CLASSES PREPARATOIRES
AUX GRANDES ECOLES SCIENTIFIQUES

E. Ramis / C. Deschamps / J. Odoux

ALGÈBRE

MASSON

NOTATIONS

$\sum_{i,j}$ ou $\prod_{i,j}$: mis pour $\sum_{(i,j)\in I}$ ou $\prod_{(i,j)\in I}$ lorsqu'il n'y a pas ambiguité sur I.

$\mathbb{N}_n$: partie $\{1,\ldots,n\}$ de $\mathbb{N}^* = \mathbb{N}\setminus\{0\}$.

$\mathfrak{S}_n$: groupe des permutations de $\mathbb{N}_n$.

$\bigwedge_{i\in I} a_i$ ou $\mathrm{PGCD}\left((a_i)_{i\in I}\right)$: plus grand commun diviseur d'une famille d'éléments d'un anneau intègre ; en particulier $a \wedge b = \mathrm{PGCD}(a,b)$.

K : corps (systématiquement supposé commutatif).

A[X] : algèbre des polynômes à une indéterminée sur l'anneau commutatif A.

$K_n[X]$: sous-espace vectoriel de dimension n+1 de K[X] formé des polynômes dont le degré n'excède pas n.

Les espaces vectoriels donnés (mais non leurs sous-espaces) sont compris : distincts de {0}.

uv : mis souvent pour l'application composée $u \circ v$ (u^2 et u^n sont mis pour $u \circ u$ et $u^{n-1} \circ u = u \circ u^{n-1}$).

$\mathcal{M}_{n,p}(E)$ [resp. $\mathcal{M}_n(E)$] : ensemble des matrices (n,p) [resp. (n,n)] à éléments dans l'ensemble E.

$\left(E_{ij}\right)_{(i,j)\in\mathbb{N}_n\times\mathbb{N}_p}$: base canonique de l'espace vectoriel $\mathcal{M}_{n,p}(K)$, de dimension np; pour (i,j) donné, l'élément de E_{ij} qui correspond à la ligne k et à la colonne ℓ est $\delta_{ik}\delta_{\ell j}$.

$GL_n(K)$: groupe multiplicatif des éléments inversibles de l'anneau $\mathcal{M}_n(K)$.

χ_u et μ_u (resp. χ_A et μ_A) : polynômes caractéristique et minimal de l'endomorphisme u (resp. de la matrice carrée A).

ALGÈBRE

EXERCICES AVEC SOLUTIONS

CHEZ LE MÊME ÉDITEUR

Des mêmes auteurs

ANALYSE. EXERCICES AVEC SOLUTIONS, par E. RAMIS, C. DESCHAMPS et J. ODOUX.
Tome 1. — 1984, 200 pages.
Tome 2. — 1985, 224 pages.

COURS DE MATHÉMATIQUES SPÉCIALES, par E. RAMIS, C. DESCHAMPS et J. ODOUX.
Volume 1. — Algèbre. 1990, 2e édition, 2e tirage, 448 pages.
Volume 2. — Algèbre et applications à la géométrie. 1990, 3e tirage corrigé, 312 pages.
Volume 3. — Topologie et éléments d'analyse. 1988, 2e édition, 2e tirage, 376 pages.
Volume 4. — Séries et équations différentielles. 1990, 2e édition, 2e tirage, 328 pages.
Volume 5. — Applications de l'analyse à la géométrie. 1981, 320 pages.

Dans la collection maîtrise de mathématiques pures

ALGÈBRE LINÉAIRE ET GÉOMÉTRIE CLASSIQUE, par J.E. BERTIN et M.-J. BERTIN. Avant-propos de J. DIEUDONNÉ. *Collection Maîtrise de Mathématiques Pures.* 1981, 152 pages.

ALGÈBRE LINÉAIRE ET GÉOMÉTRIE CLASSIQUE - EXERCICES, par M.-P. MALLIAVIN et A. WARUSFEL. *Collection Maîtrise de Mathématiques Pures.* 1981, 128 pages.

LES GROUPES FINIS ET LEURS REPÉSENTATIONS COMPLEXES - COURS, par M-P. MALLIAVIN. *Collection Maîtrise de Mathématiques Pures.* 1981, 96 pages.

LES GROUPES FINIS ET LEURS REPRÉSENTATIONS COMPLEXES - EXERCICES, par J.-P. BÉZIVIN et A. LÉVY-BRUHL. *Collection Maîtrise de Mathématiques Pures.* 1982, 108 pages.

ALGÈBRE COMMUTATIVE, APPLICATIONS EN GÉOMÉTRIE ET THÉORIE DES NOMBRES, par M.-P. MALLIAVIN. *Collection Maîtrise de Mathématiques Pures.* 1985, 250 pages.

ALGÈBRE COMMUTATIVE, APPLICATIONS EN GÉOMÉTRIE ET THÉORIE DES NOMBRES - EXERCICES, par M.-J. BERTIN et E. WEXLER-KREINDLER. *Collection Maîtrise de Mathématiques Pures.* 1986, 208 pages.

Autres ouvrages

COURS D'ALGÈBRE, AVEC ÉNONCÉS : 40 EXERCICES-300 PROBLÈMES. MAITRISE DE MATHÉMATIQUES, par J. QUERRÉ. 1977, 252 pages.

COURS DE TOPOLOGIE. Licence et 1re année de maîtrise C1. Espaces topologiques et espaces métriques. Fonctions numériques. Espaces vectoriels topologiques, par G. CHOQUET. 1992, 2e édition, 4e tirage, 328 pages.

ANALYSE RÉELLE ET COMPLEXE, par W. RUDIN. Traduit de l'anglais par N. DHOMBRES et F. HOFFMAN. 1992, 6e tirage, 408 pages.

Classes préparatoires aux grandes écoles scientifiques

ALGÈBRE

EXERCICES AVEC SOLUTIONS

E. Ramis
Inspecteur général de l'Instruction Publique

Cl. Deschamps
Professeur de Mathématiques Spéciales
au Lycée Louis-le-Grand

J. Odoux
Professeur de Mathématiques Spéciales
au Lycée Champollion, à Grenoble

2e tirage

MASSON
Paris Milan Barcelone Bonn
1992

ISBN : 2-225-**81314**-0

MASSON S.A. 120, bd Saint-Germain, 75280 Paris Cedex 06
MASSON S.p.A. Via Statuto 2/4, 20121 Milano
MASSON S.A. Avenida Principe de Asturias 20, 08012 Barcelona
DÜRR und KESSLER Maarweg, 30, 5342 Rheinbreitbach b. Bonn

TABLE DES MATIÈRES

AVANT-PROPOS

Le présent volume, consacré à l'Algèbre, est le troisième d'une série d'exercices avec solutions développées qui s'adresse aux étudiants des classes préparatoires aux Grandes Ecoles scientifiques et du premier cycle universitaire.

Les objectifs d'un recueil de ce type sont bien connus : il s'agit essentiellement d'aider le lecteur à évaluer ses connaissances et à les mettre en oeuvre : ceci implique aussi bien une réflexion sur la nature des concepts que la recherche d'une maîtrise des techniques de calcul.

Sauf rares exceptions, nous n'avons donné de chaque question qu'une solution, celle qui nous a paru s'exposer le plus brièvement ou offrir les plus larges prolongements ; il ne s'agit naturellement pas d'une solution exhaustive et le lecteur aura toujours intérêt à poursuivre le plus loin possible sa propre démarche.

Nous avons explicité tous les raisonnements et la plupart des calculs ; il nous est cependant arrivé d'omettre intentionnellement quelques intermédiaires pour laisser à l'étudiant le soin de les rétablir.

Nous remercions les lecteurs qui ont bien voulu nous faire part de leurs critiques et de leurs suggestions concernant nos deux premiers volumes. Nous espérons que le troisième bénéficiera de la même attention.

Les Auteurs

1. STRUCTURES USUELLES

Ce chapitre concerne les groupes, les anneaux et les corps ; un chapitre spécial sera consacré aux espaces vectoriels.

1.1. GROUPES

1.1.1 Le nombre premier p est fixé. Soit U le groupe multiplicatif des nombres complexes de module 1. On considère :

$$U_p = \{\exp(2i\pi.a/p^\alpha) \mid a \in \mathbb{Z} \text{ non multiple de } p,\ \alpha \in \mathbb{N}\}.$$

1° Montrer que U_p est un sous-groupe de U dont tous les éléments sont d'ordre fini.

2° Montrer que tout sous-groupe de U_p distinct de U_p (sous-groupe strict) est cyclique.

1° Il est clair que U_p est un sous-groupe de U.

Soit $z = \exp(2i\pi.a/p^\alpha)$ un élément de U_p. On constate que $(z)^{p^\alpha} = 1$; z est donc d'ordre fini, et l'ordre de z divise p^α.

Inversement soit $q \in \mathbb{N}^*$ tel que $z^q = 1$. On a : $aq = kp^\alpha$ avec $k \in \mathbb{Z}$; il en résulte que p^α, qui est premier avec a, divise q.

L'ordre de z est ainsi p^α.

2° Remarquons qu'à tout élément $z = \exp(2i\pi.a/p^\alpha)$ de U_p on peut associer un $u \in \mathbb{Z}$ tel que : $\exp(2i\pi.1/p^\alpha) = z^u$.

En effet, a et p^α étant premiers entre eux, d'après le théorème de Bezout il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + p^\alpha v = 1$. On a :

$$\exp(2i\pi.1/p^\alpha) = \exp(2i\pi(v+ua/p^\alpha)) = z^u.$$

• Il en résulte que tout sous groupe de U_p dont un élément est $z = \exp(2i\pi.a/p^\alpha)$ contient tous les éléments de U_p de la forme :

$$Z = \exp(2i\pi.b/p^\beta), \text{ avec } 0 \leqslant \beta \leqslant \alpha.$$

En effet : $Z = \exp(2i\pi.1/p^\alpha)^w$, avec $w = bp^{\alpha-\beta} \in \mathbb{Z}$, et donc $Z = z^{uw}$ avec $uw \in \mathbb{Z}$.

• Soit maintenant H un sous-groupe strict de U_p. Il existe un élément $\exp(2i\pi.c/p^\gamma)$ de U_p qui n'appartient pas à H, et d'ailleurs $\gamma \geqslant 1$ (car $1 \in H$).

D'après ce qui précède, pour tout élément $\exp(2i\pi.a/p^\alpha)$ de H, on a :

$$\exp(2i\pi.1/p^\alpha) \in H \text{ et } 0 \leqslant \alpha < \gamma.$$

On dispose ainsi de :

$$\rho = \max\{\alpha \in \mathbb{N} \mid \exp(2i\pi.1/p^\alpha) \in H\}.$$

Il est aisé de constater que H est cyclique, engendré par $\exp(2i\pi.1/p^\rho)$.

Remarque. L'exercice met en évidence l'existence de groupes infinis dont tous les éléments sont d'ordre fini, et celle de groupes infinis dont tous les sous-groupes stricts sont cycliques.

1.1.2 Soit G un groupe fini de cardinal 2n admettant deux sous-groupes distincts G_1 et G_2 de cardinal n. Montrer que G admet un troisième sous-groupe de cardinal n, distinct de G_1 et de G_2.

Indication : On traitera d'abord la question en imposant la condition supplémentaire $G_1 \cap G_2 = \{e\}$, où e est l'élément neutre de G.

Nous aurons à utiliser :

LEMME. *Soient* G *un groupe de cardinal* 2n, *et* H *un sous-groupe de* G *de cardinal* n ; *alors* H *est distingué.*

L'indice de H dans G (quotient du cardinal de G par celui de H) est 2. Il y a donc deux classes à gauche suivant H, qui sont H et $G \setminus H$, et deux classes à droite, qui sont aussi H et $G \setminus H$. □

1° Ici $G_1 \cap G_2 = \{e\}$. On a donc : $\text{card}(G_1 \cup G_2) = 2n-1$, et il existe un unique $a \in G$ n'appartenant ni à G_1, ni à G_2.

Pour tout $(x_1, x_2) \in (G_1 \setminus \{e\}) \times (G_2 \setminus \{e\})$, on a $x_1x_2 = a$; en effet x_1x_2 n'appartient pas à G_1 (sans quoi $x_2 = x_1^{-1}(x_1x_2)$ appartiendrait à $G_1 \setminus \{e\}$) et pas davantage à G_2.

Il en résulte que, pour $x_1 \in G_1 \setminus \{e\}$ fixé, l'ensemble x_1G_2, formé de n éléments deux à deux distincts, s'écrit $\{x_1, a\}$, ce qui exige $n = 2$ et $2n = 4$.

- Inversement on constate, en construisant les tables, que tout groupe de cardinal 4 est isomorphe soit à $\mathbb{Z}/4\mathbb{Z}$ et alors il admet un unique sous-groupe de cardinal 2, soit au groupe de Klein $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ et alors il admet trois sous-groupes de cardinal 2.

- La proposition est ainsi établie dans le cas où $G_1 \cap G_2 = \{e\}$.

2° Venons-en au cas général. D'après le lemme, G_1 et G_2 sont des sous-groupes distingués de G ; $H = G_1 \cap G_2$ est donc un sous-groupe distingué de G_1, de G_2 et de G. Soit p son cardinal. Les cardinaux des groupes-quotient

$$G_1/H = \{xH \mid x \in G_1\},\ G_2/H = \{xH \mid x \in G_2\} \text{ et } G/H = \{xH \mid x \in G\}$$

sont respectivement n/p, n/p et 2n/p.

G_1/H et G_2/H sont donc des sous-groupes de cardinal n/p du groupe G/H de cardinal 2n/p. On vérifie que $x_1H = x_2H$, avec $x_1 \in G_1$ et $x_2 \in G_2$, exige $x_1 \in H$ et $x_2 \in H$. On a donc :

$$(G_1/H) \cap (G_2/H) = \{H\}$$

où H est l'élément neutre de G/H. On se trouve ainsi dans la situation du 1°. On a $n/p = 2$ et le cardinal 2n de G est un multiple de 4.

- D'après 1°, G/H admet un sous-groupe Γ de cardinal 2, distinct de G_1/H et de G_2/H, et donc de la forme (H,aH), avec $a \notin G_1$, $a \notin G_2$ et, bien sûr, $a \notin H$.

La surjection canonique φ de G sur G/H est un morphisme de groupes et $\varphi^{-1}(\Gamma)$ est un sous-groupe de G, que nous notons G_3. Nous constatons que $x \in G_3$, qui s'écrit $\varphi(x) \in \Gamma$, équivaut à $x \in H \cup (aH)$; réunion de deux ensembles disjoints H et aH de cardinal p, le sous-groupe G_3 de G est de cardinal $2p = n$.

Enfin il est clair que G_3 est distinct de G_1 et de G_2. □

1.1.3 Soient G un groupe (pas nécessairement fini), et H un sous-groupe de G d'indice fini $[G : H] = n$.

Montrer qu'il existe un sous-groupe S de H, distingué dans G et tel que l'indice $[G : S]$ soit fini et divise n!

- Soit $\mathcal{R}_\gamma$ la relation d'équivalence à gauche suivant H, telle que :

$$\forall (x,y) \in G^2 \quad (x \mathcal{R}_\gamma y) \iff (x^{-1}y \in H)$$

On note E l'ensemble-quotient $G/\mathcal{R}_\gamma$, de cardinal n. La classe de $x \in G$ est xH ; elle est notée $\overline{x}$.

- A tout $g \in H$ on associe l'application θ_g de E dans E définie par :

$$\forall \overline{x} \in E \quad \theta_g(\overline{x}) = \overline{gx}$$

ce qui a un sens puisque si $x^{-1}y \in H$, alors $(gx)^{-1}(gy) \in H$.

Pour g donné, θ_g est bijective. En effet, pour tout $y \in G$, on a $\theta_g(\overline{x}) = \overline{y}$ si, et seulement si $\overline{gx} = \overline{y}$, i.e. $(gx)^{-1}y \in H$, i.e. $\overline{x} = \overline{g^{-1}y}$.

