dot{x})_p,(\dot{x})\right)=\dot{x}$$

car si $x$ est un représentant de $\dot{x},x\equiv x(\mod p)$ et $x\equiv x(\mod q)$. Calculo $g[f(\dot{y},\dot{z})]$ pour un élément $(\dot{y},\dot{z})$ de $(\mathbb{Z}/p\mathbb{Z})\times(\mathbb{Z}/q\mathbb{Z})$; soit $x$ un entier que, si $y$ et $z$ sont des représentants de $\dot{y}$ et $\dot{z}$, on ait $x\equiv y(\mod p)$ et $x\equiv z(\mod q)$, alors $f(\dot{y},\dot{z})=\dot{x}$ et $g(f(\dot{y},\dot{z}))=g(\dot{x})$ or $x\equiv y(\mod p)$ donc $(\dot{x})_p=\dot{y}$, de même $x\equiv z(\mod q)$ donc $(\dot{x})_q=\dot{z}$ par suite $g(f(\dot{x},\dot{y}))=g(\dot{x})=(\dot{y},\dot{z})$. Ces deux résultats montrent que

$$g\circ f=\text{Id}[(\mathbb{Z}/p\mathbb{Z})\times(\mathbb{Z}/q\mathbb{Z})]\quad\text{et}\quad f\circ g=\text{Id}\,\mathbb{Z}/n\mathbb{Z}$$

donc $g$ est l'isomorphisme réciproque de $f$.

**Exercice 1.18** *Soit $p$ un entier naturel supérieur ou égal à 2. On considère dans $\mathbb{Z}$ la relation d'équivalence $\mathcal{R}$ définie par :*

$$x\mathcal{R}y \Rightarrow \exists k \in \mathbb{Z} \text{ tel que } x - y = kp.$$

*On note $\mathbb{Z}/p\mathbb{Z}$ l'ensemble des classes d'équivalence pour cette relation $\mathcal{R}$.*

*1) Quelle est la classe d'équivalence de 0 ? Quelle est celle de $p$ ?*

*2) Donner soigneusement la définition de l'addition usuelle et de la multiplication usuelle dans $\mathbb{Z}/p\mathbb{Z}$. On justifiera que ces définitions sont cohérentes.*

*3) On admet que, muni de ces opérations, $\mathbb{Z}/p\mathbb{Z}$ est un anneau. Démontrer que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si $p$ est premier.*

**Solution.**

1) Les classes d'équivalences de 0 et de $p$ sont toutes deux égales à l'ensemble des multiples de $p$, c'est-à-dire à $p\mathbb{Z}$.
2) Soit $(\bar{a},\bar{b}) \in (\mathbb{Z}/p\mathbb{Z})^2$. On pose $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \times \bar{b} = \overline{ab}$. Cette définition est cohérente car elle ne dépend pas des représentants a et b choisis pour $\bar{a}$ et $\bar{b}$.
3) On suppose $p$ premier. Alors $\mathbb{Z}/p\mathbb{Z}$ est commutatif et non réduit à $\{\bar{0}\}$ car $p \geq 2$. Soit $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ tel que $\bar{a} \neq \bar{0}$.
   $\bar{a} \neq \bar{0}$ donc $p$ ne divise pas $a$. Or $p$ est premier donc $p$ est premier avec $a$. Par la relation de Bézout, il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + pv = 1$ donc $\bar{a} \times \bar{u} = \bar{1}$. Donc $\bar{a}$ est inversible et $(\bar{a}^{-1} = \bar{u}$. Ainsi, les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles et finalement $\mathbb{Z}/p\mathbb{Z}$ est un corps.
   Supposons que $\mathbb{Z}/p\mathbb{Z}$ est un corps. Soit $k \in [\![2,p-1]\!]$. $\bar{k} \neq 0$ donc, comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, il existe $k' \in \mathbb{Z}$ tel que $\bar{k}\bar{k'} = \bar{1}$. C'est-à-dire il existe $v \in \mathbb{Z}$ tel que $kk' = 1 + vp$ c'est-à-dire $k'k - vp = 1$. Donc, d'après la relation de Bézout, $k \wedge p = 1$ et donc, comme $k \neq 1$, $k$ ne divise pas $p$. On en déduit que les seuls diviseurs positifs de $p$ sont 1 et $p$. Donc $p$ est premier.

**Exercice 1.19** *Déterminer les polynômes $P \in \mathbb{R}[X]$ tels que $X^n$ divise $X + 1 - P^2$.*

**Solution.** La fonction $x \mapsto \sqrt{1+x}$ est de classe $\mathcal{C}^\infty$ sur $]-1,1[$ donc admet un développement limité à l'ordre $n-1$ au voisinage de 0, de la forme $P_0(x) + O(x^n)$, avec

$$P_0 = \sum_{k=0}^{n-1} \frac{1/2(1/2-1)\cdots(1/2-k+1)}{k!} X^k$$

qui appartient à $\mathbb{R}_{n-1}[X]$.

On a

$$x + 1 - P_0(x)^2 = \left(\sqrt{x+1} - P_0(x)\right)\left(\sqrt{x+1} + P_0(x)\right) = \left(\sqrt{x+1} + P_0(x)\right) O\left(x^n\right)$$

donc $x+1-P_0(x)^2 = O\left(x^n\right)$ quand $x \to 0$. On en déduit que 0 est racine du polynôme $X + 1 - P_0^2$ avec un ordre de multiplicité au moins égal à $n$, donc ce polynôme est divisible par $X^n$.

On remarque que si $P$ est une solution, alors $P(0)^2 = 1$ et $-P$ est aussi une solution. On supposera désormais, quitte à changer $P$ en $-P$, que $P$ est un polynôme solution tel que $P(0) = 1$. On pose $P = a_0 + a_1X + \cdots + a_pX^p$, avec $a_0 = 1$. On a $X + 1 - P^2 = 1 + X - \sum_{0\leqslant i,j\leqslant p} a_ia_jX^{i+j}$. Les coefficients de degré inférieur ou égal à $n-1$ de ce polynôme doivent être nuls, d'où $a_1 = \frac{1}{2}$ et $\forall k \in [\![2,n-1]\!]$, $2a_k + \sum_{1\leqslant i\leqslant k-1} a_ia_{k-i} = 0$. On en déduit que $p \geqslant n-1$ et que chaque coefficient $a_k$, pour $k \leqslant n-1$, est déterminé de façon unique à l'aide des précédents. L'ensemble des solutions est donc $\pm P_0 + X^n\mathbb{R}[X]$, où $P_0$ est le développement limité à l'ordre $n-1$ au voisinage de 0 de $\sqrt{1+x}$.

**Exercice 1.20** *On considère $P = \sum_{k=0} b_kX^k$ avec $0 < b_0 < \ldots < b_n$ et $Q = (X-1)P$. Montrer que si $z$ est une racine complexe de $P$, alors $Q(|z|) \leqslant 0$, et en déduire que $|z| \leqslant 1$.*

**Solution.** Après développement, on a $Q = b_nX^{n+1} + \sum_{k=1}^{n}(b_{k-1} - b_k)X^k - b_0$.
Si $P(z) = 0$, alors $Q(z) = 0$, donc $b_nz^{n+1} = \sum_{k=1}^{n}(b_k - b_{k-1})z^k + b_0$, d'où par inégalité triangulaire $b_n|z|^{n+1} \leqslant \sum_{k=1}^{n}(b_k - b_{k-1})|z|^k + b_0$ car les coefficients mis en jeu sont positifs. On en déduit l'inégalité $Q(|z|) \leqslant 0$.
Comme $b_0 > 0$, on a $z \neq 0$, d'où $P(|z|) > 0$ car les coefficients de $P$ sont strictement positifs. Comme on a $Q(|z|) \leqslant 0$, on en déduit que $|z| - 1 \leqslant 0$.

**Exercice 1.21** *Déterminer les polynômes $P \in \mathbb{R}[X]$ tels que $P'$ divise $P$.*

Soit $P$ de degré $n$ tel que $P'$ divise $P$. Dans ce cas, $P'$ est de degré $n-1$ et son coefficient dominant est égal à $n$ fois celui de $P$, donc il existe $a \in \mathbb{R}$ tel que $nP = (X-a)P'$, c'est-à-dire $\frac{P'}{P} = \frac{n}{X-a}$. L'expression de la décomposition en éléments simples de $\frac{P'}{P}$ dans $\mathbb{C}[X]$ et son unicité entraînent que $a$ est la seule racine de $P$ dans $\mathbb{C}$, donc $P = \lambda(X-a)^n$. Inversement, de tels polynômes conviennent.