On constate :

$$\forall (g,g') \in G^2 \quad \theta_g \circ \theta_{g'} = \theta_{gg'}$$

ce qui montre que l'application $\theta : g \mapsto \theta_g$ est un morphisme de groupes de G dans le groupe symétrique $\mathcal{S}(E)$.

Le noyau de ce morphisme, noté S, est un sous-groupe distingué de G ; le groupe quotient G/S est isomorphe à $\mathrm{Im}\theta$, qui est un sous-groupe du groupe fini $\mathcal{S}(E)$, de cardinal n! ; on en déduit que G/S est fini et que son cardinal divise n!

- Il ne reste plus à vérifier que $S \subset H$.

  Pour tout $g \in S$, $\theta_g = \mathrm{Id}_E$, et, en particulier :

  $\overline{e} = \theta_g(\overline{e}) = \overline{ge} = \overline{g}$, et donc $g \in H$. □

1.1.4 Soit G un groupe commutatif fini de cardinal n.

1° Montrer que s'il existe un entier $q \geqslant 2$ tel que :

$$\forall x \in G \quad x^q = e \quad \text{(élément neutre de G)} \qquad (1)$$

alors il existe une puissance de q divisible par n.

2° En déduire que, pour tout diviseur premier p de n, G admet un sous-groupe de cardinal p.

3° Montrer que, si n est de la forme $p^r q$, avec p premier, q premier avec p, et $r \in \mathbb{N}^*$, alors G admet un sous-groupe de cardinal p^r.

1° Il s'agit de montrer qu'est vraie pour tout $n \in \mathbb{N}^*$ l'assertion $(\mathcal{A}_n)$: Pour tout groupe commutatif de cardinal n, s'il existe un entier $q \geqslant 2$ vérifiant (1), alors il existe une puissance de q divisible par n.

- Il est clair que $\mathcal{A}_1$ est vraie.

- Soit $n \in \mathbb{N}^*$ tel que $\mathcal{A}_1, \ldots, \mathcal{A}_n$ aient été vérifiées. Considérons un groupe commutatif G de cardinal n+1 auquel on peut associer un entier $q \geqslant 2$ tel que $x^q = e$ pour tout $x \in G$.

D'après $n+1 \geqslant 2$, on dispose de $a \in G \setminus \{e\}$, et le sous-groupe G' de G engendré par a, qui contient a et e, est de cardinal $n' \geqslant 2$; d'après $a^q = e$, l'ordre n' de a dans G divise q ; soit $q = n'r$, $r \in \mathbb{N}^*$.

Etudions le groupe-quotient G/G', de cardinal $m = (n+1)/n'$.

L'entier $q \geqslant 2$ vérifie :

$$\forall X \in G/G' \quad X^q = \overline{e} \quad \text{(élément neutre de G/G')}.$$

Or, d'après $n' \geqslant 2$, on a : $n+1 \leqslant 2n \leqslant n'n$, et donc $m \leqslant n$; l'assertion $\mathcal{A}_m$ est vraie et, en l'appliquant à G/G' et à q, on constate qu'il existe $\alpha \in \mathbb{N}^*$ et $s \in \mathbb{N}^*$ tels que $q^\alpha = ms$.

D'où : $q^{\alpha+1} = n'rms = (n+1)rs$. $\mathcal{A}_{n+1}$ est donc vraie. □

2° Soit p un nombre premier qui divise n.

A tout $x \in G$, nous associons son ordre $\omega(x)$; le PPCM q des $\omega(x)$ vérifie (1).

Nous avons $q \geqslant 2$ (sans quoi nous aurions $G = \{e\}$ et aucun nombre premier ne diviserait n). D'après 1°, il existe une puissance de q divisible par le nombre premier p, et donc q est divisible par p.

Divisant le PPCM des $\omega(x)$, le nombre premier p divise l'un d'eux ; il existe $a \in G$ tel que $\omega(a) = pu$, $u \in \mathbb{N}^*$.

Il en résulte que a^u est d'ordre p dans G ; le sous-groupe de G qu'il engendre est de cardinal p. □

3° Ici p premier, et q premier avec p sont fixés. Il s'agit de montrer qu'est vraie pour tout $r \in \mathbb{N}^*$ l'assertion :

($\mathcal{B}_r$) Tout groupe commutatif fini de cardinal $p^r q$ admet un sous-groupe de cardinal p^r.

- $\mathcal{B}_1$ est vraie d'après 2°.
- Soit $r \in \mathbb{N}^*$ tel que $\mathcal{B}_r$ ait été vérifiée. Considérons un groupe commutatif G de cardinal $n = p^{r+1}q$.

D'après 2°, G admet un sous-groupe H de cardinal p. On dispose du groupe-quotient G/H ; la surjection canonique φ de G sur G/H est un morphisme de groupes commutatifs.

Le cardinal de G/H étant $n/p = p^r q$, d'après $\mathcal{B}_r$ il existe un sous-groupe G' de G/H de cardinal p^r ; $\varphi^{-1}(G')$ est un sous-groupe de G de cardinal p^{r+1}.

$\mathcal{B}_{r+1}$ est donc vraie. □

1.1.5 Soient m et n deux entiers naturels premiers entre eux.

1° Montrer que les groupes $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes.

2° Soient G un groupe commutatif, a et b deux éléments de G d'ordres respectifs m et n ; on pose $c = ab$. Montrer que le sous-groupe de G engendré par c contient a et b. Quel est l'ordre de c dans G ?

1° Pour tous $q \in N$ et $x \in \mathbb{Z}$, $\overline{x}_q$ désigne la classe de x dans $\mathbb{Z}/q\mathbb{Z}$.

- On constate que $\overline{x}_{mn} \mapsto (\overline{x}_m, \overline{x}_n)$ définit une application f de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$; en effet si les entiers x et y diffèrent par un multiple de mn, ils diffèrent par un multiple de m (resp. n).

On vérifie aisément que f est un morphisme de groupes. Son noyau est constitué par les $\overline{x}_{mn}$ tels que x soit multiple de m et de n, i.e. multiple du PPCM de m et n, qui est mn puisque m et n sont premiers entre eux. On a donc Ker f = $\{\overline{0}_{mn}\}$, ce qui montre que f est injectif.

Appliquant un ensemble de cardinal mn dans un ensemble de même cardinal, l'injection f est une bijection ; f est donc un isomorphisme de groupes commutatifs.

Remarque. La proposition reste valable si, dans l'énoncé et dans la démonstration, on remplace "groupes" par "anneaux".

2° D'après le 1°, on dispose de $k \in \mathbb{Z}$, auquel on peut même imposer $0 \leqslant k \leqslant mn-1$, tel que $\overline{k}_{mn} = f^{-1}(\overline{1}_m, \overline{0}_n)$, i.e. tel que les restes des divisions de k par m et n soient respectivement 1 et 0. On a (puisque G est commutatif) : $c^k = a^k b^k = a$.

Ainsi a appartient au sous-groupe G' de G engendré par c. Il en est de même pour b. □

On a : $c^{mn} = a^{mn} b^{mn} = e$ (élément neutre de G). Il en résulte que G' est fini et que son cardinal divise mn.

D'autre part G' contient les sous groupes de G respectivement engendrés par a et par b ; son cardinal est un multiple de m et de n, et donc un multiple de mn.

En conclusion, le cardinal de G', qui est l'ordre de c dans G, est mn.

Dans le 1° de l'exercice suivant, on étudie une extension du résultat du 2° de l'exercice précédent au cas où m et n ne sont pas premiers entre eux.

1.1.6 1° Soient G un groupe commutatif, a et b deux éléments de G d'ordres respectifs m et n. Montrer que G contient un élément dont l'ordre est le PPCM de m et n.

2° Soit G un groupe commutatif fini.

a) On note q le plus grand des ordres des éléments de G. Montrer :

$\forall x \in G \quad x^q = e$ (élément neutre de G).

b) En déduire que si K est un corps commutatif fini, le groupe multiplicatif K^* est cyclique.

1° Soit q le PPCM de m et n. En utilisant les décompositions de m et n en nombres premiers, on dispose du produit r des puissances p^α de nombres premiers telles que p^α divise m mais ne divise pas n ; on définit s par q = rs (c'est ainsi que si $m = 2^4.3^2.5.7^2$ et $n = 2^2.3^2.11$, alors $r = 2^4.5.7^2$ et $s = 3^2.11$).

On constate que r et s sont premiers entre eux, que r divise m, et que s divise n, ce qui permet de définir u et v par m = ru et n = sv.

On considère a^u. On a $(a^u)^k = e$ si, et seulement si ku est un multiple de m, i.e. si et seulement si k est un multiple de r. L'élément a^u de G est donc d'ordre r ; de même b^v est d'ordre s. En utilisant l'exercice précédent, on constate que $a^u b^v$ est d'ordre rs = q. □

Remarque. c = ab n'est pas nécessairement d'ordre q. C'est ainsi que si $G = \mathbb{Z}/5\mathbb{Z}$, $a = \overline{2}$ et $b = \overline{3}$ sont chacun d'ordre 5, alors que $c = \overline{5}$ est d'ordre 1.

2° a) Tout $a \in G$ admet un ordre majoré par card G et noté $\omega(a)$; on en déduit que l'entier q existe, et que l'on dispose d'un élément de G dont l'ordre est q.

Soit $x \in G$. Son ordre vérifie $\omega(x) \leqslant q$. D'après 1°), il existe $y \in G$ dont l'ordre $\omega(y)$ est le PPCM de $\omega(x)$ et de q ; d'après $\omega(y) \leqslant q$, on a $\omega(y) = q$; il en résulte que $\omega(x)$ divise q, et donc que $x^q = e$. □

b) Soit n le cardinal du groupe commutatif fini K^*. On note q le plus grand des ordres des éléments de K^* ; q est un diviseur de n, et donc $q \leqslant n$.

D'autre part, dans l'anneau $K[X]$ des polynômes à une indéterminée sur le corps commutatif K, le polynôme $X^q - 1$, dont le degré est q, admet au plus q racines. Or, d'après a), il admet pour racine chacun des n éléments de K^*. On a donc $n \leqslant q$. Finalement $n = q$.

Dans le groupe K^* de cardinal n, on dispose ainsi d'un élément d'ordre n ; le groupe est donc cyclique. □

Remarque. On démontre que tout corps fini est commutatif .

1.1.7 On appelle indicateur d'Euler l'application φ de $\mathbb{N}^*$ dans $\mathbb{N}^*$ qui à n associe le cardinal de l'ensemble E_n des éléments de $\mathbb{N}_n$ qui sont premiers avec n.

1° Soient m et n des éléments premiers entre eux de $\mathbb{N}^*$. Montrer :

$$\varphi(mn) = \varphi(m)\varphi(n). \qquad (1)$$

En déduire la valeur de $\varphi(n)$, $n \in \mathbb{N}^*$.

2° Soit $n \in \mathbb{N}^*$. On note $\mathcal{D}$ l'ensemble des éléments de $\mathbb{N}_n$ qui divisent n. Etablir la formule :

$$\sum_{d \in \mathcal{D}} \varphi(d) = n. \qquad (2)$$

1° Soit $n \in \mathbb{N}^*$. Pour tout $x \in \mathbb{Z}$, on constate, en utilisant le théorème de Bezout, que x est premier avec n si, et seulement s'il existe $u \in \mathbb{Z}$ tel que $ux \equiv 1 \pmod{n}$, i.e. tel que $\overline{u}\,\overline{x} = \overline{1}$ dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Les éléments distincts de $\mathbb{Z}/n\mathbb{Z}$ étant les $\overline{x}$ tels que $x \in \mathbb{N}_n$, il en résulte

que les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{x}$ tels que $x \in E_n$; $\varphi(n)$ est ainsi le nombre de ces éléments inversibles.

• Soit $(m,n) \in (\mathbb{N}^*)^2$ tel que $m \wedge n = 1$. Deux anneaux isomorphes ayant le même nombre d'éléments inversibles, φ_{mn} est le nombre des éléments inversibles de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (cf. 1.1.5) et donc le nombre des couples formés d'un élément inversible de $\mathbb{Z}/m\mathbb{Z}$ et d'un élément inversible de $\mathbb{Z}/n\mathbb{Z}$, à savoir $\varphi(m)\varphi(n)$. D'où (1). □

• Il est clair que $\varphi(1) = 1$. Pour calculer $\varphi(n)$, $n \geqslant 2$, nous utiliserons la décomposition de n en facteurs premiers, et la formule (1).

- Commençons par calculer $\varphi(p^\alpha)$, avec p premier et $\alpha \in \mathbb{N}^*$. Un entier k tel que $1 \leqslant k \leqslant p^\alpha$ est non premier avec p^α si, et seulement si k et p^α ont un autre diviseur commun que 1, i.e. si, et seulement si p divise k, ce qui s'écrit : $k \in \{p, 2p, \ldots, p^{\alpha-1}p\}$.

On en déduit : $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1-1/p)$.

En particulier : $\varphi(p) = p-1$ (ici $1,2,\ldots,p-1$ sont premiers avec p).

- En utilisant si nécessaire (1) et un raisonnement par récurrence, on en déduit que, si $n \geqslant 2$ admet la décomposition $n = p_1^{\alpha_1} \ldots p_q^{\alpha_q}$, alors :

$$\varphi(n) = n(1-1/p_1)\ldots(1-1/p_q).$$

2° A tout $d \in \mathcal{T}$, on associe la partie $F_d = \frac{n}{d} E_d$ de $\mathbb{N}_n$. On a :

$$\operatorname{card} F_d = \operatorname{card} E_d = \varphi(d).$$

On va montrer que $\bigcup_{d \in \mathcal{T}} F_d$ est une partition de $\mathbb{N}_n$; (2) en résultera.

i) <u>Pour tout</u> $y \in \mathbb{N}_n$, <u>il existe</u> $d \in \mathcal{T}$ <u>tel que</u> $y \in F_d$. Soit en effet $\delta = y \wedge n$. Définissons y' et n' par $y = \delta y'$ et $n = \delta n'$. Nous avons :

$$y' \wedge n' = 1,\ y' \in \mathbb{N}_{n'},\ \text{et donc } y' \in E_{n'}.$$

De $y = \frac{n}{n'} y'$, nous déduisons alors : $y \in F_{n'}$, avec $n' \in \mathcal{T}$.

ii) <u>Pour tout</u> $(d,d') \in \mathcal{T}^2$, $F_d \cap F_{d'} \neq \phi$ <u>entraîne</u> $d = d'$. $F_d \cap F_{d'} \neq \phi$ se traduit par l'existence de $k \in E_d$ et de $k' \in E_{d'}$, tels que :

$$\frac{n}{d} k = \frac{n}{d'} k',\ \text{i.e. } kd' = k'd.$$

Premier avec d et divisant k'd, k divise k' ; de même k' divise k et donc $k = k'$. Il en résulte : $d = d'$. □

1.1.8 Soit G un groupe cyclique de cardinal n. Pour tout $x \in G$, on note G(x) le sous-groupe de G engendré par x.

1° Soit a un générateur de G. Pour tout $k \in \mathbb{N}_n$, montrer que a^k engendre G si, et seulement si k est premier avec n.

En déduire que le nombre des générateurs de G est $\varphi(n)$, où φ est l'indicateur d'Euler défini dans l'exercice précédent.

2° Soit $d \in \mathbf{N}_n$ un diviseur de n. Montrer qu'il existe un et un seul sous-groupe de G dont le cardinal est d, et que ce sous-groupe admet $\varphi(d)$ générateurs. Retrouver la formule (2) de l'exercice précédent.

3° Montrer que le groupe Aut(G) des automorphismes de G est isomorphe au groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

1° Soit $k \in \mathbf{N}_n$. Notons $\delta = k \wedge n$, et écrivons $k = \delta k'$ et $n = \delta n'$.

• Montrons : $G(a^k) = G(a^\delta)$.

- De $a^k = (a^\delta)^{k'}$ résulte $G(a^k) \subset G(a^\delta)$.

- D'après Bezout, il existe $(u,v) \in \mathbb{Z}^2$ tel que $\delta = uk + vn$, et donc $a^\delta = (a^k)^u$, ce qui entraîne $G(a^\delta) \subset G(a^k)$. □

• Pour tout $\ell \in \mathbf{N}_{n'}$, on a $\delta\ell \in \mathbf{N}_n$; les $a^{\delta\ell}$, $\ell \in \mathbf{N}_{n'}$, sont donc deux à deux distincts. En outre $a^{\delta n'} = e$ (élément neutre de G). D'où :

$$\text{card } G(a^k) = \text{card } G(a^\delta) = n' = \frac{n}{k \wedge n}$$

et a^k engendre G si, et seulement si ce cardinal est n, i.e. $k \wedge n = 1$. □

• Les générateurs de G dont donc les a^k tels que $k \in \mathbf{N}_n$ et $k \wedge n = 1$, i.e. tels que $k \in E_n$ (cf. exercice précédent). Ils sont au nombre de $\varphi(n)$. □

2° Pour $d = 1$, la proposition est vraie. En effet l'unique sous-groupe de G de cardinal 1 est $\{e\}$, et e en est l'unique générateur.

• Donnons-nous maintenant un diviseur d de n tel que $d \geqslant 2$, et considérons encore un générateur a de G.

- Supposons qu'il existe un sous-groupe G' de G de cardinal d. L'ensemble $\{\ell \in \mathbf{N}_{n-1} \mid a^\ell \in G'\}$ est non vide ; soit k son plus petit élément. On constate par division euclidienne, que l'on a $a^m \in G'$ si, et seulement si m est un multiple de k ; G' est ainsi cyclique, engendré par a^k ; $a^n \in G'$, n est multiple de k, et (cf. 1°) $d = n/(k \wedge n) = n/k$, et $k = n/d$.

- S'il existe un sous-groupe de G de cardinal d, c'est donc nécessairement $G(a^{n/d})$.

- Inversement $(n/d) \wedge n = n/d$, et $G(a^{n/d})$ est un sous-groupe de G de cardinal d. Il est cyclique et (d'après 1°) le nombre de ses générateurs est $\varphi(d)$.

• Tout élément de G ayant pour ordre un diviseur de n, le procédé fournit une fois et une seule chaque élément de G quand d parcourt l'ensemble $\mathfrak{T}$ des éléments de $\mathbf{N}_n$ qui divisent n. D'où : $\sum_{d \in \mathfrak{T}} \varphi(d) = n$. □

Remarque. Nous avons montré au passage que tout sous-groupe d'un groupe cyclique est, lui aussi, cyclique.

3° Nous reprenons un générateur a de G.

• Soit $u \in Aut(G)$. Tout $y \in G$ est l'image par u d'un élément de G que nous pouvons écrire a^q, $q \in \mathbb{Z}$; on a : $y = u(a^q) = (u(a))^q$. Il en résulte que u(a) est un générateur de G. D'où $u(a) = a^k$, avec $k \in E_n$ (cf. 1°).

Tout $x \in G$ s'écrit $x = a^p$, $p \in \mathbb{Z}$, et on a :

$$u(x) = u(a^p) = (u(a))^p = a^{kp} = x^k.$$

• Inversement, soit $k \in E_n$. Associons-lui $u_k : G \longrightarrow G$ par $x \longmapsto x^k$.

En utilisant la commutativité de G, on constate que u_k est un endomorphisme de G. Par ailleurs a^k est un générateur de G (à cause de $k \in E_n$). Tout $y \in G$ s'écrit $y = (a^k)^q$, $q \in \mathbb{Z}$, et donc $y = (a^q)^k = u_k(a^q)$; u_k est ainsi surjective, et donc bijective puisque G est de cardinal fini. On a donc : $u_k \in Aut(G)$.

• Nous venons de montrer : $Aut(G) = \{u_k \mid k \in E_n\}$. Or nous avons vu dans l'exercice précédent que l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est $U_n = \{\overline{k} \mid k \in E_n\}$. Il en résulte que $u_k \longleftrightarrow \overline{k}$ est une bijection de Aut(G) sur U_n. On vérifie aisément que c'est un morphisme de groupes.

Remarque. Aut(G) est donc un groupe commutatif de cardinal $\varphi(n)$.

1.1.9 1° Soient p et n des entiers naturels vérifiant : $1 \leqslant p < n$, et $s \in \mathfrak{S}_n$ la permutation : $s = (p+1,\ldots,n,1,\ldots,p)$.

On suppose cette permutation décomposée en cycles disjoints. Calculer le nombre de cycles obtenus, la longueur de chacun d'eux. Déterminer un élément (et un seul) dans chaque orbite.

2° (Application à l'informatique). On considère n mémoires $a_1,\ldots,a_n$ contenant des données $x_1,\ldots,x_n$. On désire leur substituer respectivement $x_{s(1)},\ldots,x_{s(n)}$ en utilisant seulement une mémoire supplémentaire M ($s \in \mathfrak{S}_n$).

a) Trouver un algorithme.

b) Dans le cas de la permutation s étudiée au 1°, calculer le nombre de transferts nécessaires.

1° D'après l'isomorphisme existant entre les groupes symétriques de deux ensembles équipotents, nous pouvons remplacer l'étude de s par celle d'une permutation s de $\mathbb{Z}/n\mathbb{Z}$. En rangeant ses éléments dans l'ordre naturel $(\overline{0},\ldots,\overline{n-1})$, s peut alors s'écrire : $s = (\overline{p},\ldots,\overline{n-1},\overline{0},\ldots\overline{p-1})$ et on constate :

$$\forall x \in \mathbb{Z}/n\mathbb{Z} \quad s(x) = x + \overline{p}. \tag{1}$$

Notons $\mathcal{O}(x)$ l'orbite de l'élément x de $\mathbb{Z}/n\mathbb{Z}$. Nous constatons que $\mathcal{O}(\overline{0})$ n'est autre que $gr(\overline{p})$, sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\overline{p}$, et que, compte tenu de (1) :

$$\forall x \in \mathbb{Z}/n\mathbb{Z} \quad \sigma(x) = x + gr(\overline{p}) \qquad (2)$$

Or, en reprenant, avec d'autres notations, le calcul de la première question de l'exercice précédent (ou en utilisant un isomorphisme), on obtient, δ désignant le PGCD de n et p :

$$gr(\overline{p}) = gr(\overline{\delta}) \text{ et card } gr(\overline{\delta}) = n/\delta.$$

En utilisant (2), on en déduit que chaque orbite a n/δ éléments, et donc qu'il y a δ orbites. D'autre part, toujours d'après (2), deux éléments x et y de $\mathbb{Z}/n\mathbb{Z}$ ont la même orbite si, et seulement si x-y appartient à $gr(\overline{p}) = gr(\overline{\delta})$.

Comme $\overline{0},\overline{1},\ldots,\overline{\delta-1}$ sont δ éléments distincts de $\mathbb{Z}/n\mathbb{Z}$ dont les différences mutuelles ne peuvent appartenir à $gr(\overline{\delta})$, leurs orbites sont les δ orbites recherchées.

• En revenant à la permutation $s = (p+1,\ldots,n,1,\ldots,p)$ initialement donnée, on peut affirmer qu'elle se décompose en un produit de δ cycles disjoints ($\delta = n \wedge p$) dont les supports, de longueur commune n/δ, sont les orbites de $1,\ldots,\delta$.

2° a) L'algorithme est immédiat lorsque s est un cycle de longueur n. Il s'agit de :

$$M := a_1 \; ; \quad a_1 := a_{s(1)} \; ; \; \ldots \; ; \; a_{s^{n-1}(1)} := M.$$

où une notation telle que $a_i := a_j$ signifie que l'on transfère le contenu de la mémoire a_j dans la mémoire a_i.

Il y a n+1 transferts. Dans le cas général, on décompose s en cycles et on applique l'algorithme précédent à chaque cycle.

b) Dans le cas de la permutation du 1°, il y a δ cycles de longueur n/δ. Il faudra donc $\delta(n/\delta+1) = n+\delta$ transferts.

Du point de vue pratique on appliquera un même algorithme δ fois, en partant successivement de $x_1,\ldots,x_\delta$. □

1.1.10 Soient G un groupe et $A \subset G$. Montrer que :

$$N(A) = \{x \in G \mid xAx^{-1} = A\} \text{ et } C(A) = \{x \in G \mid \forall a \in A \quad xax^{-1} = a\}$$

qui sont respectivement appelés *normalisateur* et *centralisateur* (ou *commutant*) de A dans G, sont des sous-groupes de G, et que C(A) est un sous-groupe distingué de N(A).

Montrer que, si A est un sous-groupe de G, alors N(A) est le plus grand sous-groupe de G qui contient A dans lequel A est distingué.

Exercice facile, laissé au lecteur. Il s'agit de notions qui interviennent dans l'étude d'un groupe opérant sur lui-même par conjugaison ; ces notions seront utilisées dans les deux exercices qui suivent.

Notons qu'en particulier C(G) est un sous-groupe distingué de N(G) = G ; C(G), qui s'écrit $\{x \in G \mid \forall a \in G \quad xa = ax\}$, est dit <u>centre</u> de G.

1.1.11 Soient G un groupe fini, et H un sous-groupe de G, distinct de G. A tout $x \in G$ on associe la partie $G(x) = xHx^{-1}$ de G. Montrer que la réunion $E = \bigcup_{x \in G} G(x)$ ne recouvre pas G.

• Commençons par noter que, pour $x \in G$ donné, G(x) est l'image du sous-groupe H de G par l'application $y \mapsto xyx^{-1}$ de G dans G qui est un automorphisme du groupe G (automorphisme intérieur). Il en résulte que G(x) est un sous-groupe de G et que :

$$\text{card } G(x) = \text{card } H < \text{card } G. \tag{1}$$

• Remarquons que, dans la réunion E, nous pouvons remplacer tous les G(x) qui sont égaux par l'un d'eux ; or, pour tout $(x,y) \in G^2$, G(x) = G(y) équivaut à $x^{-1}yH(x^{-1}y)^{-1} = H$, i.e. à $x^{-1}y \in N(H)$, où $N(H) = \{x \in G \mid xHx^{-1} = H\}$ est le normalisateur de H, qui est un sous-groupe de G contenant H, i.e. à $x \mathcal{R}_\gamma y$, où $\mathcal{R}_\gamma$ est l'équivalence à gauche dans le groupe G suivant le sous-groupe N(H).

• Choisissons un élément et un seul dans chacune des classes de l'ensemble quotient $G/\mathcal{R}_\gamma$; nous obtenons ainsi un ensemble X, et :

$$\text{card } X = \text{card } G/\text{card } N(H) \leqslant \text{card } G/\text{card } H. \tag{2}$$

Nous avons : $E = \bigcup_{x \in X} G(x)$, et donc (compte tenu de (1)) ;

$$\text{card } E \leqslant \text{card } X.\text{card } H \tag{3}$$

- Si card X = 1 (i.e. N(H) = G), (3) donne card E ⩽ card H < card G ; d'où $E \neq G$.

- Si card X ⩾ 2 (i.e. $N(H) \neq G$), nous avons strictement :

$$\text{card } E < \text{card } X.\text{card } H$$

(en effet les G(x) tels que $x \in X$ ont en commun l'élément neutre de G). D'où, d'après (2) : card E < card G, et $E \neq G$. □

1.1.12 1° a) Soit G un groupe. Montrer que la relation sur G :

$$(g \mathcal{R} g') \Leftrightarrow (\exists x \in G \quad g' = xgx^{-1})$$

est une relation d'équivalence.

b) Montrer que si G est fini, alors, pour tout $g \in G$, le cardinal de la classe $\overline{g}$ de g pour $\mathcal{R}$ est $[G : N(g)]$, où N(g) est le normalisateur de {g}.

2° Ici G est un groupe fini de cardinal p^n, p premier et $n \geqslant 1$.

Montrer que le centre C(G) n'est pas réduit à {e}.

En déduire que si n = 2, alors G est commutatif.

1° a) Pour montrer que $\mathcal{R}$ est une relation d'équivalence, il suffit de remarquer que, pour tous éléments g, g', g'', x, y de G on a :

$$g = ege^{-1} \; ; \; (g' = xgx^{-1}) \Rightarrow (g = x^{-1}g'x) \; ;$$

$$\big((g' = xgx^{-1}) \wedge (g'' = yg'y^{-1})\big) \Rightarrow \big(g'' = yxg(yx)^{-1}\big).$$

b) Ici G est fini et $g \in G$ est fixé. Il est clair que :

$$\overline{g} = \{xgx^{-1} \mid x \in G\}.$$

Or, pour tout $(x,y) \in G^2$, $xgx^{-1} = ygy^{-1}$ équivaut à $x^{-1}ygy^{-1}x = g$, i.e. à $x^{-1}y \in N(g)$, i.e. à $x\mathcal{R}_\gamma y$, où $\mathcal{R}_\gamma$ est l'équivalence à gauche dans le groupe G suivant le sous-groupe N(g).

Le cardinal de $\overline{g}$ est donc égal au nombre des classes de $G/\mathcal{R}_\gamma$, c'est-à-dire à l'indice de N(g) dans G. □

Notons que l'on a card $\overline{g} = 1$ si, et seulement si $N(g) = G$, ce qui s'écrit $g \in C(G)$.

2° Choisissons un élément et un seul dans chacune des classes de l'ensemble quotient $G/\mathcal{R}$. Nous obtenons ainsi un ensemble X composé de C(G) et éventuellement d'éléments $g_1, \ldots, g_q$ de G tels que, pour tout $i \in \mathbf{N}_q$, $\overline{g}_i$ ait pour cardinal un diviseur de card $G = p^n$ autre que 1, et donc un multiple de p.

Comme $\bigcup_{g \in X} \overline{g}$ est une partition de G, il vient :

$$\text{card } G = \text{card } C(G) + \sum_{i=1}^{q} \text{card } \overline{g}_i$$

ce qui montre que card C(G) est un multiple de p ; divisant p^n, c'est même un entier de la forme p^m, $1 \leqslant m \leqslant n$. □

• Ici card $G = p^2$. On a donc : card $C(G) \in \{p, p^2\}$.

Si l'on avait card C(G) = p, il existerait $a \in G \setminus C(G)$. On aurait $a \in N(a)$ et $a \notin C(G)$, si bien que l'inclusion $C(G) \subset N(a)$ (qui est générale) serait stricte; Excédant p et divisant p^2, le cardinal de N(a) serait p^2 ; on aurait N(a) = G et donc $a \in C(G)$ ce qui constituerait une contradiction.

En conclusion : card $C(G) = p^2$, et C(G) = G, et G est commutatif.

L'exercice qui suit fait intervenir le cours de Géométrie.

1.1.13 Soit $S = \{m = (x,y,z) \in \mathbf{R}^3 \mid P(m) = 1\}$ où $P(m) = x^3+y^3+z^3-3xyz$.

1° Etudier la loi interne sur $\mathbf{R}^3$ définie par $m \star m' = m''$, avec :

$$x'' = xx' + zy' + yz' \; ; \; y'' = yx' + xy' + zz' \; ; \; z'' = zx' + yy' + xz' \qquad (1)$$

Montrer que S est stable pour $\star$; étudier $(S,\star)$.

2° $\mathbf{R}^3$ étant muni de sa structure affine canonique, trouver les courbes continues C de la surface S telles que, pour tout couple (m,m') de points d'une C, le point $m \star m'$ appartienne à cette C. (On se limitera aux courbes paramétrées $t \longmapsto F(t)$, où F est une application continue de $\mathbf{R}$ dans $\mathbf{R}^3$).

1° On constate que (1) s'écrit :

$$\begin{bmatrix} x'' \\ y'' \\ z'' \end{bmatrix} = M(m) \begin{bmatrix} x' \\ y' \\ z' \end{bmatrix}, \text{ où } M(m) = \begin{bmatrix} x & z & y \\ y & x & z \\ z & y & x \end{bmatrix} \tag{2}$$

et que P(m) est le déterminant de la matrice M(m).

La question fait donc intervenir l'application $m \longleftrightarrow M(m)$ de $\mathbb{R}^3$ dans $\mathcal{M}_3(\mathbb{R})$, qui est visiblement linéaire et injective.