**Exercice 1.22** *Soit $P \in \mathbb{R}[X]$ scindé à racines simples dans $\mathbb{R}[X]$. Montrer que $P$ ne peut avoir deux coefficients consécutifs nuls.*

On note $P = \sum_{j=0}^{n} a_jX^j$ avec $a_n \neq 0$. On raisonne par l'absurde en supposant qu'il existe $k \leqslant n-1$ tel que $a_k = a_{k+1} = 0$. On a alors $n \geqslant 3$. En appliquant le théorème de Rolle à $P$ dans chaque intervalle formé de deux racines consécutives de $P$, on obtient ainsi $n-1$ racines distinctes de $P'$ qui est de degré $n-1$, donc $P'$ est également simplement scindé dans $\mathbb{R}[X]$. On en déduit par récurrence que $P^{(k)}$ est simplement scindé dans $\mathbb{R}[X]$. Or

$$P^{(k)} = \sum_{j=k+2}^{n} j(j-1)\cdots(j-k+1)a_jX^{j-k}$$

qui est divisible par $X^2$, donc 0 est racine double de $P^{(k)}$, ce qui entraîne une contradiction.

**Exercice 1.23** *Soit $(P,Q) \in \mathbb{Q}[X]^2$. Démontrer l'équivalence entre les assertions suivantes :*

– *Les polynômes $P$ et $Q$ sont premiers entre eux dans $\mathbb{C}[X]$.*

– *Les polynômes $P$ et $Q$ sont premiers entre eux dans $\mathbb{Q}[X]$.*

**Solution.**

– Si $P$ et $Q$ sont premiers entre eux dans $\mathbb{C}[X]$, alors ils ne peuvent pas avoir de diviseur commun dans $\mathbb{Q}[X]$ non constant (car ce serait également un diviseur dans $\mathbb{C}[X]$ ) donc ils sont premiers entre eux dans $\mathbb{Q}[X]$.
– Si $P$ et $Q$ sont premiers entre eux dans $\mathbb{Q}[X]$, alors il existe grâce au théorème de Bézout deux polynômes $U$ et $V$ dans $\mathbb{Q}[X]$ tels que $UP+VQ = 1$. Ceci constitue également une relation de Bézout dans $\mathbb{C}[X]$, donc $P$ et $Q$ sont premiers entre eux dans $\mathbb{C}[X]$.

**Exercice 1.24** *Montrer que tout polynôme irréductible de $\mathbb{Q}[X]$ n'a que des racines simples dans $\mathbb{C}$.*

**Solution.** On applique le résultat de l'exercice précédent aux polynômes $P$ et $P'$, qui appartiennent à $\mathbb{Q}[X]$. Comme $P$ est irréductible dans $\mathbb{Q}[X]$ et que $P'$ est de degré inférieur à celui de $P$, leur PGCD dans $\mathbb{Q}[X]$ est un diviseur strict de $P$, donc $P$ et $P'$ sont premiers entre eux dans $\mathbb{Q}[X]$. En conséquence, ils sont également premiers entre eux dans $\mathbb{C}[X]$, ce qui signifie exactement que $P$ et $P'$ n'ont pas de racines communes, c'est-à-dire que les racines de $P$ dans $\mathbb{C}$ sont simples.

## 1.8 Problèmes résolus

**Problème 1.1** *(Sous-groupes additifs de $\mathbb{R}$ )*

*1) Soit $G$ un sous-groupe additif de $\mathbb{R}$ et $m = \inf(G \cap \mathbb{R}_+^*)$.*

*a) Montrer que si $m > 0$, alors $G = m\mathbb{Z}$.*
*b) Montrer que si $m = 0$, alors $G$ est dense dans $\mathbb{R}$.*

*2) Soient $(x,y) \in \mathbb{R}\times\mathbb{R}_+^*$ et $H$ le sous-groupe de $(\mathbb{R},+)$ engendré par $x$ et $y$. Montrer que les propriétés suivantes sont équivalentes.*

*i) $\exists m \in \mathbb{R}$, tel que $G = m\mathbb{Z}$.*
*ii) $\frac{x}{y} \in \mathbb{Q}$.*

*3) Soit $r$ un nombre irrationnel. Pour tout $n \in \mathbb{N}$, on pose $u_n = nr - E(nr)$.*

*a) Montrer que l'ensemble $E = \{u_n = nr - E(nr) \mid n \in \mathbb{Z}\}$ est dense dans $[0,1]$.*
*b) Montrer que $0$ est un point d'accumulation de l'ensemble $F = \{u_n \mid n \in \mathbb{N}\}$ et que $F$ est dense dans $[0,1]$.*

**Solution.**

1) (a) On suppose que $m > 0$. Il résulte de la caractérisation de la borne inférieure qu'il existe $a \in G \cap \mathbb{R}_+^*$ tel que

$$m \leq a \leq m + \frac{m}{2} < 2m$$

Si $m < a$, alors il existe $b \in G \cap \mathbb{R}_+^*$ tel que : $m \leq b < a < 2m$. Donc, si on pose $x = a - b$, alors $x \in G$ et $0 < x < 2m - b \leq m$, ceci contredit le fait que $m = \inf G \cap \mathbb{R}_+^*$. Par suite, $m = a \in G$. D'où $m\mathbb{Z} \subset G$.
Réciproquement, soit $x \in G$ ; on pose $n = E\left(\frac{x}{m}\right)$. On a :
$nm \leq x < (n+1)m$. Par la suite $0 \leq x - nm < m$ puisque $x - nm \in G$ et $m = \inf(G \cap \mathbb{R}_+^*)$, alors on a $x - nm = 0$ c'est-à-dire $x = nm \in m\mathbb{Z}$. Ce qui montre que $G = m\mathbb{Z}$.

(b) Supposons que $m = 0$ et on montre que $G$ est un ensemble dense dans $\mathbb{R}$. En effet, soient $(a,b) \in \mathbb{R}^2$ tel que $a < b$. Montrons que $]a,b[ \cap G \neq \emptyset$.
Puisque $b - a > 0$, alors il existe $x \in G$ tel que $0 < x < b - a$. Posons $n = E(a/x)$, on a $nx \leq a < (n+1)x$. Donc

$$0 < (n+1)x - a = (nx - a) + x \leq x < b - a.$$

Par conséquent $a < (n+1)x < b$. Comme $(n+1)x \in G$, alors
$(n+1)x \in ]a,b[ \cap G$.
On en déduit que $]a,b[ \cap G \neq \emptyset$, c'est-à-dire que $G$ est dense dans $\mathbb{R}$.

2) Soient $x$ et $y$ des nombres réels tel que $y \neq 0$. Considérons le sous-groupe $H$ de $(\mathbb{R},+)$ engendré par $x$ et $y$. On a $H = x\mathbb{Z} + y\mathbb{Z}$.
Montrons (i)⇒(ii) Supposons qu'il existe $m \in \mathbb{R}$ tel que $H = m\mathbb{Z}$. Alors il existe un couple d'entiers $(p,q) \in \mathbb{Z}^2$ tel que

$$x = mp \text{ et } y = mq \ (q \neq 0).$$

D'où

$$\frac{x}{y} = \frac{p}{q} \in \mathbb{Q}.$$

Montrons (ii)⇒(i).
Si $\frac{x}{y} \in \mathbb{Q}$, il existe $(p,q) \in \mathbb{Z}^2$ avec $q \neq 0$, tel que $\frac{x}{y} = \frac{p}{q}$. Donc,

$$x\mathbb{Z} + y\mathbb{Z} = y(\frac{x}{y}\mathbb{Z} + \mathbb{Z}) = y(\frac{p}{q}\mathbb{Z} + \mathbb{Z})$$

Soit,

$$x\mathbb{Z} + y\mathbb{Z} = \frac{y}{q}(p\mathbb{Z} + q\mathbb{Z}).$$

Puisque $p$ et $q$ sont premiers entre eux, alors $(p\mathbb{Z}+q\mathbb{Z}) = \mathbb{Z}$. Par conséquent, on a

$$x\mathbb{Z} + y\mathbb{Z} = \frac{y}{q}\mathbb{Z} = m\mathbb{Z}$$

avec $m = y/q$.