En calculant le produit matriciel M(m)M(m') on obtient :

$$\forall (m,m') \in (\mathbb{R}^3)^2 \quad M(m \star m') = M(m)M(m') \tag{3}$$

ce qui entraîne :

$$\forall (m,m') \in (\mathbb{R}^3)^2 \quad P(m \star m') = P(m)P(m') \tag{4}$$

et donc la stabilité de S pour la loi $\star$.

• Etudions la loi $\star$ sur $\mathbb{R}^3$. Elle est commutative d'après (1).

Pour tout $(m_1,m_2,m_3) \in (\mathbb{R}^3)^3$, on a, d'après (3) :

$$\begin{aligned} M((m_1 \star m_2) \star m_3) &= M(m_1 \star m_2)M(m_3) = M(m_1)M(m_2)M(m_3) \\ &= M(m_1)M(m_2 \star m_3) = M\big(m_1 \star (m_2 \star m_3)\big) \end{aligned}$$

et, d'après l'injectivité de l'application $m \mapsto M(m)$:

$$(m_1 \star m_2) \star m_3 = m_1 \star (m_2 \star m_3)$$

La loi $\star$ sur $\mathbb{R}^3$ est donc associative.

Il est clair (d'après (2)) qu'elle admet l'élément neutre $a = (1,0,0)$, qui appartient d'ailleurs à S. En utilisant (4) et (2) on constate que $m \in \mathbb{R}^3$ n'admet de symétrique que si $P(m) \neq 0$, le symétrique étant alors donné par :

$$\big(M(m)\big)^{-1} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

La loi $(\star)$ n'est donc pas symétrisable sur $\mathbb{R}^3$.

• En revanche, tout $m \in S$ admet un symétrique m^{-1}, et, d'après $P(m)P(m^{-1}) = 1$, on a $P(m^{-1}) = 1$ et donc $m^{-1} \in S$.

• En conclusion, $(\mathbb{R}^3,\star)$ n'est pas un groupe, mais S, muni de la loi induite, est un groupe commutatif.

2° Il est commode de considérer $\mathbb{R}^3$ comme affine euclidien, et de remarquer qu'il existe des rotations qui conservent S (en fait, S est *de révolution*).

Considérons donc les deux repères orthonormaux directs $(0;\varepsilon)$ canonique, et $(0;e)$ tel que $e_3 = \frac{1}{\sqrt{3}}(\varepsilon_1+\varepsilon_2+\varepsilon_3)$ et $\varepsilon_1 = \sqrt{\frac{2}{3}}\, e_1 + \frac{1}{\sqrt{3}}\, e_3$. Les coordonnées (x,y,z) cartésiennes dans $(0;\varepsilon)$ et (r,θ,Z) cylindriques dans $(0;e)$ sont liées par :

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{2}{3}} & 0 & \frac{1}{\sqrt{3}} \\ \frac{-1}{\sqrt{6}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} \\ \frac{-1}{\sqrt{6}} & \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{3}} \end{bmatrix} \begin{bmatrix} r\cos\theta \\ r\sin\theta \\ Z \end{bmatrix}$$

Le calcul du déterminant d'une matrice circulante (cf. 4.2.5 ci-dessous) donne : $P(m) = Q(m)\,R(m)\,\overline{R(m)}$, avec :

$$Q(m) = x+y+z = \sqrt{3}Z \quad \text{et} \quad R(m) = x+jy+j^2z = \sqrt{\frac{3}{2}}\,re^{i\theta}.$$

Par (1), on obtient :

$$Q(m*m') = Q(m)Q(m') \; ; \; R(m*m') = R(m)R(m').$$

On en déduit que, pour tous $m \in \mathbb{R}^3$ et $m' \in \mathbb{R}^3$ de coordonnées cylindriques (r,θ,Z) et (r',θ',Z'), $m*m'$ admet pour coordonnées cylindriques :

$$\left(r'' = \sqrt{\frac{3}{2}}\,rr',\ \theta'' = \theta+\theta',\ Z'' = \sqrt{3}\,ZZ'\right).$$

Par ailleurs S admet l'équation cylindrique $3\sqrt{3}\,Zr^2 - 2 = 0$, et est donc de révolution autour de $(0;e_3)$. On notera que, pour tout $m \in S$, on a $Z>0$ et $r^2>0$, ce qui (par continuité) permet d'imposer $r>0$ sur une courbe C.

Les courbes C sont ainsi les courbes représentées paramétriquement par :

$$[\theta \in \mathbb{R}] \wedge [r = f(\theta)] \wedge \left[Z = \frac{2}{3\sqrt{3}}\left(f(\theta)\right)^{-2}\right] \qquad (5)$$

où f est une application continue de $\mathbb{R}$ dans $\mathbb{R}_+^*$, qui vérifie :

$$\forall(\theta,\theta') \qquad f(\theta+\theta') = \sqrt{\frac{3}{2}}\,f(\theta)f(\theta')$$

ce qui, s'écrit, en posant $g(\theta) = \ell n\left(\sqrt{\frac{3}{2}}\,f(\theta)\right)$:

$$\forall(\theta,\theta') \qquad g(\theta+\theta') = g(\theta)+g(\theta')$$

ou encore (calcul classique) : $g(\theta) = k\theta$, $k \in \mathbb{R}$, et $f(\theta) = \sqrt{\frac{2}{3}}\exp(k\theta)$.

Les solutions sont toutes les courbes de S qui contiennent le point neutre a et se projettent orthogonalement sur le plan $Z=0$ suivant une spirale logarithmique de point asymptote 0, ou suivant un cercle de centre 0 (pour $k=0$).

1.2. Anneaux et Corps

Ce sous-chapitre commence par des exercices d'arithmétique.

1.2.1 Soit $n \in \mathbb{N}^*$. Calculer la somme $\Sigma\ 1/pq$, étendue à tous les couples d'entiers (p,q) vérifiant : $1 \leqslant p < q \leqslant n$, $p+q>n$, et $p \wedge q = 1$.

Nous noterons P_n l'ensemble des entiers compris entre 1 et n et premiers avec n, et $S_n = \sum_{(p,q)\in A_n} 1/pq$ où $A_n = \{(p,q) \in \mathbb{N}_n^2 \mid p \wedge q = 1 \; ; \; p+q>n\}$.

Nous allons étudier, pour un $n \in \mathbb{N}^*$ donné, les ensembles $A_{n+1} \setminus A_n$ et $A_n \setminus A_{n+1}$.

• Le couple (p,q) appartient à $A_{n+1} \setminus A_n$ si et seulement si :

$$[(p,q) \in \mathbb{N}_{n+1}^2 \quad \text{et} \quad p \wedge q = 1 \quad \text{et} \quad p+q > n+1]$$

et : $$[(p,q) \notin \mathbb{N}_n^2 \quad \text{ou} \quad p \wedge q \neq 1 \quad \text{ou} \quad p+q \leqslant n].$$

Mais un couple vérifiant les assertions de la première ligne ne peut pas vérifier $p \wedge q \neq 1$ ni $p+q \leqslant n$. Donc $A_{n+1} \setminus A_n$ est constitué des $(p,q) \in A_{n+1}$ pour lesquels $(p,q) \notin \mathbb{N}_n^2$, c'est-à-dire $p = n+1$ ou $q = n+1$. Autrement dit :

$$A_{n+1} \setminus A_n = \{(n+1,q) \mid q \in P_{n+1}\} \cup \{(p,n+1) \mid p \in P_{n+1}\} \qquad (1)$$

en notant bien que les deux ensembles sont *disjoints* ($n+1 \notin P_{n+1}$).

• Par un raisonnement analogue on constate :

$$A_n \setminus A_{n+1} = \{(p,q) \in \mathbb{N}_n^2 \mid p \wedge q = 1 \ ; \ p+q = n+1\}$$

ou encore : $A_n \setminus A_{n+1} = \{(p,n+1-p) \mid p \in \mathbb{N}_n \ ; \ p \wedge (n+1-p) = 1\}$. Or, pour tout $p \in \mathbb{N}_n$, on a : $(p \wedge (n+1-p)) = 1 \iff (p \wedge (n+1) = 1)$. Donc :

$$A_n \setminus A_{n+1} = \{(p,n+1-p) \mid p \in P_{n+1}\}$$

• Ecrivons alors : $S_{n+1} = S_n + \sum\limits_{A_{n+1} \setminus A_n} 1/pq - \sum\limits_{A_n \setminus A_{n+1}} 1/pq$

En utilisant le fait que les deux ensembles intervenant dans l'écriture (1) sont disjoints, il vient :

$$\sum_{(p,q) \in A_{n+1} \setminus A_n} 1/pq = (2/(n+1)) \sum_{p \in P_{n+1}} 1/p$$

De même :

$$\sum_{(p,q) \in A_n \setminus A_{n+1}} 1/pq = (1/n+1) \left[\sum_{p \in P_{n+1}} 1/p + \sum_{p \notin P_{n+1}} 1/(n+1-p) \right]$$

et, en remarquant que, pour tout $p \in \mathbb{N}_{n+1}$, $(p \in P_{n+1}) \iff (n+1-p \in P_{n+1})$:

$$\sum_{(p,q) \in A_n \setminus A_{n+1}} 1/pq = (2/(n+1)) \sum_{p \in P_{n+1}} 1/p$$

D'où, finalement :

$$\forall n \in \mathbb{N}^* \qquad S_{n+1} = S_n$$

et, compte tenu du résultat immédiat $S_1 = 1$:

$$\forall n \in \mathbb{N}^* \qquad S_n = 1.$$

• Pour revenir à la somme demandée par l'énoncé, on constate qu'elle est nulle pour $n = 1$, et que pour $n \geqslant 2$ elle vaut $S_n/2$, soit $1/2$. □

1.2.2 1° Soit $n \in \mathbb{N}^*$. Simplifier

$$S_n = \sum_{0 \leqslant j < k \leqslant n+1} C_n^j \, C_{n+1}^k$$

2° a) Soit $n \in \mathbb{N}^*$. Deux joueurs A et B disposent d'une pièce de monnaie telle qu'à chaque lancer la probabilité d'obtenir "face" soit 1/2 ; A lance n fois la pièce et relève le nombre a de tirages "face" ; puis B lance n+1 fois la pièce et relève le nombre b de tirages "face". Quelle est la probabilité π pour que $b > a$?

b) Utiliser 2° a) pour retrouver le résultat du 1°.

1° On a : $S_n = \sum_{0 \leqslant j < k \leqslant n+1} C_n^{n-j} \, C_{n+1}^{n+1-k}$.

On constate que : $0 \leqslant j < k \leqslant n+1$ s'écrit $0 \leqslant n+1-k \leqslant n-j \leqslant n$.

D'où : $S_n = \sum_{0 \leqslant k \leqslant j \leqslant n} C_n^j \, C_{n+1}^k$

et : $2S_n = \sum_{(j,k) \in I} C_n^j \, C_{n+1}^k$, où $I = \{0,..,n\} \times \{0,...,n+1\}$

et enfin : $S_n = \frac{1}{2} \left(\sum_{j=0}^{n} C_n^j \right) \cdot \left(\sum_{k=0}^{n+1} C_{n+1}^k \right) = \frac{1}{2} \cdot 2^n \cdot 2^{n+1} = 2^{2n}$.

2° a) On constate que : $0 \leqslant a < b \leqslant n+1$ s'écrit $0 \leqslant b' \leqslant a' \leqslant n$, où $a' = n-a$ et $b' = n+1-b$ sont les nombres de tirages "pile" de A et B respectivement ; π est donc la probabilité pour que $b' \leqslant a'$; il en résulte que $1-\pi$ est la probabilité pour que $a' < b'$; mais, d'après le rôle symétrique de pile et face, celle-ci est aussi π.

Finalement $\pi = 1-\pi$, et $\pi = 1/2$.

b) Nous allons maintenant chercher une expression de π par un dénombrement.

Il y a $2^{n+1} \times 2^n$ façons d'associer un tirage de B et un tirage de A.

Pour $k \in \mathbb{N}_{n+1}$ donné, il y a C_{n+1}^k possibilités pour B de tirer k "faces". A chacune d'elles on peut associer les possibilités pour A de tirer moins de k faces, qui sont au nombre de $\sum_{j=0}^{k-1} C_n^j$. D'où :

$$\pi = \frac{1}{2^{2n+1}} \sum_{k=1}^{n+1} C_{n+1}^k \left(\sum_{j=0}^{k-1} C_n^j \right) = \frac{1}{2^{2n+1}} S_n. \qquad \square$$

1.2.3 Soit un entier $n \geqslant 2$. Montrer que n est premier si et seulement s'il divise $1 + (n-1)!$ (théorème de Wilson).

La condition est suffisante. Par hypothèse n divise $1 + (n-1)!$. Or $1 + (n-1)!$ n'est divisible par aucun des entiers 2,...,n-1 (le reste de la division étant manifestement 1 dans chaque cas). Il en résulte que les seuls diviseurs de n dans $\mathbb{N}^*$ sont 1 et n, i.e. que n est premier. $\square$

La condition est nécessaire. Par hypothèse n est premier. Si $n=2$, il est clair que n divise $1+(n-1)!$ Supposons maintenant $n \geqslant 3$.

Soit F_n le corps $\mathbb{Z}/n\mathbb{Z}$. Dans $F_n^* = F_n \setminus \{0\}$, dont le cardinal est pair, on a $x = x^{-1}$ si et seulement $x^2 = \overline{1}$, soit $x = \overline{1}$ ou $x = -\overline{1} = \overline{n-1}$.

Les éléments $\overline{2},\ldots,\overline{n-2}$ de F_n^* peuvent donc s'associer deux à deux par paires du type $\{x,x^{-1}\}$, ce qui montre que le produit de ces éléments est $\overline{1}$. On en déduit : $\overline{(n-1)!} = \overline{n-1} = -\overline{1}$, i.e. $\overline{1+(n-1)!} = \overline{0}$, i.e. n divise $1+(n-1)!$ □

1.2.4 Montrer que si un entier naturel n vérifie l'une des assertions :

($\mathcal{A}_n$) k^2+k+n est premier pour tout entier $k \in [0, \sqrt{n/3}]$,

($\mathcal{B}_n$) k^2+k+n est premier pour tout entier $k \in [0,n-2]$,

alors n vérifie l'autre assertion.

On constate (en utilisant $k=0$) qu'aucune des deux assertions n'est vérifiée si n n'est pas premier.

a) Si $n=2$ (resp. $n=3$) il est clair que $\mathcal{A}_n$ et $\mathcal{B}_n$, qui sont confondues, sont vérifiées.

b) Dans la suite n est premier, tel que $n \geqslant 5$. En utilisant :

$$(n-2)^2-n/3 = (n-3)(n-4/3)$$

on obtient : $[0, \sqrt{n/3}] \subset [0,n-2]$, inclusion stricte.

Il en résulte que si $\mathcal{B}_n$ est vérifié, alors $\mathcal{A}_n$ l'est aussi.

c) Reste à considérer un nombre premier $n \geqslant 5$ qui vérifie $\mathcal{A}_n$, et à montrer qu'il vérifie $\mathcal{B}_n$. On raisonne par l'absurde, en supposant :

$$E_n = \{k \in \mathbb{N} \mid (k \in [0,n-2]) \wedge (k^2+k+n \text{ non premier})\} \neq \phi .$$

• E_n admet un plus petit élément ℓ, et l'on a : $\sqrt{n/3} < \ell \leqslant n-2$.

L'entier $\ell^2+\ell+n$, qui est non premier et excède 5, admet un plus petit diviseur premier d, et on constate : $d^2 \leqslant \ell^2+\ell+n$. On a :

$$d^2 \leqslant (n-2)^2 + (n-2) + n < n^2, \text{ et } d \leqslant n-1.$$

Dans le corps $\mathbb{Z}/d\mathbb{Z}$, le polynôme $X^2+X+\overline{n}$ admet $\overline{\ell}$ pour racine, et (par division euclidienne) il s'écrit $(X-\overline{\ell})(X+\overline{1}+\overline{\ell})$; il admet donc les seules racines $\overline{\ell}$ et $-\overline{1}-\overline{\ell}$ (par nécessairement distinctes) ; celles-ci sont représentées, de façon unique, par des entiers r et s tels que :

$$0 \leqslant r \leqslant s \leqslant d-1 \leqslant n-2$$

avec $r+s = d-1$, et donc $2r \leqslant d-1$.

Vérifiant $r^2+r+n \geqslant n > d$ et étant divisible par d, r^2+r+n est non premier ; r appartient à E_n et donc $\ell \leqslant r$. Comme $\overline{\ell} \in \{\overline{r},\overline{s}\}$, on ne peut avoir $0 \leqslant \ell < r < s$. D'où :

$\ell = r$ et donc $2\ell = 2r \leqslant d-1$.

Il vient :

$$(2\ell+1)^2 \leqslant d^2 \leqslant \ell^2+\ell+n.$$

Retenons $3\ell^2 \leqslant n-1-3\ell$, et a fortiori $3\ell^2 < n$, ce qui constitue une contradiction avec $\ell > \sqrt{n/3}$.

L'hypothèse $E_n \neq \phi$ est donc absurde. On a $E_n = \phi$. □

1.2.5 A tout $n \in \mathbb{N}^*$ on associe la somme $\sigma(n) \in \mathbb{N}^*$ de ses diviseurs. Trouver une condition nécessaire et suffisante pour que l'entier $\sigma(n)$ soit impair.

Soit $n \in \mathbb{N}^*$. Comme tout entier strictement positif, il s'écrit, d'une façon et d'une seule :

$$n = 2^\alpha a, \text{ avec } \alpha \in \mathbb{N} \text{ et } a \in \mathbb{N}^* \text{ impair.}$$

Les diviseurs de n sont tous les $2^\lambda \ell$ tels que $\lambda \in \{0,\ldots,\alpha\}$ et ℓ divise a (ce qui implique ℓ impair). D'où :

$$\sigma(n) = \sum_{\ell \mid a} \left(\sum_{\lambda=0}^{\alpha} 2^\lambda \right) \ell = (2^{\alpha+1} - 1)\sigma(a)$$

où $\sigma(a)$ est la somme des diviseurs de a.

Comme $2^{\alpha+1} - 1$ est impair, la parité de $\sigma(n)$ est celle de $\sigma(a)$, et aussi (les diviseurs de a étant tous impairs) celle du nombre $\nu(a)$ des diviseurs de a.

Si $a = 1$, on a $\nu(a) = 1$ et $\sigma(n)$ est impair.

Sinon on utilise l'unique décomposition en facteurs premiers :

$$a = p_1^{k_1} \ldots p_r^{k_r}, \text{ avec } p_i \geqslant 3 \text{ et } k_i \geqslant 1.$$

Les diviseurs de a sont les $p_1^{h_1} \ldots p_r^{h_r}$, avec $0 \leqslant h_i \leqslant k_i$, et :

$$\nu(a) = (1+k_1)\ldots(1+k_r).$$

Il en résulte que $\sigma(n)$ est impair si et seulement si chacun des k_i est pair.

En conclusion, $\sigma(n)$ est impair si, et seulement si n est de la forme $2^\alpha q^2$, avec q impair. □

1.2.6 On donne le nombre premier p et on note :

$$Q_p = \left\{ \frac{a}{b} \mid (a,b) \in \mathbb{Z} \times \mathbb{N}^*,\ a \wedge b = 1,\ p \text{ ne divise pas } b \right\}.$$

Montrer que Q_p est un anneau principal.

• Nous laissons au lecteur le soin de vérifier que Q_p est un sous-anneau de $\mathbb{Q}$, et donc un anneau intègre.

Reste à vérifier que tout idéal de Q_p est principal, ce qui est évidemment vrai pour l'idéal réduit à $\{0\}$.

• Considérons donc un idéal I de Q_p, non réduit à $\{0\}$.

A tout élément a/b de $I \setminus \{0\}$ nous associons l'unique entier naturel m tel que p^m divise a et p^{m+1} ne divise pas a (avec éventuellement $m = 0$).

Quand a/b parcourt $I \setminus \{0\}$, m parcourt une partie non vide de $\mathbb{N}$; celle-ci admet un plus petit élément k.

- Il existe un élément a/b de $I \setminus \{0\}$ tel que $a = p^k a'$, avec a' non divisible par p et non nul. On constate que l'un des rationnels b/a' ou (-b)/(-a') appartient à Q_p. Le produit de ce rationnel par a/b, qui est p^k, appartient donc à I.

Retenons que l'idéal $p^k Q_p$ de Q_p est inclus dans I.

- Inversement soit a/b un élément quelconque de $I \setminus \{0\}$. Il existe $h \in \mathbb{N}$ et $a' \in \mathbb{Z}$ tels que :

$$\frac{a}{b} = p^k \frac{p^h a'}{b} .$$

On a : $(p^h a') \wedge b = 1$ et p ne divise pas b. D'où :

$$\frac{p^h a'}{b} \in Q_p \quad \text{et} \quad \frac{a}{b} \in p^k Q_p .$$

$I \setminus \{0\}$, et donc I est inclus dans $p^k Q_p$.

Finalement I est l'idéal principal $p^k Q_p$ de Q_p. □

1.2.7 Soient A un anneau commutatif et $\mathcal{J}$ l'ensemble des idéaux de A. On dit que $M \in \mathcal{J}$ est maximal si, et seulement s'il est maximal dans $(\mathcal{J} \setminus A, \subset)$.

1° Montrer que $M \in \mathcal{J}$ est maximal si, et seulement si A/M est un corps.

2° Ici l'anneau A est principal. Montrer que, pour tout $x \in A$, l'idéal (x) de A est maximal si, et seulement si x est irréductible (dans un anneau intègre A, dont l'ensemble des éléments inversibles est noté U, un élément x est irréductible si, et seulement s'il n'appartient pas à U et si ses seuls diviseurs sont les u et les ux, $u \in U$).

L'idéal $M \in \mathcal{J}$, $M \neq A$ est maximal si, et seulement si les seuls idéaux de A qui le contiennent sont M et A.

1° La condition est nécessaire. Soit M un idéal maximal de A. D'après $M \neq A$, A/M est un anneau commutatif non nul. Soient X un élément non nul de A/M, et x un représentant de X ; on a $x \notin M$.

$M + Ax$ est un idéal de A ; contenant $\{x\}$, il est distinct de M ; contenant M, il est égal à A. Il existe donc $(m,y) \in M \times A$ tel que $1_A = m + yx$, et X admet la classe de y pour inverse dans A/M.

L'anneau A/M, dont tout élément non nul est inversible, est un corps. □

La condition est suffisante. Soit M un idéal de A tel que A/M soit un corps. Puisque A/M a au moins deux éléments, on a $M \neq A$. Soit I un idéal de A

tel que $M \subset I$ et $M \neq I$. Il existe $x \in I$ tel que $x \notin M$; la classe X de x, distincte de l'élément nul de A/M, admet un inverse Y dans le corps A/M ; soit y un représentant de Y. On a $yx - 1_A \in M$, et, d'autre part $yx \in I$. D'où $1_A \in I$, et $A = I$.

L'idéal M de A est maximal. □

2° On remarque que, dans un anneau intègre A, les assertions : y divise x et $y \in U$ équivalent respectivement à : $(x) \subset (y)$, et $(y) = A$. On en déduit que $x \in A$ est irréductible si, et seulement si (x) est maximal dans $(\mathfrak{T} \setminus A, \subset)$ où $\mathfrak{T}$ est l'ensemble des idéaux principaux de A.

Si, en outre, A est principal, alors $\mathfrak{T} = \mathfrak{J}$. □

L'exercice suivant fait appel au Cours d'Analyse.

1.2.8 On note A l'anneau (commutatif) des applications continues de [0,1] dans **R**.

1° Soit $x \in [0,1]$. Montrer que $M(x) = \{f \in A \mid f(x) = 0\}$ est un idéal maximal de A.

2° On va montrer que tout idéal maximal J de A s'écrit $M(x_o)$, où x_o est un élément convenablement choisi de [0,1].

a) Soit I un idéal de A tel que $E_I = \bigcap_{f \in I} f^{-1}(0)$ soit vide. Montrer qu'il existe un élément de I ne prenant la valeur 0 en aucun point de [0,1]. En déduire I = A.

b) Conclure.

1° On vérifie aisément que M(x) est un idéal de A.

Soit I un idéal de A contenant M(x) et distinct de M(x). Il existe donc $f \in I \setminus M(x)$, et on a $f(x) \neq 0$. On note α l'élément $t \mapsto f(x)$ de A ; on constate que $f - \alpha$ est un élément de M(x), et donc de I ; d'où $\alpha \in I$; il en résulte que I contient l'application constante $t \mapsto 1$, et que $I = A$. □

2° a) Soit $x \in [0,1]$. D'après la vacuité de E_I, il existe $f_x \in I$ tel que $f_x(x) \neq 0$. D'après la continuité de f_x au point x, il existe un voisinage ouvert V_x de x dans **R** tel que : $0 \notin f_x(V_x \cap [0,1])$.

Du recouvrement du compact [0,1] par la famille $(V_x)_{x \in [0,1]}$ d'ouverts, on peut extraire un recouvrement par une famille finie $(V_{x_i})_{1 \leqslant i \leqslant n}$; $g = f_{x_1}^2 + \ldots + f_{x_n}^2$, qui est visiblement un élément de I, ne prend la valeur 0 en aucun point de [0,1] ; $h : x \longrightarrow 1/g(x)$ est inverse de g dans l'anneau A. On a $hg = 1_A$ et $hg \in I$. D'où $1_A \in I$, et $I = A$.

b) Soit J un idéal maximal de A. On a $J \neq A$, et donc E_J n'est pas vide (cf. a)) ; il existe $x_o \in E_J$; on a $f(x_o) = 0$ pour tout $f \in J$, et donc $J \subset M(x_o)$. Comme $M(x_o) \neq A$ et comme J est maximal, ceci exige $J = M(x_o)$. □

1.2.9 Soit A un anneau commutatif. Un idéal premier de A est un idéal P distinct de A, et tel que :

$$\forall (x,y) \in A^2 \quad (xy \in P) \Rightarrow (x \in P) \vee (y \in P)$$

1° Montrer qu'un idéal P de A est premier si, et seulement si A/P est un anneau intègre.

2° Donner un exemple d'idéal non nul, premier et non maximal.

1° Pour tout idéal $P \neq A$ de A, A/P est un anneau commutatif non nul.

La condition est nécessaire. Soit P un idéal premier de A.

Considérons deux éléments X et Y de l'anneau non nul A/P tels que $XY = 0$; soient x et y des représentants de X et Y ; xy est un représentant de XY, et donc $xy \in P$; il en résulte $(x \in P) \vee (y \in P)$, i.e. $(X = 0) \vee (Y = 0)$.

L'anneau A/P est ainsi intègre. □

La condition est suffisante. Soit P un idéal de A, non premier, distinct de A. On dispose de $(x,y) \in A^2$ tel que :

$$(xy \in P) \wedge (x \notin P) \wedge (y \notin P)$$

Les classes X et Y de x et y vérifient :

$$(XY = 0) \wedge (X \neq 0) \wedge (Y \neq 0)$$

L'anneau A/P n'est donc pas intègre. □

2° Il est clair que, dans tout anneau commutatif A, tout idéal maximal est premier. La réciproque est fausse : si A est intègre sans être un corps, l'idéal {0} est premier sans être maximal.

Voici un contre-exemple non trivial. On considère l'idéal (X) de K[X,Y] engendré par le polynôme X. C'est le noyau du morphisme d'anneaux $u : Q(X,Y) \longmapsto Q(0,Y)$ de K[X,Y] dans K[Y]. L'anneau K[X,Y]/(X), isomorphe à l'image K[Y] de u, est un anneau intègre, mais n'est pas un corps. □

Remarque. Dans un anneau commutatif, un élément premier est un élément non nul p tel que l'idéal (p) de A soit premier. Le lecteur vérifiera aisément que tout élément premier d'un anneau intègre est irréductible, et que, dans un anneau principal, les éléments premiers sont les éléments irréductibles.

1.2.10 Montrer que le sous-anneau $A = \mathbb{Z} + i\mathbb{Z}$ de $\mathbb{C}$ est principal.

• Il est clair que $A = \{u+iv \mid (u,v) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$, et donc un anneau intègre.

• Soit I un idéal non nul de A ; $\{|z|^2 \mid z \in I \setminus \{0\}\}$ est une partie non vide de $\mathbb{N}$, et admet donc un plus petit élément ; il existe $z_0 \in I \setminus \{0\}$ tel que $|z| \geqslant |z_0|$ pour tout $z \in I \setminus \{0\}$; I étant un idéal, on a $Az_0 \subset I$.

- Inversement soit $z \in I$. La division dans $\mathbb{C}$ de z par z_o fournit $z = (a+ib)z_o$, avec $(a,b) \in \mathbb{R}^2$. En s'aidant d'une figure, le lecteur vérifiera qu'il existe $(u,v) \in \mathbb{Z}^2$ tel que $|a+ib-(u+iv)| < 1$. En utilisant : $z - z_o(u+iv) \in I$, et en posant $\alpha = a-u$ et $\beta = b-v$, il vient :

$$(\alpha+i\beta)z_o \in I \quad \text{et} \quad |(\alpha+i\beta)z_o| < |z_o|$$

ce qui exige (d'après la définition de z_o) : $\alpha+i\beta = 0$, et donc $z \in Az_o$.

En conclusion $I = Az_o$. L'idéal I est principal. □

1.2.11 Soit un entier premier de la forme $p = 4n+1$, $n \in \mathbb{N}^*$.

1° Montrer qu'il existe $u \in \mathbb{Z}$ tel que $u^2+1 \equiv 0 \pmod p$.

2° Montrer que p est somme de deux carrés.

1° Le corps $F_p = \mathbb{Z}/p\mathbb{Z}$ étant fini, d'après 1.1.6 le groupe multiplicatif F_p^* est cyclique, de cardinal $p-1 = 4n$. Soit α un générateur de ce groupe ; on a $\alpha^{4n} = 1$ et $\alpha^{2n} \neq 1$; d'où $\alpha^{2n} = -1$.

L'élément α^n de F_p est donc la classe (modulo p) d'un entier $u \in \mathbb{Z}$ qui vérifie $u^2+1 \equiv 0 \pmod p$.

2° Il résulte du 1° que, dans l'anneau intègre $A = \mathbb{Z}+i\mathbb{Z}$, l'élément p divise le produit $(u+i)(u-i)$; or il ne divise ni $u+i$, ni $u-i$ (car les nombres complexes $\frac{u+i}{p}$ et $\frac{u-i}{p}$ n'appartiennent pas à A) ; l'idéal (p) de A n'est donc pas premier, et, a fortiori, il n'est pas maximal ; l'élément p de l'anneau principal A n'est pas irréductible (cf. 1.2.9 et 1.2.7) ; il existe donc deux éléments non inversibles de A dont le produit est p, soit

$$p = (a+ib)(a'+ib'), \quad a^2+b^2 \neq 1 \quad \text{et} \quad a'^2+b'^2 \neq 1.$$

En passant au carré des modules, il vient $p^2 = (a^2+b^2)(a'^2+b'^2)$; comme p est un entier premier, il en résulte $p = a^2+b^2$.

1.2.12 Résoudre et discuter l'équation sur $F_{17} = \mathbb{Z}/17\mathbb{Z}$:

$$x^2 - \overline{3}x + k = 0 \qquad (E)$$

dans laquelle $k \in F_{17}$ est un paramètre.

Comme 17 est premier, F_{17} est un corps commutatif ; (E) a donc au plus deux solutions ; (E) s'écrit :

$$(x-\overline{10})^2 = \overline{15}-k$$

ce qui nous conduit à calculer l'ensemble F' des carrés des éléments de F_{17}, qui

est l'ensemble des carrés des éléments de $\{\overline{0},\ldots,\overline{8}\}$, à savoir :

$$F' = \{\overline{0},\overline{1},\overline{2},\overline{4},\overline{8},\overline{9},\overline{13},\overline{15},\overline{16}\}.$$

D'où la discussion.

1er cas : $\overline{15}-k \notin F'$, i.e. $k \in \{\overline{1},\overline{3},\overline{4},\overline{5},\overline{8},\overline{9},\overline{10},\overline{12}\}$; alors E n'admet pas de solution.