3) a) Soit $G = \{nr + m,(n,m) \in \mathbb{Z}^2\}$ le sous-groupe de $(\mathbb{R},+)$ engendré par $r$ et 1. Puisque $r \notin \mathbb{Q}$, alors $G$ est dense dans $\mathbb{R}$. En particulier, $G$ est dense dans l'intervalle $[0,1]$.
Pour $x = nr + m \in G$, on a :

$$x \in [0,1[ \Leftrightarrow -m \leq nr < -m + 1 \Leftrightarrow m = -E(nr),$$

soit,

$$x \in [0,1[ \Leftrightarrow x = nr - E(nr) \in E$$

Donc $G \cap [0,1[ = E$. Ce qui prouve que $E$ est dense dans $[0,1]$.

b) Montrons que 0 est un point d'accumulation de $F$. En utilisant la densité de $E$ dans $[0,1]$, on obtient que pour tout $\varepsilon > 0$ tel que $0 < \varepsilon < 1$, il existe $n \in \mathbb{Z}$ tel que $0 < nr - E(nr) < \varepsilon$.
Si $n < 0$, alors

$$E(nr) < nr < E(nr) + 1 \ (r \notin \mathbb{Q}).$$

D'où $-E(nr) - 1 < -nr < -E(nr)$. Par suite $E(-nr) = -E(nr) - 1$. Puisque $0 < nr - E(nr) < \varepsilon$ ; alors on a

$$0 < nr - E(nr) = nr + E(-nr) + 1 < 1$$

Soit

$$1 - \varepsilon < u_{-n} = -nr - E(-nr) = -nr + E(nr) + 1 < 1.$$

Ceci montre que 1 est un point d'accumulation de $F$; donc, il existe $p \geq -n$ tel que $u_{-n} < u_p < 1$, soit $1 - u_p < 1 - u_{-n}$, donc

$$0 < u_p - u_{-n} < 1 - u_{-n} < \varepsilon < 1.$$

Et puisque $E(pr) - E(-nr) = E(pr) + E(nr) + 1$, alors

$$E(pr) - E(-nr) \leq (p + n)r < E(pr) + E(nr) + 2.$$

La première inégalité est stricte car $r \notin \mathbb{Q}$. Donc

$$E(pr) - E(-nr) < (p + n)r < E(pr) - E(-nr) + 1.$$

Ce qui montre que l'on a

$$E\left((p + n)r\right) = E(pr) - E(-nr).$$

Comme $p + n \in \mathbb{N}$, et

$$0 < u_{n+p} = (n + p)r - E\left((p + n)r\right) = u_p - u_{-n} < \varepsilon.$$

on a

$$u_{p+n} \in ]0,\varepsilon[ \cap F;$$

donc 0 est un point d'accumulation de $F$.

Il reste à montrer que $F$ est dense dans $[0,1]$. Soient $x \in ]0,1[$ et $\varepsilon > 0$. Il existe $p \in \mathbb{N}$ tel que $0 < u_p < \varepsilon$. Posons

$$q = E\left(\frac{x}{u_p}\right).$$

Alors $0 \leq qu_p < x < 1$. Soit,

$$0 \leq qpr - qE(pr) < x < 1,$$

ou encore

$$qE(pr) \leq qpr < qE(pr) + 1.$$

Ceci montre que $E(qpr) = qE(pr)$. Par conséquent,

$$u_{qp} = qpr - E(qpr) = q\,(pr - E(pr)) = qu_p.$$

Par suite

$$0 < x - qu_p = x - u_{qp} < u_p < \varepsilon.$$

On a montré que, pour tout $x \in ]0,1[$, il existe $n \in \mathbb{N}$ tel que
$0 < x - u_n < \varepsilon$. Donc $x$ est un point adhérent à $F$. Puisque 0 et 1 sont des points d'accumulation de $F$, alors $F$est dense dans $[0,1]$.

# Chapitre 2

# Réduction des endomorphismes et des matrices carrées

## 2.1 Compléments d'algèbre linéaire

**Définition 2.1 (Somme)** *La somme de n sous-espaces vectoriels $F_1$,$F_2$,...,$F_n$ d'un $\mathbb{K}$-espace vectoriel E est l'ensemble de tout élément qui s'écrit comme somme d'éléments de $F_1$,$F_2$,...,$F_n$.*

**Définition 2.2 (Somme directe)** *La somme de n sous-espaces vectoriels $F_1$,$F_2$,...,$F_n$ d'un $\mathbb{K}$-espace vectoriel E est dite directe si et seulement si tout élément de $F1 + F2 + \cdots + F_n$ s'écrit d'une manière unique comme somme d'éléments de $F_1$,$F_2$,...,$F_n$.*

La somme directe de $F_1$,$F_2$,...,$F_n$ est notée : $F_1 \oplus F_2 \oplus \cdots \oplus F_n$.

**Théorème 2.1** *Si $F_1$,...,$F_p$ sont des sous-espaces de dimension finie,*

$$\dim\left(\sum_{i=1}^{p} F_i\right) \leq \sum_{i=1}^{p} \dim(F_i)$$

*avec égalité si et seulement si la somme est directe.*

**Théorème 2.2** *Si $E_1$,...,$E_p$ sont des sous-espaces de E tels que $E = \oplus E_i$ et si $u_i \in \mathcal{L}(E_i,F)$ pour tout i, alors il existe une et une seule $u \in \mathcal{L}(E,F)$ telle que $u_{|E_i} = u_i$ pour tout i.*

**Définition 2.3 (Matrice définie par blocs)** *Une matrice définie par blocs est une matrice pouvant être divisée en matrices rectangulaires de dimensions inférieures appelées blocs.*

**Théorème 2.3 (Déterminant d'une matrice triangulaire par blocs.)** *Soit A une matrice de $\mathcal{M}_{n+p}(\mathbb{K})$ de la forme $\begin{pmatrix} A_1 & A_2 \\ O & A_3 \end{pmatrix}$ où $A_1$ est un élément de $\mathcal{M}_n(\mathbb{K})$, $A_3$ un élément de $\mathcal{M}_p(\mathbb{K})$ et O la matrice nulle de $\mathcal{M}_{p,n}(\mathbb{K})$. Alors*

$$\det(A) = \det(A_1)\det(A_3).$$

## 2.2 Éléments propres d'un endomorphisme, d'une matrice carrée

**Définition 2.4** • $\lambda \in K$ *est une valeur propre de* $u$ *si et seulement si* $\exists v \in E$, $v \neq 0$ *:* $u(v) = \lambda v$.
• $v \in E$ *est dit vecteur propre de* $u$ *si et seulement si* $v \neq 0$ *et* $\exists \lambda \in K$ : $u(v) = \lambda v$.
• $E_u(\lambda) := \operatorname{Ker}(u - \lambda Id)$ *est dit sous-espace propre de* $u$ *associé à* $\lambda$.

**Définition 2.5 (Spectre d'un endomorphisme)** *Le spectre d'un endomorphisme d'un espace de dimension finie est l'ensemble de ses valeurs propres.*

**Théorème 2.4** *La somme d'une famille finie de sous-espaces propres est directe.*

**Théorème 2.5** *Toute famille de vecteurs propres associés à des valeurs propres deux à deux distinctes est libre.*

**Théorème 2.6** *Le spectre d'un endomorphisme d'un espace de dimension finie* $n$ *est fini de cardinal au plus* $n$.

**Théorème 2.7** *Si deux endomorphismes* $u$ *et* $v$ *commutent, alors tout sous-espace propre de* $u$ *est stable par* $v$.

## 2.3 Polynôme caractéristique

$E$ est un $\mathbb{K}$-espace vectoriel, $\dim E = n$ et $u \in (E)$.

**Définition 2.6 (Polynôme caractéristique)** *On appelle le polynôme caractéristique de* $u$: $P_u(X) = \det(mat_e u - XI)$.