2ème cas : $k = \overline{15}$; alors (E) admet $\overline{10}$ pour solution unique.

3ème cas : $\overline{15}-k \in F' \setminus \{0\}$, i.e. $k \in \{\overline{0},\overline{2},\overline{6},\overline{7},\overline{11},\overline{13},\overline{14},\overline{16}\}$; alors $\overline{15}-k$ est le carré de deux éléments opposés et non nuls, ω et $-\omega$, de F_{17}, et (E) admet deux solutions, $\overline{10}+\omega$ et $\overline{10}-\omega$.

1.2.13 Soient L un corps commutatif et K un sous-corps de L. On dit que $a \in L$ est *algébrique* ou *transcendant* sur K selon qu'il existe ou qu'il n'existe pas un polynôme non nul de $K[X]$ admettant a pour racine.

On note A l'ensemble des éléments de L qui sont algébriques sur K.

1° a) Soit $a \in L$. Prouver l'équivalence des deux assertions :

i) a est algébrique sur K ;

ii) L_K désignant L muni de sa structure de K-espace vectoriel, le sous-espace $K[a] = \{P(a) \in L \mid P \in K[X]\}$ de L_K est de dimension finie.

b) Montrer que A est un sous-corps de L.

2° a) Soit $a \in A$. Montrer qu'il existe un unique polynôme $P_o \in K[X] \setminus \{0\}$ unitaire, irréductible dans $K[X]$, et tel que $P_o(a) = 0$.

Vérifier : $\dim_K K[a] = \deg P_o$.

b) Soit $a \in A$. Montrer que $K[a]$ est le plus petit sous-corps de L contenant K et a.

c) Montrer que si L est algébriquement clos, alors A est algébriquement clos.

3° Ici $L = \mathbb{C}$ et $K = \mathbb{Q}$.

a) Montrer que le corps A est dénombrable et algébriquement clos.

b) Montrer que le plus petit sous-corps M de $\mathbb{C}$ qui contient $\sqrt{2}$ et i est un $\mathbb{Q}$-espace vectoriel dont on donnera une base.

1° a) La loi externe sur L_K est celle qui à $(\alpha,x) \in K \times L$ associe $\alpha x \in L$.

- Il est clair que $K[a]$ est le sous-espace vectoriel de L_K engendré par la famille $(a^n)_{n\in\mathbb{N}}$.

- Notons que $K[a]$ contient a et tout $\alpha \in K$ (qui est $P(a)$ pour $P = \alpha \in K[X]$).

Preuve de i) $\Rightarrow$ ii). Par hypothèse, il existe $P \in K[X] \setminus \{0\}$ tel que $P(a) = 0$, ce qui entraîne que le degré p de P vérifie $p \geqslant 1$.

Pour tout $n \in \mathbb{N}$, effectuons la division euclidienne de X^n par P ; comme il s'agit de polynômes à coefficients dans K, le reste R_n, de degré $\rho_n < p$, est

à coefficients dans K. On a $a^n = R_n(a)$, ce qui montre que a^n appartient au sous-espace de L_K qui est engendré par $(1,a,\ldots,a^{p-1})$; K[a] est donc confondu avec ce sous-espace, qui est de dimension finie $q \leqslant p$.

Preuve de ii) ⇒ i). Par hypothèse, K[a] est de dimension finie q.

La famille $(1,a,\ldots,a^q)$ de q+1 éléments de K[a] est liée ; il existe q+1 éléments non tous nuls $\alpha_o,\alpha_1,\ldots,\alpha_q$ de K tels que $\alpha_o+\alpha_1 a+\ldots+\alpha_q a^q = 0$.

$P = \alpha_o+\alpha_1 X+\ldots+\alpha_q X^q$ est donc un élément non nul de K[X] tel que $P(a) = 0$. □

b) A contient K (tout $a \in K$ est racine du polynôme X-a) ; il contient donc -1.

- Soient a et b deux éléments de A. Les sous-espaces vectoriels K[a] et K[b] de L_K sont de dimension finie.

Soit V le sous-espace de L_K engendré par la famille $(a^m b^n)_{(m,n)\in\mathbb{N}^2}$.

Pour tout $m \in \mathbb{N}$ (resp. $n \in \mathbb{N}$), a^m (resp. b^n) est une combinaison linéaire à coefficients dans K d'une famille finie :

$(1,a,\ldots,a^{p-1})$ [resp. $(1,b,\ldots,b^{q-1})$].

Il en résulte que, pour tout $(m,n)\in\mathbb{N}^2$, $a^m b^n$ est une combinaison linéaire à coefficients dans K des $a^i b^j$, $(i,j) \in \{0,\ldots,p-1\} \times \{0,\ldots,q-1\}$, et donc que V est de dimension finie.

Or V contient les sous-espaces K[a+b] et K[ab] de L_K ; a+b et ab sont donc algébriques sur K.

A ce stade, nous pouvons affirmer que A est un sous-anneau de L.

- Soit a un élément non nul de A, racine de $P \in K[X]$ de degré $p \geqslant 1$; $X^p P(1/X)$ est un polynôme non nul de K[X] qui admet 1/a pour racine ; 1/a est donc algébrique sur K.

- A ce stade, nous pouvons affirmer que A est un sous-corps de L.

2° Soit $a \in L$. On note K(a) le plus petit sous-corps de L qui contient K et a ; K(a) contient K[a], c'est donc le plus petit sous-corps de L qui contient K[a] (lequel contient a et K).

L'application $\varphi : P \mapsto P(a)$ de K[X] dans K(a) est un morphisme d'anneaux. Son noyau, $I = \{P \in K[X] \mid P(a) = 0\}$ est un idéal de l'anneau principal K[X] ; son image K[a] est un sous-anneau de K(a) isomorphe à K[X]/I.

• Si $a \notin A$, alors $I = \{0\}$ et $K[a] \simeq K[X]$; le corps K(a) est isomorphe au corps K(X) des fractions de K[X] (corps des fractions rationnelles).

a) Dans la suite : $a \in A$. Il existe ici un unique polynôme unitaire $P_o \in K[X]$ tel que $I = (P_o)$; on a $\deg P_o \geqslant 1$ (à cause de $P_o \neq 0$ et $P_o(a) = 0$).

P_o est irréductible dans K[X] car, s'il existait deux éléments P_1 et P_2 de K[X] de produit P tels que $\deg P_1 < \deg P_o$ et $\deg P_2 < \deg P_o$, on aurait

$P_1(a)P_2(a) = 0$ et, L étant un corps, P_1 ou P_2 appartiendrait à I, ce qui constituerait une contradiction sur les degrés.

P_o est enfin le seul élément unitaire et irréductible de (P_o).

• On a vu au 1° que : $\dim_K K[a] \leqslant p_o$, où $p_o = \dim P_o$. D'autre part la famille $(1,a,\ldots,a^{p_o-1})$ est libre (sinon il existerait un élément de $I \setminus \{0\}$ de degré strictement inférieur à p_o). Il en résulte : $\dim_K K[a] = p_o$. □

b) Toujours dans le cas $a \in A$, nous allons montrer que $K[a]$ est un sous-corps de $K(a)$, ce qui entraînera $K[a] = K(a)$. Il suffit de montrer que l'inverse dans $K(a)$ de tout élément non nul du sous-anneau $K[a]$ est dans $K[a]$.

Soit $b \in K[a] \setminus \{0\}$. L'application $x \mapsto bx$ du K-espace vectoriel $K[a]$ dans lui-même est visiblement K-linéaire et injective ; s'agissant d'un espace vectoriel de dimension finie, elle est surjective : il existe $b' \in K[a]$ vérifiant $bb' = 1$. □

Autre solution de b). Ici P_o étant irréductible, $I = (P_o)$ est maximal (cf. 1.2.7) et $K[X]/I$ est un corps. Par isomorphisme, $K[a]$ est un corps.

c) LEMME. Soient U,V,W des corps commutatifs tels que $U \subset V \subset W$. On suppose que les espaces vectoriels V_U et W_V sont de dimension finie. Alors l'espace vectoriel W_U est de dimension finie, et $\dim W_U = \dim W_V \dim V_U$.

Soient $(\lambda_1,\ldots,\lambda_n)$ et $(\mu_1,\ldots,\mu_m)$ des bases de V_U et W_V. Tout $x \in W$ s'écrit $\sum_{j=1}^{m} \alpha_j \mu_j$, avec $\alpha_j \in V$, et donc $\alpha_j = \sum_{i=1}^{n} \alpha_{ij}\lambda_i$ avec $\alpha_{ij} \in U$: d'où :

$$x = \sum_{i,j} \alpha_{ij}\lambda_i\mu_j, \quad (i,j) \in \mathbf{N}_n \times \mathbf{N}_m, \ \alpha_{ij} \in U.$$

Dans cette égalité, on a $x = 0$ si et seulement si $\sum_j \left(\sum_i \alpha_{ij}\lambda_i\right) \mu_j = 0$, ce qui s'écrit : $\sum_i \alpha_{ij}\lambda_i = 0$ pour tout j, et $\alpha_{ij} = 0$ pour tout (i,j). La famille $(\lambda_i\mu_j)_{(i,j)\in \mathbf{N}_n \times \mathbf{N}_m}$ est donc une base de W_U. □

• Reprenons K, L et A, avec ici : L est algébriquement clos. Pour montrer que A est algébriquement clos, il faut montrer que tout polynôme non constant de $A[X]$ a au moins une racine dans A.

Soit $a_o + a_1X + \ldots + a_pX^p$, $a_i \in A$, $p \geqslant 1$, un tel polynôme, qui sera noté P.

Au titre d'élément de $L[X]$, il admet une racine α. Nous allons montrer $\alpha \in A$. La proposition en résultera.

Opérons pour "extensions successives" :

- Partons de $K[a_o]$, plus petit sous-corps de L qui contient K et a_o ; c'est un K-espace vectoriel de dimension finie.

- Algébrique sur K, a_1 est algébrique sur le sur-corps $K[a_o]$ de K. Notons $K[a_o,a_1]$ le corps $(K[a_o])[a_1]$ (on vérifie que c'est le plus petit sous-corps de L qui contient K, a_o et a_1) ; c'est un $K[a_o]$-espace vectoriel de dimension finie et, d'après le lemme, un K-espace vectoriel de dimension finie.

- De proche en proche, nous arrivons à $M = K[a_o,\ldots,a_p]$ (plus petit sous-corps de L qui contient $K,a_o,\ldots,a_p$), et nous constatons que c'est un K-espace vectoriel de dimension finie.

- Au titre de racine du polynôme non nul P à coefficients dans M, α est algébrique sur M, et d'après 1°, le corps $M[\alpha]$ est un M-espace vectoriel de dimension finie. En utilisant le lemme, on constate que $M[\alpha]$ est un K-espace vectoriel de dimension finie ; d'après $K \subset M$, le K-espace vectoriel $K[\alpha]$ en est un sous-espace, et est donc de dimension finie, ce qui, d'après 1°, donne : $\alpha \in A$. □

3° a) Ici $L = \mathbb{C}$, algébriquement clos, et $K = \mathbb{Q}$. D'après ce qui précède, le corps A des nombres complexes algébriques (éléments de $\mathbb{C}$ algébriques sur $\mathbb{Q}$) est algébriquement clos.

A tout $n \in \mathbb{N}^*$, associons l'ensemble A_n des éléments de A qui sont racines d'un polynôme de $Q[X]$ de degré n. On a : $A = \bigcup_{n \in \mathbb{N}^*} A_n$.

Soit $n \in \mathbb{N}^*$. $\mathbb{Q}$ étant dénombrable, $\mathbb{Q}^{n+1}$ est dénombrable ; l'ensemble des polynômes de $Q[X]$ de degré n, qui est une partie de $\mathbb{Q}^{n+1}$, est dénombrable, et comme chacun d'eux a au plus n racines dans $\mathbb{C}$, il est clair que A_n est dénombrable.

Réunion dénombrable d'une famille d'ensembles dénombrables, A est dénombrable. □

Notons que, $\mathbb{C}$ étant non dénombrable et A dénombrable, $\mathbb{C} \setminus A$ n'est pas vide : il existe des nombres complexes transcendants (sur $\mathbb{Q}$).

Remarquons d'autre part que $a \in \mathbb{C}$ est algébrique (sur $\mathbb{Q}$) si, et seulement s'il est racine d'un polynôme non nul de $\mathbb{Z}[X]$.

b) Tout sous-corps de $\mathbb{C}$ contient $\mathbb{Z}$, et donc le corps des fractions de $\mathbb{Z}$, qui est $\mathbb{Q}$; M est ainsi le plus petit sous-corps de $\mathbb{C}$ qui contient $\mathbb{Q}$, $\sqrt{2}$ et i.

Racines des polynômes X^2-2 et X^2+1, à coefficients dans $\mathbb{Q}$, $\sqrt{2}$ et i sont algébriques sur $\mathbb{Q}$, et, avec la notation du 2° c), $M = K[i]$ où $K = \mathbb{Q}[\sqrt{2}]$.

K est le sous-espace de $\mathbb{C}_{\mathbb{Q}}$ engendré par $\left((\sqrt{2})^n\right)_{n \in \mathbb{N}}$, et aussi par $(1, \sqrt{2})$; en effet tout $(\sqrt{2})^n$ appartient à $\mathbb{Q}$ ou à $\mathbb{Q}\sqrt{2}$. Mais la famille $(1, \sqrt{2})$ est libre dans $\mathbb{C}_{\mathbb{Q}}$, sinon $\sqrt{2}$ serait rationnel ; c'est donc une base de l'espace vectoriel $K_{\mathbb{Q}}$.

M est le sous-espace de $\mathbb{C}_K$ engendré par $(i^n)_{n \in \mathbb{N}}$, et aussi par $(1,i)$; en effet tout i^n appartient à K ou à Ki. Mais la famille $(1,i)$ est libre dans $\mathbb{C}_K$, sinon i serait réel ; c'est donc une base de l'espace vectoriel M_K.

D'après le lemme du 2° c), dans lequel on a fait $U = \mathbb{Q}$, $V = K$ et $W = M$, $(1, \sqrt{2}, i, i\sqrt{2})$ est une base de $M_{\mathbb{Q}}$. Le plus petit sous-corps de $\mathbb{C}$ qui contient $\sqrt{2}$ et i est ainsi :

$$\{\alpha + \beta\sqrt{2} + \gamma i + \delta i\sqrt{2} \mid (\alpha,\beta,\gamma,\delta) \in \mathbb{Q}^4\}.$$ □

L'exercice qui suit fournit un exemple de nombres réels transcendants.

1.2.14 1° Soient a un réel algébrique (sur $\mathbb{Q}$), et $P = c_0 + c_1X + \ldots + c_nX^n$, $n \geqslant 1$ et $c_n \neq 0$, un élément de $\mathbb{Z}[X]$ tel que $P(a) = 0$.

Vérifier : $|a| < \mu+1$, où $\mu = \max_{i\in\{0,\dots,n-1\}} |c_i/c_n|$.

En déduire que l'on peut associer à (a,P) un $N\in\mathbb{N}^*$ vérifiant :

i) Pour tous entiers $q \geqslant N$ et $p\in\mathbb{Z}$ tels que $|a-p/q| \leqslant 1/q$, on a :

$$\left(P(p/q) = 0\right) \vee \left(|a-p/q| > 1/q^{n+1}\right)$$

2° On appelle nombre de Liouville tout réel de la forme :

$$a = \sum_{k=1}^{+\infty} \alpha_k \, 10^{-k!} \qquad (1)$$

où $(\alpha_k)_{k\in\mathbb{N}^*}$ est une suite d'éléments de $\{0,\dots,9\}$ telle que $\{k\in\mathbb{N}^* \mid \alpha_k \neq 0\}$ soit infini.

Montrer qu'un tel réel est transcendant (sur $\mathbb{Q}$).

3° Montrer que l'ensemble F des nombres de Liouville est non dénombrable.