**Théorème 2.8** *On a :*

$$P_u(X) = (-1)^n X^n + (-1)^{n-1} Tr(mat_e u) X^{n-1} + \cdots + \det(mat_e u)$$

*où* $Tr$ *est la trace d'une matrice, i.e. somme des éléments de sa diagonale.*

**Théorème 2.9** *Si* $P_u$ *ne dépend pas de la base* $e$ *alors* $S_P u = \{\lambda \in K \mid P_u(\lambda) = 0\}$

**Corollaire 2.1** *On a les deux résultats suivants :*
*1)* $S_P(u)$ *a au plus* $n$ *éléments.*
*2)* $S_P(u)$ *a au moins un élément si* $K = \mathbb{C}$.

**Théorème 2.10** *Si* $\lambda \in S_P u$ *est d'ordre* $m$ *(i.e. racine de* $P_u$ *de multiplicité* $m$*) alors* $1 \leq \dim E_u(\lambda) \leq m$.

Le polynôme caractéristique d'une matrice est celui de son endomorphisme.

**Exemple 2.1** Eléments propres de $A = \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix}$ :

$P_A(\lambda) = \begin{vmatrix} 2-\lambda & 1 \\ 4 & 2-\lambda \end{vmatrix} = (2-\lambda)^2 - 2^2 = 0 \Leftrightarrow \begin{cases} \lambda = 0 \\ \lambda = 4 \end{cases} \Rightarrow S_P A = \{0,4\}$.

$E_A(0) = \text{Ker } u_A = \{x : u_A(x) = 0\}, u_A(x) = 0 \Leftrightarrow AX = 0 \Leftrightarrow 2x_1 + x_2 = 0$.

D'où $v_1 = (1,-2)^t$ est le vecteur propre associé à la valeur propre $\lambda_1 = 0$.

$E_A(4) = \text{Ker } (u_A - 4Id), x \in E_A(4) \Leftrightarrow AX = 4X \Leftrightarrow 2x_1 - x_2 = 0$.

D'où $v_2 = (1,2)^t$ est le vecteur propre associé à la valeur propre $\lambda_2 = 4$.

**Théorème 2.11** *Si deux matrices sont semblables alors elles ont même polynôme caractéristique.*

**Remarque 2.1** 1) Le polynôme caractéristique est unitaire.

2) La dimension du sous-espace propre associé à $\lambda$ est majorée par la multiplicité de $\lambda$.

## 2.4 Endomorphismes et matrices carrées diagonalisables

**Définition 2.7** *Un endomorphisme d'un espace vectoriel $E$ de dimension finie est dit diagonalisable s'il existe une base de $E$ dans laquelle sa matrice est diagonale.*

**Théorème 2.12** *Pour qu'un endomorphisme soit diagonalisable, il faut et il suffit que la somme de ses sous-espaces propres soit égale à $E$.*

**Définition 2.8** *Une matrice carrée est dite diagonalisable si elle est semblable à une matrice diagonale.*

**Théorème 2.13** *Pour qu'une matrice carrée soit diagonalisable, il faut et il suffit que l'endomorphisme canoniquement associé soit diagonalisable.*

**Théorème 2.14** *Pour qu'un endomorphisme $u$ soit diagonalisable, il faut et il suffit que $P_u$ soit scindé et que, pour toute valeur propre de $u$, la dimension de l'espace propre associé soit égale à sa multiplicité.*

## 2.5 Endomorphismes et matrices carrées trigonalisables

**Définition 2.9** • *Un endomorphisme est dit trigonalisable s'il existe une base dans laquelle sa matrice est triangulaire supérieure.*

- *Une matrice carrée est dite trigonalisable si elle est semblable à une matrice triangulaire supérieure.*

**Théorème 2.15** *Pour qu'une matrice carrée soit trigonalisable, il faut et il suffit que l'endomorphisme canoniquement associé le soit.*

**Théorème 2.16** *Un endomorphisme est trigonalisable si et seulement si son polynôme caractéristique est scindé.*

## 2.6 Endomorphismes nilpotents, matrices nilpotentes

**Définition 2.10 (Endomorphisme nilpotent)** *$u \in \mathcal{L}(E)$ est dit nilpotent si il existe $k$ entier naturel non nul tel que : $u^k = 0$.*

dans le cas où $i = \min\{k \in \mathbb{N}^* \mid u^k = 0\}$ est dit indice de nilpotence.

**Définition 2.11 (Matrice nilpotente)** *Une matrice carrée $A$ est dite nilpotente si son endomorisme canonique $u_A$ l'est.*

**Théorème 2.17** *Un endomorphisme est nilpotent si et seulement s'il est trigonalisable avec pour seule valeur propre* 0.

**Théorème 2.18** *L'indice de nilpotence est majoré par la dimension de $E$.*

## 2.7 Polynômes d'un endomorphisme, d'une matrice carrée

**Théorème 2.19** *Pour $u$ dans $\mathcal{L}(E)$, morphisme d'algèbres $P \mapsto P(u)$ de $\mathbb{K}[X]$ dans $\mathcal{L}(E)$. Le noyau de ce morphisme est l'idéal annulateur de $u$. Son image est la sous-algèbre commutative $\mathbb{K}[u]$ de $\mathcal{L}(E)$.*

**Théorème 2.20** *Si $d$ est le degré du polynôme minimal, alors la famille $(u^k)_{0 \leq k \leq d-1}$ est une base de $\mathbb{K}[u]$.*

**Théorème 2.21** *Si $P$ annule $u$, toute valeur propre de $u$ est racine de $P$.*

## 2.8 Lemme de décomposition des noyaux

**Lemme 2.1** *Si $P_1, \ldots, P_r$ sont des éléments de $\mathbb{K}[X]$ deux à deux premiers entre eux de produit égal à $P$, alors on a :*

$$\mathrm{Ker}(P(u)) = \bigoplus_{i=1}^{r} \mathrm{Ker}(P_i(u)).$$

## 2.9 Polynômes annulateurs et réduction

**Théorème 2.22** *Un endomorphisme $u$ est diagonalisable si et seulement s'il existe un polynôme scindé à racines simples annulant $u$, ou encore si et seulement si son polynôme minimal est scindé à racines simples.*

**Théorème 2.23** *Un endomorphisme est trigonalisable si et seulement s'il annule un polynôme scindé, ou encore si et seulement si son polynôme minimal est scindé.*

## 2.10 Théorème de Cayley-Hamilton et sous-espaces caractéristiques

**Théorème de Cayley-Hamilton 1**
*Soient $E$ un $\mathbb{K}$-espace vectoriel,* $\dim E = n$, $u \in \mathcal{L}(E)$ *et* $A \in \mathcal{M}_n(\mathbb{K})$. *On a*

1) $P_u(u) = 0$.
2) $P_A(A) = 0$.

**Théorème 2.24** *S'il existe un polynôme scindé annulant $u$, décomposition de $E$ en somme directe de sous-espaces stables par $u$ sur chacun desquels $u$ induit la somme d'une homothétie et d'un endomorphisme nilpotent.*

## 2.11 Exercices résolus

**Exercice 2.1** *Soit $E$ un espace vectoriel de dimension $n$ et $u$ un endomorphisme de $E$ ayant $n$ valeurs propres distinctes $\{\lambda_1, \ldots, \lambda_n\}$.*

1) *Montrer que l'ensemble* $\mathrm{Com} = \{v \in \mathcal{L}(E,E) \mid uv = vu\}$ *des endomorphismes de $E$ qui commutent avec $u$ est un espace vectoriel.*
2) a) *Soit $v$ un élément de* Com. *Montrer que $v$ préserve les espaces propres de $u$ (c'est à dire que si $E_\lambda$ est un espace propre de $u$ associé à la valeur propre $\lambda$, on a $\forall x \in E_\lambda$, $v(x) \in E_\lambda$).*
   b) *Donner la dimension des espaces propres de $u$ et montrer que si $x$ est un vecteur propre de $u$ alors c'est aussi un vecteur propre de $v$.*
   c) *A l'aide d'une base convenablement choisie, décrire tous les éléments de* Com, *et montrer que* Com *est de dimension $n$.*
3) *Montrer que* $\mathrm{Vect}(id,u,u^2,\ldots,u^{n-1}) \subset \mathrm{Com}$.
4) *On veut maintenant étudier l'indépendance linéaire de la famille $\{id,u,u^2,\ldots,u^{n-1}\}$. Pour cela, on considère $n$ réels $\alpha_0,\ldots,\alpha_{n-1}$ tels que* $\sum_{i=0}^{n} \alpha_i u^i = 0$.
   a) *Montrer que les $(\alpha_i)$ sont solution du système suivant :*

$$\left\{\begin{array}{ccccccccccc} \alpha_0 & + & \alpha_1\lambda_1 & + & \alpha_2\lambda_1^2 & + & \ldots & + & \alpha_{n-1}\lambda_1^{n-1} & = & 0 \\ \alpha_0 & + & \alpha_1\lambda_2 & + & \alpha_2\lambda_2^2 & + & \ldots & + & \alpha_{n-1}\lambda_2^{n-1} & = & 0 \\ \vdots & & \vdots & & \vdots & & & & \vdots & & \vdots \\ \alpha_0 & + & \alpha_1\lambda_n & + & \alpha_2\lambda_n^2 & + & \ldots & + & \alpha_{n-1}\lambda_n^{n-1} & = & 0 \end{array}\right. \tag{2.1}$$

*b) On rappelle que :* $\begin{vmatrix} 1 & \lambda_1 & \lambda_1^2 & \dots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \lambda_2^2 & \dots & \lambda_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \dots & \lambda_n^{n-1} \end{vmatrix} = \prod_{1 \le i < j \le n} (\lambda_j - \lambda_i)$. *En déduire l'ensemble des solutions du système (2.1) et conclure.*

*5) Montrer que* $\mathrm{Com} = \mathrm{Vect}(id, u, u^2, \dots, u^{n-1})$.

**Solution.**

1) Soit $(v,w) \in \mathrm{Com}$, $(\lambda,\mu) \in \mathbb{R}^2$.
$u(\lambda v + \mu w) = \lambda uv + \mu uw = \lambda vu + \mu wu = (\lambda v + \mu w)u$. Donc Com est un sous-espace vectoriel de $\mathcal{L}(E,E)$.

2) a) Soit $x \in E_\lambda$. $u(v(x)) = uv(x) = vu(x) = v(\lambda x) = \lambda v(x)$ donc $v(x) \in E_\lambda$.

   b) Chaque valeur propre est de multiplicité 1, donc chaque espace propre est de dimension 1. Ainsi, si $x \in E_\lambda \setminus \{0\}$, $E_\lambda = \mathbb{R}.x$. Comme $v(x) \in E_\lambda$, $\exists \alpha \in \mathbb{R}$, $v(x) = \alpha x$. Donc $x$ est un vecteur propre de $v$.

   c) Soit $(e_1, \dots, e_n)$ une base de vecteurs propres de $u$. C'est aussi une base de vecteurs propres pour tout élément de Com. Tout élément de Com est donc représenté par une matrice diagonale dans $(e_1, \dots, e_n)$. Réciproquement, tout endomorphisme représenté dans cette base par une matrice diagonale commute avec $u$. Donc

$$\mathrm{Com} = \{v \in \mathcal{L}(E,E), \exists(\alpha_1, \dots, \alpha_n) \in \mathbb{R}^n, M_{v/(e_1,\dots,e_n)} = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix}\}$$

   On en déduit que Com est de dimension $n$.

3) $u\,u^i = u(u \cdots u) = (u \cdots u)u = u^i\,u$. Donc $\forall i \in \{0, \dots, n-1\}, u^i \in \mathrm{Com}$. Ainsi $\mathrm{Vect}(\mathrm{id}, u, \dots, u^{n-1}) \subset \mathrm{Com}$.

4) a) Soit $x_k \in E_{\lambda_k} \setminus \{0\}$. $u^i(x) = \lambda_k^i\, x$. Donc

$$(\sum \alpha_i u^i)x = \sum \alpha_i u^i(x) = (\sum \alpha_i \lambda_k^i)x = 0.$$

   Par conséquent $\forall k \in \{1, \dots, n\}, \sum \alpha_i \lambda_k^i = 0$.

   b) Le déterminent du système (2.1) est non nul. C'est un système de Cramer, il existe une solution unique, $\alpha_0 = \dots = \alpha_{n-1} = 0$. La famille $(\mathrm{id}, u, \dots, u^{n-1})$ est donc libre.

5) On a $\dim \mathrm{Vect}(\mathrm{id}, u, \dots, u^{n-1}) = n = \dim \mathrm{Com}$ et $\mathrm{Vect}(\mathrm{id}, u, \dots, u^{n-1}) \subset \mathrm{Com}$ donc $\mathrm{Vect}(\mathrm{id}, u, \dots, u^{n-1}) = \mathrm{Com}$.

**Exercice 2.2** *Énoncer le théorème de Cayley-Hamilton. Le démontrer dans le cas particulier où le polynôme caractéristique est scindé à racines simples.*

**Solution.** Soit $u$ un endomorphisme d'un espace vectoriel $E$ de dimension finie, alors le polynôme caractéristique de $u$ est aussi un polynôme annulateur de $u$.

Si $\chi_u$ est scindé à racines simples : $u$ est alors diagonalisable et il existe donc une base $B$ dans laquelle $Mat_B(u) = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$.

Alors $Mat_B(\chi_u(u)) = \begin{pmatrix} \chi_u(\lambda_1) & & \\ & \ddots & \\ & & \chi_u(\lambda_n) \end{pmatrix}$. Et comme $\forall i \in \{1,\dots,n\}$ on a $\chi_u(\lambda_i) = 0$, on en déduit que $\chi_u(u) = 0$.

**Exercice 2.3** *La matrice $A$ suivante est-elle diagonalisable, triangularisable ? Effectuer explicitement la réduction.*

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

**Solution.** $\chi_A = (-1-X)(2-X)^2$. Donc $A$ est diagonalisable si et seulement si $\dim \mathrm{Ker}(A-2I) = 2$. Or $\mathrm{rg}(A-2I) = 2$, donc $\dim \mathrm{Ker}(A-2I) = 1$ donc $A$ n'est pas diagonalisable. Cependant, $\chi_A$ est scindé sur $\mathbb{R}$ donc $A$ est triangularisable sur $\mathbb{R}$.

$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathrm{Ker}(A+I) \iff \begin{cases} 4x+2y+4z &= 0 \\ -x+4y-z &= 0 \\ -2x-y-2z &= 0 \end{cases} \iff \begin{cases} x+z &= 0 \\ y &= 0 \end{cases}$ donc $\mathrm{Ker}(A+I) = \mathbb{R}\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$.

De même,

$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathrm{Ker}(A-2I)$ si et seulement si $\begin{cases} x+2y+4z=0 \\ -x+y-z=0 \\ -2x-y-5z=0 \end{cases}$ si et seulement si $\begin{cases} x=2y \\ z=-y \end{cases}$ donc $\mathrm{Ker}(A+I) = \mathbb{R}\begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix}$

On sait que $\mathrm{Ker}((A-2I)^2)$ est de dimension 2, et que $\begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix} \in \mathrm{Ker}(A-2I) \subset \mathrm{Ker}((A-2I)^2)$. On cherche donc un deuxième vecteur dans $\mathrm{Ker}((A-2I)^2)$, linéairement indépendant de $\begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix}$.

$(A-2I)^2 = \begin{pmatrix} -9 & 0 & -18 \\ 0 & 0 & 0 \\ 9 & 0 & 18 \end{pmatrix}$ donc $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ convient. De plus :

$A\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix} + 2\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$.

Donc en posant $P = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ -1 & -1 & 0 \end{pmatrix}$, on obtient $P^{-1}AP = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$.

**Exercice 2.4** *Soit $J = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ et $A = \left(\begin{array}{c|c} 0 & J \\ \hline J & 0 \end{array}\right)$. Calculer $A^2$, puis $A^3$. A l'aide d'un polynôme annulateur de $A$, montrer que $A$ est diagonalisable.*

*Sans chercher à calculer le polynôme caractéristique de $A$, donner un ensemble fini contenant toutes les valeurs propres de $A$, puis donner les valeurs valeurs propres elles mêmes ainsi que leurs multiplicités. En déduire le polynôme caractéristique de $A$.*

**Solution.** On a $A^3 = A$, donc $P = X^3 - X = (X-1)(X+1)X$ est un polynôme annulateur de $A$. Il s'agit d'un polynôme scindé à racine simples donc $A$ est diagonalisable. Les valeurs propres de $A$ sont des racines de $P$ donc $\mathrm{Sp}(A) \subset \{0,1,-1\}$. On a $\mathrm{rg}\, A = 2$ donc 0 est valeur propre de multiplicité 2. La résolution de système $(A+I)X = 0$ montre que $\mathrm{Ker}(A+I) = \mathbb{R}\begin{pmatrix}1\\-1\\-1\end{pmatrix}$, donc $-1$ est valeur propre de multiplicité 1. Donc 1 est nécessairement valeur propre de multiplicité 1 : on en déduit que $\chi_A = X^2(X-1)(X+1)$.