1° Si $a=0$, il est clair que $|a| < \mu+1$. Sinon on a $a\neq 0$; on écrit :

$$-1 = \frac{c_{n-1}}{c_n}\frac{1}{a} + \dots + \frac{c_o}{c_n}\frac{1}{a^n}$$

et on constate que l'hypothèse $|a| \geqslant \mu+1$ entraînerait :

$$1 \leqslant \mu \sum_{j=1}^{n} (\mu+1)^{-j} < \mu \sum_{j=1}^{+\infty} (\mu+1)^{-j} = 1$$

et conduirait donc à une contradiction. □

• Soit $(q,p)\in\mathbb{N}^* \times \mathbb{Z}$ tel que $|a-p/q| \leqslant 1/q$, et $P(p/q)\neq 0$.

On écrit $P(p/q) = c/q^n$, $c\in\mathbb{Z}^*$, et compte tenu de $P(a)=0$, on a, par la formule des accroissements finis :

$$-c/q^n = (a-p/q)P'(\xi)$$

où ξ est un réel compris entre a et p/q, et donc tel que $|\xi| \leqslant |a| + 1/q$ et à fortiori tel que $|\xi| < \mu+2$. On a ainsi :

$$|P'(\xi)| < \sum_{j=1}^{n} j|c_j|(\mu+2)^{j-1} = M, \text{ où } M\in\mathbb{R}_+^* \text{ est connu,}$$

et donc :

$$\left|a - \frac{p}{q}\right| > \frac{|c|}{Mq^n} \geqslant \frac{1}{Mq^n}.$$

- Tout entier $N \geqslant M$ répond donc à la question.

2° On note E l'ensemble des suites $(\alpha_k)_{k\in\mathbb{N}^*}$ d'éléments de $\{0,\dots,9\}$ qui ne sont pas tous des 0 à partir d'un certain rang.

• Soit $(\alpha_k)\in E$; (1) lui associe la somme a d'une série à termes réels positifs qui converge pour être majorée par la série géométrique convergente $\sum_{k\geqslant 1} 9.10^{-k}$.

- A tout $m \in \mathbb{N}^*$, associons $(q_m, p_m) \in \mathbb{N}^* \times \mathbb{N}$ par :

$$q_m = 10^{m!}, \quad p_m = q_m \sum_{k=1}^{m} \alpha_k \, 10^{-k!}$$

La suite $m \mapsto p_m/q_m$ est croissante et non stationnaire (sans quoi on aurait $\alpha_k = 0$ à partir d'un certain rang) ; elle a donc une infinité d'éléments distincts.

Pour m donné, le réel $r_m = a - p_m/q_m$ vérifie $r_m > 0$ et :

$$r_m \leqslant 9 \sum_{k=m+1}^{+\infty} 10^{-k!} < 9.10^{-(m+1)!} \sum_{h=0}^{+\infty} 10^{-h}$$

et : $$r_m < 10^{1-(m+1)!} \leqslant (10^{-m!})^m = q_m^{-m} .$$

- Faisons l'hypothèse : a est algébrique. Il existe $P \in \mathbb{Z}[X]$ de degré $n \geqslant 1$, tel que $P(a) = 0$. Il existe donc $N \in \mathbb{N}^*$, associé à (a,P) vérifiant i) (cf. 1°).

On décèle une contradiction en donnant au couple (q,p) qui intervient dans i) la valeur (q_m, p_m) où m est tel que $m \geqslant n+1$, que $q_m \geqslant N$ et que p_m/q_m ne soit pas racine de P (comme P n'a qu'un nombre fini de racines, il existe une infinité de tels m). Notre hypothèse est donc absurde. □

3° Nous allons montrer que d'une part l'application $\psi : (\alpha_k) \mapsto \sum_{k=1}^{+\infty} \alpha_k 10^{-k!}$ de E dans F, qui est surjective par définition, est injective et donc bijective, que d'autre part l'application $\varphi : (\alpha_k) \mapsto \sum_{k=1}^{+\infty} \alpha_k 10^{-k}$ de E dans]0,1] est bijective. Il en résultera que $\varphi \circ \psi^{-1}$ est une bijection de F sur]0,1], et que, comme]0,1], F est non dénombrable.

Preuve de l'injectivité de ψ. Soient (α_k) et (β_k) deux éléments distincts de E : il existe $m \in \mathbb{N}^*$ tel que $\alpha_k = \beta_k$ pour tout $k < m$, et, par exemple : $0 \leqslant \beta_m < \alpha_m \leqslant 9$. On a :

$$\psi((\alpha_m)) - \psi((\beta_m)) = (\alpha_m - \beta_m)\, 10^{-m!} + \rho_m \geqslant 10^{-m!} + \rho_m$$

avec :

$$|\rho_m| \leqslant 9 \sum_{k=m+1}^{+\infty} 10^{-k!} < (10^{-m!})^m \leqslant 10^{-m!}$$

D'où : $\psi((\alpha_m)) - \psi((\beta_m)) > 0$.

Preuve de l'injectivité de φ. Même méthode.

Preuve de la surjectivité de φ. Soit $t \in]0,1]$. Posons $x = 1 - t \in [0,1[$. On sait (existence du développement décimal propre de x) qu'il existe une suite $(\beta_k)_{k \in \mathbb{N}^*}$ d'éléments de $\{0,\ldots,9\}$ qui ne sont pas tous des 9 à partir d'un certain rang, telle que : $x = \sum_{k=1}^{+\infty} \beta_k \, 10^{-k}$.

On a : $t = \sum_{k=1}^{+\infty} \alpha_k \, 10^{-k}$, avec $\alpha_k = 9 - \beta_k$, ce qui montre : $(\alpha_k)_{k \in \mathbb{N}^*} \in E$. □

1.2.15 Soient P un plan affine euclidien, et O un point de P. On note S l'ensemble des similitudes directes de P de centre O telles que, pour tout $s \in S$ et pour tout $m \in P$ il existe une droite contenant les points m, s(m) et $s^3(m)$.

Trouver l'ensemble L des images d'un point donné $m_o \in P \setminus \{O\}$ par les éléments de S.

Soit $(O;\vec{i},\vec{j})$ un repère orthonormal positif de P orienté. Au point de coordonnées (x,y) on associe son affixe $z = x+iy$. Une similitude directe de centre O, s, se traduit par la multiplication de l'affixe du point générique $m \in P$ par un nombre complexe $a \neq 0$.

Pour que s appartienne à S, il faut et il suffit que, pour tout $z \in \mathbb{C} \setminus \{0\}$ les points d'affixes z, az et a^3z appartiennent à une même droite, c'est-à-dire (à une similitude près) que les points d'affixes $1, a, a^3$ appartiennent à une même droite, i.e. que les vecteurs représentés par a^3-a et par a-1 soient colinéaires.

Si $a = 1$, cette condition est remplie ; on a alors $Id_P \in S$, ce qui était évident a priori. Si $a \neq 1$, cette condition s'écrit :

$$\frac{a^3-a}{a-1} \in \mathbb{R} \quad \text{i.e.} \quad a^2+a \in \mathbb{R}.$$

Si l'on pose $a = \alpha+\beta i$, $(\alpha,\beta) \in \mathbb{R}^2 \setminus \{(0,0)\}$, elle devient $(2\alpha+1)\beta = 0$.

En conclusion, les éléments de S sont les similitudes représentées par les réels non nuls, i.e. les homothéties de centre O (ce qui était évident a priori) et les similitudes représentées par un nombre complexe de partie réelle -1/2.

• En passant par l'intermédiaire du point d'affixe 1, on constate que l'ensemble L est la réunion de la droite Om_o, et de la symétrique par rapport à O de la médiatrice du segment $[O,m_o]$.

1.2.16 Soit $\tilde{\mathbb{C}}$ l'ensemble obtenu en adjoignant à $\mathbb{C}$ un élément noté ∞.

On appelle homographie toute application h de $\tilde{\mathbb{C}}$ dans $\tilde{\mathbb{C}}$ définie par :

$$(1)\begin{cases} h(z) = (az+b)(cz+d)^{-1} \text{ pour } z \in \mathbb{C} \setminus \{-dc^{-1}\} \text{ (pour } z \in \mathbb{C} \text{ si } c = 0) ; \\ h(-dc^{-1}) = \infty \text{ si } c \neq 0 \ ; \ h(\infty) = ac^{-1} \text{ si } c \neq 0 \ ; \ h(\infty) = \infty \text{ si } c = 0. \end{cases}$$

où $(a,b,c,d) \in \mathbb{C}^4$ est donné tel que $ad-bc \neq 0$.

1° Montrer que l'ensemble H des homographies est un sous-groupe du groupe symétrique de $\tilde{\mathbb{C}}$.

2° Soient : $U = \{z \in \mathbb{C} \mid |z| = 1\}$ et $D = \{z = \mathbb{C} \mid |z| < 1\}$.

Trouver toutes les homographies h telles que $h(U) = U$.

Parmi elles, trouver celles pour lesquelles $h(D) = D$.

1° L'homographie définie par (1) est notée h_M, avec $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. On a :

$H = \{h_M \mid M \in G\}$ où G est le groupe linéaire de type 2 sur $\mathbb{C}$.

Pour $M = I_2$, on a $h_M = Id_{\widetilde{\mathbb{C}}}$; on vérifie (assez laborieusement) :

$$\forall (M,M') \in G^2 \quad h_{M'} \circ h_M = h_{M'M}$$

On en déduit que toute homographie est une bijection $\left((h_M)^{-1} = h_{M^{-1}}\right)$, et que $M \mapsto h_M$ est un morphisme de groupes de G dans le groupe symétrique de $\widetilde{\mathbb{C}}$; l'image H de ce morphisme est un sous-groupe du groupe symétrique de $\widetilde{\mathbb{C}}$. □

2° Nous allons raisonner par condition nécessaire et suffisante.

a) Supposons qu'il existe $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$ telle que $h_M(U) = U$.

Pour tout $\varphi \in \mathbf{R}$, nous avons :

$$(ae^{i\varphi}+b)(\bar{a}e^{-i\varphi}+\bar{b}) = (ce^{i\varphi}+d)(\bar{c}e^{-i\varphi}+\bar{d})$$

i.e. $$Ae^{2i\varphi} + Be^{i\varphi} + \bar{A} = 0$$

avec : $$A = a\bar{b} - c\bar{d} \quad \text{et} \quad B = |a|^2 + |b|^2 - |c|^2 - |d|^2.$$

Le polynôme $AX^2 + BX + \bar{A}$, qui a plus de deux racines, est nul : $(A,B) = (0,0)$.

Comme $A = 0$ exige $|a||b| = |c||d|$, compte tenu de $B = 0$, on a :

$$[|a| + |b| = |c| + |d|] \wedge [(|a| - |b|) = \pm(|c| - |d|)]$$

ce qui s'écrit : $\{|a|,|b|\} = \{|c|,|d|\}$.

On ne peut avoir $(|a| = |c|) \wedge (|b| = |d|)$ car, avec $A = 0$, on aurait :

$$[a = c = 0] \vee [(a = ce^{i\theta} \neq 0) \wedge (b = de^{i\theta})], \quad \theta \in \mathbf{R}$$

ce qui est incompatible avec $ad - bc \neq 0$. D'où la condition nécessaire :

$$(|a| = |d|) \wedge (|b| = |c|) \wedge (a\bar{b} - c\bar{d} = 0) \wedge (ad - bc \neq 0).$$

Elle entraîne la condition nécessaire : (2) ∨ (3) avec :

$$(a = d = 0) \wedge (b = ce^{i\theta} \neq 0), \quad \theta \in \mathbf{R} \tag{2}$$

$$(a = de^{i\theta} \neq 0) \wedge (a\bar{b} = c\bar{d}) \wedge (ad - bc \neq 0), \quad \theta \in \mathbf{R} \tag{3}$$

b) Les homographies qui vérifient (2) sont définies, avec $\theta \in \mathbf{R}$, par :

$h(z) = e^{i\theta}/z$ si $z \in \mathbb{C} \setminus \{0\}$; $h(0) = \infty$; $h(\infty) = 0$.

Pour chacune d'elles, on constate :

$h(e^{i\varphi}) = e^{i(\theta-\varphi)}$, et on en déduit $h(U) = U$.

Notons qu'ici $h(D) = E \cup \{\infty\}$, où $E = \{z \in \mathbb{C} \mid |z| > 1\}$.

b') Si h_M vérifie (3), on a $d \neq 0$ et, quitte à multiplier a,b,c,d par un même élément de $\mathbb{C} \setminus \{0\}$ ce qui ne change pas h_M, on peut supposer $d = 1$, et remplacer (3) par :

$$(a,b,c,d) = (e^{i\theta}, \bar{c}e^{i\theta}, c, 1), \text{ avec } \theta \in \mathbf{R} \text{ et } c \in \mathbb{C} \setminus U \tag{4}$$

Inversement, toute $h \in H$ de la forme (4) convient car, pour $z \in \mathbb{C} \setminus \{-1/c\}$:

$$1 - \left| e^{i\theta} \frac{z+\bar{c}}{cz+1} \right|^2 = 1 - \frac{(z+\bar{c})(\bar{z}+c)}{(cz+1)(\bar{c}\bar{z}+1)}$$

$$= \frac{(1-|z|^2)(1-|c|^2)}{|cz+1|^2} \quad , \text{ et } h(U) = U.$$

On peut même préciser que :

- Si $|c| < 1$, h induit la bijection de D sur D qui s'écrit :

$$z \longmapsto e^{i\theta} \frac{z+\bar{c}}{cz+1} \quad , \text{ avec } \theta \in \mathbf{R} \text{ et } c \in D \tag{5}$$

(Les bijections de D sur D de la forme (5) forment évidemment un sous-groupe du groupe symétrique de D).

- Si $|c| > 1$, on a $h(D \setminus \{-1/c\}) = E$.

2. POLYNÔMES.

FRACTIONS RATIONNELLES

2.1 Polynômes

2.1.1 Déterminer $n \in \mathbb{N}$ tel que, dans $K[X]$, B divise A, avec :

$$A = (X^2-X+1)^n - X^{2n} + X^n - 1 \; ; \; B = X^3 - X^2 + X - 1$$

Indication. On fera intervenir la caractéristique du corps K.

On a $B = (X-1)(X^2+1)$.

Le reste de la division euclidienne de X^2+1 par $X-1$ est 2.

1er Cas. K n'est pas de caractéristique 2. Ici $X-1$ et X^2+1 sont premiers entre eux. Comme $A(1) = 0$ montre que A est divisible par $X-1$, il suffit d'écrire que A est divisible par X^2+1.

En remplaçant X^2 par -1 dans $A(X)$, on constate :

$$A \equiv (1 + (-1)^n)(X^n-1), \text{ mod } X^2+1.$$

Si n est impair : $A \equiv 0$, mod X^2+1 ; B divise A.

Soit n pair, $n = 2p$; $A \equiv 2((-1)^p-1)$, mod X^2+1 ; B divise A si, et seulement si p est pair.

Les solutions sont : n impair ou n multiple de 4.

2ème Cas. K est de caractéristique 2. Ici $X-1$ et X^2+1 ne sont pas premiers entre eux ; on peut écrire $B = (X-1)^3$.

Eliminons $n \in \{0,1\}$, auquel cas $A = 0$ et B divise A.

La formule du binôme appliquée à $(X^2 - (X-1))^n$ donne :

$$A \equiv - C_n^1 X^{2n-2}(X-1) + C_n^2 X^{2n-4}(X-1)^2 + X^n - 1, \text{ mod } B.$$

En posant $X-1 = Y$, nous avons à écrire que :

$$P = -nY(1+Y)^{2n-2} + C_n^2Y^2(1+Y)^{2n-4} + (1+Y)^n - 1$$

est divisible par Y^3. Or P est égal, mod Y^3, à :

$$-nY + C_n^2Y^2 + nY + C_n^2Y^2 = 2C_n^2Y^2 = 0$$

Ici tout $n \in \mathbb{N}$ est solution.

2.1.2 Ici K est un sous-corps d'un corps commutatif L. Soient $P \in K[X]$ irréductible, et $Q \in K[X]$. On suppose P et Q, considérés comme éléments de $L[X]$, ont une racine commune. Montrer que P divise Q.