**Exercice 2.5** *Déterminer les valeurs propres des matrices suivantes. Sont-elles diagonalisables, triangularisables ?*

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

*A l'aide du polynôme caractéristique de $B$, calculer $B^{-1}$.*

**Solution.**

1) $A$ est triangulaire inférieure donc ses valeurs sont ses coefficients diagonaux : 1, 2 et 3. $A$ a trois valeurs propres distinctes donc $A$ est diagonalisable.
2) $\chi_B = -(X-1)(X+1)^2$. $B+I = \begin{pmatrix}3&-2&1\\3&-2&1\\-1&2&1\end{pmatrix}$, donc $\mathrm{rg}(B+I) = 2$, $\dim(\mathrm{Ker}\, B+I) = 1 < 2$ donc $B$ n'est pas diagonalisable.
$\chi_B(B) = 0$ donc $B(B^2+B-I) = I$, soit $B^{-1} = B^2+B-I = \begin{pmatrix}-2&2&1\\-1&1&1\\3&-2&0\end{pmatrix}$.

**Exercice 2.6** *Soit $A$ la matrice définie par* $A = \begin{pmatrix}1&-1&-1\\-1&1&-1\\-1&-1&1\end{pmatrix}$.

*1) Calculer ${}^tA$. La matrice $A$ est-elle diagonalisable ?*
*2) Diagonaliser $A$.*
*3) Diagonaliser $A$ dans une base orthonormée (pour le produit scalaire usuel de $\mathbb{R}^3$).*

**Solution.**

1) ${}^tA = A$ donc $A$ est diagonalisable dans une base orthonormée.
2) Par exemple : $P = \begin{pmatrix}1&1&1\\1&-1&0\\1&0&-1\end{pmatrix}$, $P^{-1}AP = \begin{pmatrix}-1&0&0\\0&2&0\\0&0&2\end{pmatrix}$.
3) $Q = \begin{pmatrix}1/\sqrt{3}&1/\sqrt{2}&1/\sqrt{6}\\1/\sqrt{3}&-1/\sqrt{2}&1/\sqrt{6}\\1/\sqrt{3}&0&-2/\sqrt{6}\end{pmatrix}$, $Q^{-1}AQ = \begin{pmatrix}-1&0&0\\0&2&0\\0&0&2\end{pmatrix}$ et ${}^tQ = Q^{-1}$

**Exercice 2.7** *On considère l'endomorphisme $a$ de $E = \mathbb{R}^2$ dont la matrice représentative $A = [a]_e^e$ dans la base canonique $e$ est $\begin{bmatrix} 7 & -10 \\ 5 & -8 \end{bmatrix}$. Calculer la trace, le déterminant, le polynôme caractéristique et le spectre de $a$. Quel théorème du cours garantit l'existence d'une base $f = (\vec{f_1},\vec{f_2})$ de vecteurs propres ? Choisir ensuite $f$ telle que $[\mathrm{id}_E]_f^e$ et $[\mathrm{id}_E]_e^f$ soient à coefficients entiers.*

*Trouver deux matrices $P$ et $D$ carrées d'ordre 2 telles que $D$ soit diagonale, $P$ inversible et $A = PDP^{-1}$. Calculer $[a^{50}]_f^f$, $[a^{50}]_e^e$ et $A^{50}$. Calculer $\lim_{n\to\infty} \frac{1}{3^{2n}} a^{2n}$.*

**Solution.** $\mathrm{tr}a = \mathrm{tr}A = -1$, $\det a = \det A = -6$

$$P_a(X) = X^2 - \mathrm{tr}X + \det a = X^2 + X - 6 = (X-2)(X+3).$$

Donc le spectre est $\{2, -3\}$, il est de taille 2 comme l'espace est de dimension 2. D'après le cours, $a$ est diagonalisable et les espaces propres de dimension 1. L'espace propre associé à la valeur propre 2 est l'ensemble des $(x,y)$ tels que $7x - 10y = 2x$ ou $x = 2y$. On peut prendre $\vec{f_1} = (2,1)$ pour base de cet espace propre. L'espace propre associé à la valeur propre $-3$ est l'ensemble des $(x,y)$ tels que $7x - 10y = -3x$ ou $x = y$. On peut prendre $\vec{f_2} = (1,1)$ pour base de cet espace propre. Alors si $f = (\vec{f_1},\vec{f_2})$ on a

$$P = [\mathrm{id}_E]_f^e = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, P^{-1} = [\mathrm{id}_E]_e^f = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix},$$
$$D = [a]_f^f = \begin{bmatrix} 2 & 0 \\ 0 & -3 \end{bmatrix}, D^{50} = [a^{50}]_f^f = \begin{bmatrix} 2^{50} & 0 \\ 0 & (-3)^{50} \end{bmatrix},$$

$$A^{50} = [a^{50}]_e^e = PD^{50}P^{-1} = \begin{bmatrix} 2.2^{50} - (-3)^{50} & -2.2^{50} + 2.(-3)^{50} \\ 2^{50} - (-3)^{50} & -2^{50} + 2.(-3)^{50} \end{bmatrix}$$

Donc $\lim_{n\to\infty} \frac{1}{3^{2n}} [a^{2n}]_f^f = L = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$, et $\lim_{n\to\infty} \frac{1}{3^{2n}} [a^{2n}]_e^e = PLP^{-1} = \begin{bmatrix} -1 & 2 \\ -1 & 2 \end{bmatrix}$.

**Exercice 2.8** *Soit $\mathbb{K}$ un corps commutatif quelconque, et soit $F = \mathcal{M}_n(\mathbb{K})$ l'espace vectoriel sur $\mathbb{K}$ des matrices carrées d'ordre $n$ à coefficients dans $\mathbb{K}$. Si $i$ et $j$ sont des entiers compris entre 1 et $n$, on note par $F_{ij}$ l'élément de $F$ dont le coefficient $(i,j)$ est 1 et dont les autres coefficients sont nuls.*

1) *Montrer que les $F_{ij}$ forment une base de $F$. Donner la dimension de $F$ ?*
2) *Soit $D$ dans $F$ et diagonale. Soient $\alpha$ et $\beta$ dans $K$ et soit l'endomorphisme $\Phi$ de $F$ qui à la matrice $X$ fait correspondre la matrice $\Phi(X) = \alpha XD + \beta DX$. Calculer $\Phi(F_{ij})$. $\Phi$ est il un endomorphisme diagonalisable ?*
3) *Donner son polynôme caractéristique en fonction des coefficients de $D$ et de $\alpha$ et $\beta$.*

**Solution.**

1) Si $X = (x_{ij})_{1\le i,j\le n} \in F$, il est clair que $X = \sum_{1\le i,j\le n} x_{ij}F_{ij}$. C'est donc une famille génératrice. Elle est indépendante, car si $\sum_{1\le i,j\le n} x_{ij}F_{ij}$ est la matrice nulle, cela implique que $x_{ij} = 0$ pour tous $i$ et $j$. C'est donc une base de $F$. Elle est de taille $n^2$, donc $F$ est de dimension $n^2$.

2) Si $D = \mathrm{diag}(d_1,\ldots,d_n)$ et si $X = (x_{ij})_{1\leq i,j\leq n}$ alors le coefficient $(i,j)$ de la matrice $\Phi(X) = \alpha XD + \beta DX$ est $(\alpha d_j + \beta d_i)x_{ij}$. Donc $\Phi(F_{ij}) = (\alpha d_j + \beta d_i)F_{ij}$, ce qui est dire que $F_{ij}$ est un vecteur propre de $\Phi$ pour la valeur propre $\alpha d_j + \beta d_i$. L'espace $F$ admet donc une base de vecteurs propres de $\Phi$. Cela entraîne que $\Phi$ est diagonalisable.
3) Si on le représente dans la base de vecteurs propres, le déterminant de $\Phi$ est donc le produit des éléments diagonaux, c'est à dire $\det\Phi = \prod_{i=1}^n \prod_{j=1}^n (\alpha d_j + \beta d_i)$. Plus généralement $\det(\Phi - \lambda \mathrm{id}_F) = \prod_{i=1}^n \prod_{j=1}^n (\alpha d_j + \beta d_i - \lambda)$.

**Exercice 2.9** *Soit $\theta \in ]0,\pi[$. On considère les deux matrices d'ordre $n$ :*

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix},$$

$$B = \begin{bmatrix} 2\cos\theta & 1 & 0 & \cdots & 0 & 0 \\ 1 & 2\cos\theta & 1 & \cdots & 0 & 0 \\ 0 & 1 & 2\cos\theta & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 2\cos\theta & 1 \\ 0 & 0 & 0 & \cdots & 1 & 2\cos\theta \end{bmatrix}$$

*1) Montrer par récurrence que* $\det B = \frac{\sin(n+1)\theta}{\sin\theta}$
*2) Montrer que* $\det B$ *s'annule pour $n$ valeurs distinctes de $\theta$ de $]0,\pi[$, et les déterminer.*
*3) Si $P_A$ est le polynôme caractéristique de $A$, calculer $P_A(-2\cos\theta)$ et déduire de ce qui précède les valeurs propres de $A$.*
*4) Montrer que les valeurs propres des matrices $2I_n + A$ et $2I_n - A$ sont strictement positives.*

**Solution.**

1) On note $D_n = \det B$. Alors $D_1 = 2\cos\theta = \frac{\sin 2\theta}{\sin\theta}$ et $D_2 = 4\cos^2\theta - 1 = \frac{\sin 3\theta}{\sin\theta}$. Si $n > 2$, développons $D_n$ par rapport à la dernière ligne, en recommençant encore une fois avec un des déterminants d'ordre $n-1$ obtenus. On obtient $D_n = 2\cos\theta D_{n-1} - D_{n-2}$. Faisons l'hypothèse de récurrence que $D_k = \frac{\sin(k+1)\theta}{\sin\theta}$ pour $k < n$. On a vu que c'est vrai pour $k = 1$ et 2. Alors par des identités trigonométriques classiques

$$D_n = \frac{2\cos\theta\sin n\theta}{\sin\theta} - \frac{\sin(n-1)\theta}{\sin\theta} = \frac{\sin(n+1)\theta}{\sin\theta},$$

et la récurrence est étendue.
2) Puisque $\sin x = 0$, il existe un entier relatif $k$ tel que $x = k\pi$ alors $D_n = 0$ si et seulement si il existe $k = 1,2,\ldots,n$ tel que $\theta = \frac{k\pi}{n+1}$ les autres valeurs de $k$ étant exclues car $0 < \theta < \pi$.

3) Par définition de $P_A$ on a $P_A(-2\cos\theta) = D_n = \frac{\sin(n+1)\theta}{\sin\theta}$ qui s'annule pour les $n$ nombres distincts $-2\cos\frac{k\pi}{n+1}$, $k = 1,2,\ldots,n$ qui sont nécessairement toutes les valeurs propres de $A$.
4) Les valeurs propres de $2I_n + A$ sont donc $2 - 2\cos\frac{k\pi}{n+1} = 4\sin^2\frac{k\pi}{2n+2} > 0$. Le spectre de $2I_n - A$ est le même.

**Exercice 2.10** *Soit $E$ un $\mathbb{R}$-espace vectoriel de dimension finie $n$, et $u$ un endomorphisme de $E$.*

*Soit $x_0 \in E \setminus \{0\}$. On note $x_k = u^k(x_0)$ et $F$ le sous-espace vectoriel engendré par la famille $\{x_k, k \in \mathbb{N}\}$, c'est à dire l'ensemble des combinaisons linéaires finies de vecteurs de $x_k, k \in \mathbb{N}$ :*

$$F = \left\{ x \in E \ / \ \exists N \in \mathbb{N}, \exists(\alpha_0 \ldots \alpha_N) \in \mathbb{R}^{N+1},\ x = \sum_{i=0}^{N} \alpha_i x_i \right\}$$

*1) Montrer que $F$ est stable par $u$, c'est à dire que $\forall x \in F, u(x) \in F$.*
*2) Montrer qu'il existe un entier $k \leq n$ tel que $(x_0, x_1, \ldots, x_k)$ soit libre et $(x_0, x_1, \ldots, x_{k+1})$ soit liée. Montrer alors qu'il existe des scalaires $(a_0, a_1, \ldots, a_k)$ tels que*

$$x_{k+1} = a_0 x_0 + a_1 x_1 + \cdots + a_k x_k$$

*3) En déduire que le polynôme $P_0 = X^{k+1} - \sum_{i=0}^{k} a_i X^i$ satisfait $\big(P_0(u)\big)(x_0) = 0$.*
*4) Montrer que pour tout $x$ de $F$, il existe un polynôme $P \in \mathbb{R}[X]$ tel que $x = \big(P(u)\big)(x_0)$.*
*5) A l'aide des questions (3)) et (4)), montrer que $\forall x \in F$, $\exists R \in \mathbb{R}_k[X]$, $x = \big(R(u)\big)(x_0)$.*
*6) En déduire que $(x_0 \ldots x_k)$ est une base de $F$.*
*7) Ecrire la matrice de la restriction $u_{|_F}$ de $u$ à $F$ dans cette base. Quel est le polynôme caractéristique de $\tilde{u}$ ?*
*8) Montrer qu'il existe une base $\mathcal{B}$ de $E$ dans la quelle*

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} C_1 & 0 & \cdots & 0 \\ 0 & C_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & C_r \end{pmatrix}$$

*où les matrices $C_i$ sont des matrices Compagnon.*

**Solution.**

1) $u\big(\sum_{i=1}^{N} \alpha_i x_i\big) = \sum_{i=1}^{N} \alpha_i u(u^i(x_0)) = \sum_{i=1}^{N} \alpha_i x_{i+1}$. Donc $\forall x \in F$, $u(x) \in F$.
2) Si à un rang $k$, $x_{k+1}$ est une combinaison linéaire des $x_i$ pour $i \leq k$ : $x_{k+1} = \sum_{i=0}^{k} a_i x_i$. On en déduit que $x_{k+2} = \sum_{i=0}^{k} a_i x_{i+1}$, et donc que $x_{k+2} \in Vect(x_1, \ldots, x_{k+1}) \subset Vect(x_0, \ldots, x_k)$, et par récurrence, on obtient finalement que $\forall p > k, x_p \in Vect(x_0, \ldots, x_k)$. On en déduit que le rang de la famille $\{x_0, \ldots, x_m\}$, est strictement croissant avec $m$ puis éventuellement constant à partir d'un certain rang. Comme $E$ est de dimension finie $n$, on en déduit que ce rang est constant à partir d'un rang $k \leq n$ : la famille $(x_0, \ldots, x_k)$ est alors libre, et $x_{k+1}$ est une combinaison linéaire de $(x_0, \ldots, x_k)$.

3) $x_{k+1} - \sum_{i=0}^{k} a_i x_i = u^{k+1}(x_0) - \sum_{i=0}^{k} a_i u^i(x_0) = 0$ donc $P_0(u)(x_0) = 0$.
4) Si $x \in F$ alors $x = \sum_{i=0}^{N} \alpha_i u^i(x_0)$. En posant $P = \sum_{i=0}^{N} \alpha_i X^i$, on a : $x = P(u)(x_0)$.
5) Soit $P = QP_0 + R$ la division euclidienne de $P$ par $P_0$, alors $\deg(R) < \deg(P_0) = k+1$. On note $R = \sum_{i=0}^{k} r_i X^i$. On a :

$$x = P(u)(x_0) = Q(u)P_0(u)(x_0) + R(u)(x_0) = R(u)(x_0)$$

6) La famille $(x_0, \ldots, x_k)$ est donc libre et génératrice dans $F$ : c'est une base.
7) La matrice de $u_{|_F}$ dans cette base est la matrice compagnon associée au polynôme $P_0$, et $\chi_{u_{|_F}} = P_0$.
8) On choisit un vecteur $y \in E \setminus F$, et on recommence le même travail avec ce vecteur, et on continue ainsi jusqu'à avoir obtenu une base de tout l'espace. La matrice de $u$ dans la base finale est alors du type demandé.

**Exercice 2.11** *Soit* $A = \begin{pmatrix} 3 & 1 & 0 \\ -4 & -1 & 0 \\ 4 & 8 & -2 \end{pmatrix}$

*1) Vérifier que $A$ n'est pas diagonalisable.*
*2) Déterminer $Ker(A-I)^2$.*
*3) Montrer que $A$ est semblable à une matrice de la forme*

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

*4) Calculer $A^n$ pour $n$ entier naturel donné.*

**Solution.**

1)

$$\begin{aligned} U_A &= -(2+X)((3-X)(-1-X)+4) \\ &= -(X+2)(X^2-2X+1) \\ &= -(X+2)(X-1)^2. \end{aligned}$$

$A$ diagonalisable $\Rightarrow \dim(\mathrm{Ker}(A-I)) = 2 \Rightarrow \mathrm{rg}(A-I) = 1$. Donc $A$ n'est pas diagonalisable. De plus,

$E_{-2} = \mathrm{Vect}(e_1)$ où $e_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ et $E_1 = \mathrm{Vect}(e_2)$ où $e_2 = \begin{pmatrix} 1 \\ -2 \\ -4 \end{pmatrix}$.

2) $(A-I)^2 = \begin{pmatrix} 2 & 1 & 0 \\ -4 & -2 & 0 \\ 4 & 8 & -3 \end{pmatrix}\begin{pmatrix} 2 & 1 & 0 \\ -4 & -2 & 0 \\ 4 & 8 & -3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ -36 & -36 & 9 \end{pmatrix}$ et donc $\mathrm{Ker}(A-I)^2$ est le plan d'équation $4x + 4y - z = 0$.

3) On note $f$ l'endomorphisme de $\mathbb{R}^3$ dont la matrice dans la base canonique de $\mathbb{R}^3$ est $A$. Le théorème de Cayley-Hamilton et le théorème de décomposition des noyaux permettent d'affirmer

$$M_3(\mathbb{R}) = \mathrm{Ker}(A+2I) \oplus \mathrm{Ker}(A-I)^2.$$

De plus, chacun des sous-espaces $\mathrm{Ker}(A+2I)$ et $\mathrm{Ker}(A-I)^2$ étant stables par $f$, la matrice de $f$ dans toute base adaptée à cette décomposition est diagonale par blocs. Enfin, $\mathrm{Ker}(A-I)$ est une droite vectorielle contenue dans le plan $\mathrm{Ker}(A-I)^2$ et en choisissant une base de $\mathrm{Ker}(A-I)^2$ dont l'un des deux vecteurs est dans $\mathrm{Ker}(A-I)$.

On a déjà choisi $e_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ et $e_2 = \begin{pmatrix} 1 \\ -2 \\ -4 \end{pmatrix}$ puis on prend $e_3 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$.

On note $P = \begin{smallmatrix} 0 & 1 & 1 \\ 0 & -2 & -1 \\ 1 & -4 & 0 \end{smallmatrix}$. $P$ est inversible d'inverse $P^{-1} = \begin{smallmatrix} -4 & -4 & 1 \\ -1 & -1 & 0 \\ 2 & 1 & 0 \end{smallmatrix}$. On peut déjà affirmer que $P^{-1}AP$ est de la forme $\begin{pmatrix} -2 & 0 & 0 \\ 0 & 1 & \times \\ 0 & 0 & 1 \end{pmatrix}$. Plus précisément

$$Ae_3 - e_3 = \begin{pmatrix} 3 & 1 & 0 \\ -4 & -1 & 0 \\ 4 & 8 & -2 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \\ -4 \end{pmatrix} = e_2$$

et donc $Ae_3 = e_2 + e_3$ puis

$A = PTP^{-1}$ où $P = \begin{pmatrix} 0 & 1 & 1 \\ 0 & -2 & -1 \\ 1 & -4 & 0 \end{pmatrix}$, $P^{-1} = \begin{pmatrix} -4 & -4 & 1 \\ -1 & -1 & 0 \\ 2 & 1 & 0 \end{pmatrix}$ et

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

4) Soit $n \in \mathbb{N}$. On pose $T = D + N$ où $D = \mathrm{diag}(-2,1,1)$ et $N = E_{2,3}$. On a $ND = DN$ et $N^2 = 0$. Puisque les matrices $D$ et $N$ commutent, la formule du binôme de Newton permet d'écrire

$$\begin{aligned} T^n &= D^n + nD^{n-1}N \\ &= \mathrm{diag}((-2)^n,1,1) + n\mathrm{diag}((-2)^{n-1},1,1)E_{2,3} \\ &= \mathrm{diag}((-2)^n,1,1) + nE_{2,3} \\ &= \begin{pmatrix} (-2)^n & 0 & 0 \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

Puis

$$A^n = PT^nP^{-1} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & -2 & -1 \\ 1 & -4 & 0 \end{pmatrix} \begin{pmatrix} (-2)^n & 0 & 0 \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -4 & -4 & 0 \\ -1 & -1 & 0 \\ 2 & 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 1 & n+1 \\ 0 & -2 & -2n-1 \\ (-2)^n & -4 & -4n \end{pmatrix} \begin{pmatrix} -4 & -4 & 1 \\ -1 & -1 & 0 \\ 2 & 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 2n+1 & n & 0 \\ -4n & -2n+1 & 0 \\ -4(-2)^n - 8n + 4 & -4(-2)^n - 4n + 4 & (-2)^n \end{pmatrix}$$

d'où

$$\forall n \in \mathbb{N},\ A_n = \begin{pmatrix} 2n+1 & n & 0 \\ -4n & -2n+1 & 0 \\ -4(-2)^n - 8n + 4 & -4(-2)^n - 4n + 4 & (-2)^n \end{pmatrix}$$

**Exercice 2.12** *Soit la fonction $f$ qui à $P$ élèment de $\mathbb{R}_{2n}[X]$ associe $f(P) = (X^2-1)P' - 2nXP$*

*Vérifier que $f$ est un endomorphisme de $\mathbb{R}_{2n}[X]$ puis déterminer les valeurs et vecteurs propres de $f$. $f$ est-il diagonalisable ?*

**Solution.** Soit $P$ un élèment de $\mathbb{R}_{2n}[X]$. $f(P)$ est un polynôme de degré inférieur ou égal à $2n+1$ et de plus, si $a$ est le coefficient de $X^{2n}$ dans $P$, le coefficient de $X^{2n+1}$ dans $f(P)$ est $2na - 2na = 0$. Donc $f(P)$ est un élèment de $\mathbb{R}_{2n}[X]$. $f$ est linéaire, $f$ est donc un endomorphisme de $\mathbb{R}_{2n}[X]$.

On cherche maintenant $P$ polynôme non nul et $\lambda$ réel tels que $f(P) = \lambda P$ ce qui équivaut à

$$\frac{P'}{P} = \frac{2nX+\lambda}{X^2-1} = \frac{1}{2} = \left(\frac{2nX+\lambda}{X-1} - \frac{-2nX+\lambda}{X+1}\right).$$

En identifiant à la décomposition en éléments simples classique de $\frac{P'}{P}$ (à savoir si $P = K(X-z_1)^{\alpha_1}...(X-z_k)^{\alpha_k}$ avec $K \neq 0$ et les $z_i$ deux à deux distincts, alors $\frac{P'}{P} = \sum_{i=1}^{k} \frac{\alpha_i}{X-z_i}$, on voit que nécessairement $P$ ne peut admettre pour racines dans $\mathbb{C}$ que $-1$ et $1$ et d'autre part que $P$ est de degré $\frac{1}{2}(2n+\alpha+2n-\alpha) = 2n$. $P$ est donc nécessairement de la forme $P = aP_k$ avec $a \in \mathbb{R}^*$ et $P_k = (X-1)^k(X+1)^{2n-k}$ avec $k \in [\![0,2n]\!]$.

Réciproquement, chaque $P_k$ est non nul et vérifie

$$\frac{P_k'}{P_k} = \frac{k}{X-1} + \frac{2n-k}{X+1} = \frac{1}{2}\left(\frac{2n+(2k-2n)}{X-1} + \frac{2n-(2k-2n)}{X+1}\right)$$

Donc, pour chaque $k \in [0,2n]$, $P_k$ est vecteur propre de $f$ associé à la valeur propre $\lambda_k = 2(k-n)$.