- Notons Δ le PGCD de P et Q dans $K[X]$. Le PGCD de P et Q, considérés comme éléments de $L[X]$, est aussi Δ (ne serait-ce que parce que l'on peut l'obtenir par divisions successives).

Les éléments P et Q de $L[X]$ ayant une racine commune, on a $\deg \Delta \geqslant 1$.

- Revenons à $K[X]$; Δ, de degré au moins égal à 1, divisant le polynôme irréductible P, on a $P = k\Delta$, $k \in K^*$; comme Δ divise Q, il en résulte que P divise Q. □

2.1.3 Soit $(m,n) \in (\mathbb{N}^*)^2$. Dans $K[X]$ déterminer le PGCD de X^m-1 et X^n-1.

• Commençons par rappeler un résultat classique.

Soit $p \in \mathbb{N}^*$. Tout $P \in K[X]$ s'écrit, d'une façon et d'une seule :

$$P = \sum_{k=0}^{p-1} Q_k(X^p).X^k, \quad (Q_o,\ldots,Q_{p-1}) \in (K[X])^p.$$

Nous constatons aisément que le reste de la division euclidienne de $Q_k(X^p)$ par X^p-1 est $Q_k(1)$. Le reste de la division de P par X^p-1 est donc :

$$\sum_{k=0}^{p-1} Q_k(1)X^k.$$

• Il en résulte que, pour $(p,q) \in (\mathbb{N}^*)^2$ tel que $1 \leqslant p \leqslant q$, le reste de la division de X^q-1 par X^p-1 est $X^\rho-1$, où ρ est le reste de la division de q par p.

• Venons en à notre exercice, en supposant, pour fixer les idées : $1 \leqslant m \leqslant n$.

En désignant par r le reste de la division de n par m, nous avons :

$$(X^n-1) \wedge (X^m-1) = (X^m-1) \wedge (X^r-1).$$

Par itération, nous devons effectuer les divisions successives dans $\mathbb{N}$ de n par m, puis de m par r (reste de la division de n par m)..., jusqu'à trouver un reste r_{k+1} nul. Par ce procédé, qui constitue l'algorithme d'Euclide dans $\mathbb{Z}$, nous déterminons $r_k = \delta$ où δ est le PGCD de m et n et nous constatons

$$(X^n-1) \wedge (X^m-1) = X^\delta-1.$$

2.1.4 Soit $P \in \mathbb{Z}[X]$ de la forme $a_o + a_1X + \ldots + a_nX^n$ avec $a_o a_n \neq 0$.

On suppose que P admet une racine rationnelle de représentant canonique p/q (avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ et $p \wedge q = 1$).

1° Montrer qu'il existe $Q \in \mathbb{Z}[X]$ tel que $P = (qX-p)Q$.

2° En déduire que p divise a_o, que q divise a_n, que p-q divise P(1) et que p+q divise P(-1).

3° Application. Factoriser sur $\mathbb{Q}$ le polynôme :

$$P = 4X^4 - 28X^3 + 45X^2 - 6X - 18.$$

1° Dans $\mathbb{Q}[X]$, P, qui admet pour racine p/q, est divisible par qX-p. On dispose donc de $Q \in \mathbb{Q}[X]$ défini par : $P = (qX-p)Q$.

Le calcul du quotient d'une division euclidienne conduit à :

$$Q = \frac{\alpha_{n-1}}{q} X^{n-1} + \ldots + \frac{\alpha_k}{q^{n-k}} X^k + \ldots + \frac{\alpha_o}{q^n} \qquad (1)$$

avec $\alpha_k \in \mathbb{Z}$ pour tout $k \in \{0,\ldots,n-1\}$.

En outre, on a $p \neq 0$ à cause de $a_o \neq 0$, ce qui permet de diviser P par $-p+qX$ suivant les puissances croissantes à l'ordre n-1 ; le quotient est alors Q et le reste est nul ; on obtient ainsi :

$$Q = \frac{\beta_o}{p} + \ldots + \frac{\beta_k}{p^{k+1}} X^k + \ldots + \frac{\beta_{n-1}}{p^n} X^{n-1} \qquad (2)$$

avec $\beta_k \in \mathbb{Z}$ pour tout $k \in \{0,\ldots,n-1\}$.

La comparaison de (1) et (2) fournit :

$$\forall k \in \{0,\ldots,n-1\} \quad \beta_k q^{n-k} = \alpha_k p^{k+1}.$$

Comme p et q sont premiers entre eux, p^{k+1} et q^{n-k} le sont ; il en résulte que p^{k+1} divise β_k, ce qui prouve que $Q \in \mathbb{Z}[X]$. □

2° On a donc : $Q = \sum_{k=0}^{n-1} \gamma_k X^k$, $\gamma_k \in \mathbb{Z}$. En particulier :

$$a_o = -p\gamma_o \; ; \; a_n = q\gamma_{n-1}$$

ce qui montre que p divise a_o et que q divise a_n.

• En utilisant $P(1) = (q-p)Q(1)$ et $P(-1) = -(q+p)Q(-1)$, où Q(1) et Q(-1) sont dans $\mathbb{Z}$, on constate que P(1) et P(-1) sont respectivement divisibles par p-q et par p+q. □

3° Pour toute racine rationnelle éventuelle de P de la forme canonique p/q, p divise ici 18 et q divise 4. On a donc :

$$p \in \{\pm1, \pm2, \pm3, \pm6, \pm9, \pm18\} \; : \; q \in \{\pm1, \pm2, \pm4\} \; ;$$

$$p/q \in \left\{\pm\frac{1}{1}, \pm\frac{2}{1}, \pm\frac{3}{1}, \pm\frac{6}{1}, \pm\frac{9}{1}, \pm\frac{18}{1}, \pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{9}{2}, \pm\frac{1}{4}, \pm\frac{3}{4}, \pm\frac{9}{4}\right\}.$$

Comme $P(1) = -3$ et $P(-1) = 65$, on conserve que les p/q tels que :

$$[(p-q) \in \{\pm 1, \pm 3\}] \wedge [(p+q) \in \{\pm 1, \pm 5, \pm 13, \pm 65\}]$$

i.e. les : $p/q \in \{-2, -\frac{1}{2}, \frac{3}{2}, \frac{1}{4}\}$.

Il est clair que $P(-2) \neq 0$.

Pour essayer $\frac{p}{q} = \frac{1}{4}$, on effectue la division euclidienne de P par 4X-1 ; on constate que l'on trouve au quotient un coefficient non entier (ici celui de X^2) ; l'essai est donc infructueux.

En revanche dans la division euclidienne de P par 2X+1 le reste est nul, et on constate que le quotient est divisible par 2X-3. On trouve :

$$P = (2X+1)(2X-3)(X^2-6X+6) \qquad (3)$$

$X^2 - 6X + 6$ n'a pas de racine dans $\mathbb{Q}$; (3) est la factorisation de P sur $\mathbb{Q}$. Sur $\mathbb{R}$ ou $\mathbb{C}$, on aurait :

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

2.1.5 LEMME DE GAUSS. 1° Pour tout polynôme non nul $P \in \mathbb{Z}[X]$, on note $\gamma(P)$ le PGCD des coefficients.

Soient P_1 et P_2 deux éléments non nuls de $\mathbb{Z}[X]$. Montrer que :

a) Si $\gamma(P_1) = \gamma(P_2) = 1$, alors $\gamma(P_1P_2) = 1$.

b) Dans le cas général : $\gamma(P_1P_2) = \gamma(P_1)\gamma(P_2)$.

2° En déduire qu'un polynôme non constant, à coefficients entiers, est irréductible dans $\mathbb{Z}[X]$ si, et seulement s'il l'est dans $\mathbb{Q}[X]$.

1° a) Ici $\gamma(P_1) = \gamma(P_2) = 1$. On note $P = P_1P_2$, et on suppose $\gamma(P) \neq 1$; il existe donc un nombre premier p divisant tous les coefficients de P.

Soit φ la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z}$, qui est un morphisme d'anneaux. On la prolonge de façon naturelle en $\overline{\varphi} : \mathbb{Z}[X] \longrightarrow (\mathbb{Z}/p\mathbb{Z})[X]$ en posant : $\sum a_k X^k \mapsto \sum \varphi(a_k) X^k$, et on constate aisément que $\overline{\varphi}$ est encore un morphisme d'anneaux.

On a : $\overline{\varphi}(P) = 0$ et $\overline{\varphi}(P) = \overline{\varphi}(P_1)\overline{\varphi}(P_2)$; d'où $\overline{\varphi}(P_1) = 0$ ou $\overline{\varphi}(P_2) = 0$ puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps. Mais ceci contredit $\gamma(P_1) = \gamma(P_2) = 1$. □

b) On peut écrire : $P_1 = \gamma(P_1)Q_1$ et $P_2 = \gamma(P_2)Q_2$, avec $\gamma(Q_1) = \gamma(Q_2) = 1$.
D'où : $P_1P_2 = \gamma(P_1)\gamma(P_2)Q_1Q_2$, avec (cf.a)) : $\gamma(Q_1Q_2) = 1$.
On en déduit $\gamma(P_1P_2) = \gamma(P_1)\gamma(P_2)$ en utilisant la propriété du PGCD :

$$\bigwedge_{i \in I} (\lambda a_i) = \lambda \Big(\bigwedge_{i \in I} a_i \Big). \qquad \square$$

2° • Si P, à coefficients entiers, est irréductible dans $\mathbb{Q}[X]$, il l'est a fortiori dans $\mathbb{Z}[X]$.

• Inversement, supposons $P = qr$, où q et r sont des éléments non constants de $\mathbb{Q}[X]$. Soit a le carré d'un multiple commun à tous les dénominateurs des coefficients de q et r. On peut écrire :

$aP = QR$, où Q et R sont des éléments non constants de $\mathbb{Z}[X]$.

D'où : $aP = \gamma(Q)\gamma(R)Q_1R_1$, avec $\gamma(Q_1) = \gamma(R_1) = 1$, et $a\gamma(P) = \gamma(Q)\gamma(R)$.

Comme $a \in \mathbb{Z}^*$, il vient : $P = \gamma(P)Q_1R_1 = ST$, où $S = \gamma(P)Q_1$ et $T = R_1$ sont des éléments non constants de $\mathbb{Z}[X]$. □

2.1.6 CRITERE D'EISENSTEIN. Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme non constant, à coefficients entiers. On suppose qu'il existe un nombre premier p divisant tous les a_k sauf a_n, et tel que p^2 ne divise pas a_o.

Montrer que P est irréductible dans $\mathbb{Q}[X]$.

Application. Pour p premier, $1+X+\ldots+X^{p-1}$ est irréductible dans $\mathbb{Q}[X]$.

D'après l'exercice précédent, il suffit de montrer que P est irréductible dans $\mathbb{Z}[X]$.

Raisonnant par l'absurde nous supposons que $P = P_1P_2$, où P_1 et P_2 sont des éléments non constants de $\mathbb{Z}[X]$, que nous écrivons :

$$\sum_{k=o}^{r} b_k X^k \quad \text{et} \quad \sum_{k=o}^{s} c_k X^k, \quad b_r c_s \neq 0, \quad 1 \leqslant r \leqslant n-1, \quad s = n-r.$$

Reprenons le morphisme d'anneaux $\bar{\varphi} : \mathbb{Z}[X] \longrightarrow (\mathbb{Z}/p\mathbb{Z})[X]$ utilisé dans l'exercice précédent. Comme $\varphi(a_k) = 0$ pour $0 \leqslant k \leqslant n-1$, il vient :

$$\sum_{k=o}^{r} \varphi(b_k)X^k \cdot \sum_{k=o}^{s} \varphi(c_k)X^k = \varphi(a_n)X^n, \quad \varphi(a_n) \neq 0.$$

On a : $\varphi(b_r)\varphi(c_s) \neq 0$; d'où $\varphi(b_r) \neq 0$ et $\varphi(c_s) \neq 0$

et : $\varphi(b_o)\varphi(c_o) = 0$; d'où $\varphi(b_o) = 0$ ou $\varphi(c_o) = 0$.

On n'a pas $\varphi(b_o) = \varphi(c_o) = 0$, sans quoi b_o et c_o seraient divisibles par p et $a_o = b_oc_o$ serait divisible par p^2. Pour fixer les idées, supposons $\varphi(b_o) = 0$ et $\varphi(c_o) \neq 0$.

Nous constatons qu'il existe un unique entier $i \in [0, r-1]$ tel que :

$$\varphi(b_o) = \ldots = \varphi(b_i) = 0 \quad \text{et} \quad \varphi(b_{i+1}) \neq 0$$

$\varphi(a_{i+1})$ se réduit donc à : $\varphi(b_{i+1})\varphi(c_o)$ qui n'est pas nul, ce qui constitue une contradiction puisque : $i+1 \leqslant r < n$ entraîne $\varphi(a_{i+1}) = 0$. □

Application. Il est clair que $P = 1 + X + \ldots + X^{p-1}$ est irréductible dans $\mathbb{Q}[X]$ si, et seulement si $Q = P(1+X) = ((1+X)^p - 1)/X$ est irréductible dans $\mathbb{Q}[X]$. Nous avons :

$$Q = C_p^1 + C_p^2 X + \ldots + C_p^{p-1} X^{p-2} + X^{p-1} .$$

Il est clair que p divise $C_p^1 = p$, que p^2 ne divise pas C_p^1, et que p ne divise pas le coefficient de X^{p-1}, qui est 1.

Montrons que, pour tout $i \in \mathbb{N}_{p-1}$, p divise C_p^i.

De : $p(p-1)\ldots(p-i+1) = 1.2\ldots i.C_p^i$, $C_p^i \in \mathbb{N}^*$, on déduit que le nombre premier p divise l'un des facteurs du produit $1.2\ldots i\ C_p^i$; comme, à cause de $i \leqslant p-1$, p ne divise ni 1, ni 2,...,ni i, il divise C_p^i.

Le critère d'Eisenstein s'applique donc à Q. □

2.1.7 POLYNÔMES DE LAGRANGE. 1° a) Soient $a_0,\ldots,a_n$ des éléments deux à deux distincts du corps commutatif K.

- Montrer que, pour $i \in \{0,\ldots,n\}$ fixé, il existe un unique $L_i \in K_n[X]$ tel que :

$$\forall j \in \{0,\ldots,n\} \quad L_i(a_j) = \delta_{ij}.$$

- Montrer que $(L_i)_{0 \leqslant i \leqslant n}$ est une base de $K_n[X]$.

b) Soit $(\alpha_0,\ldots,\alpha_n) \in K^{n+1}$. Déterminer les $P \in K[X]$ vérifiant :

$$\forall j \in \{0,\ldots,n\} \quad P(a_j) = \alpha_j \qquad (1)$$

2° Application. Montrer qu'il existe un unique $m \in \mathbb{N}^*$ auquel on peut associer un polynôme $P \in \mathbb{R}[X]$ de degré $n \leqslant 3m$ vérifiant :

i) $\forall k \in \{0,\ldots,m\}$ $P(3k) = 2$;

ii) $\forall k \in \{1,\ldots,m\}$ $P(3k-2) = 1$ et $P(3k-1) = 0$;

iii) $P(3m+1) = 730$.

1° a) Un polynôme de degré au plus n admettant les n racines distinctes a_j, $j \in \{0,\ldots,n\} \setminus \{i\}$, est nécessairement de la forme :

$$L_i = A_i \prod_{j \neq i} (X-a_j), \quad A_i \in K.$$

Inversement un polynôme de cette forme convient si, et seulement s'il vérifie $L_i(a_i) = 1$, condition qui s'écrit :

$$A_i = \frac{1}{\prod_{j \neq i} (a_i - a_j)}.$$ □

- La famille $(L_i)_{0 \leqslant i \leqslant n}$ de n+1 éléments de l'espace vectoriel $K_n[X]$, de dimension n+1, est libre et c'est donc une base. En effet si $\sum_{i=0}^{n} \lambda_i L_i$ est le polynôme nul, on a, pour tout $j \in \{0,\ldots,n\}$:

$$\left(\sum_{i=0}^{n} \lambda_i L_i\right)(a_j) = 0, \quad \text{i.e. } \lambda_j = 0.$$ □

b) Tout élément de $K_n[X]$ s'écrit $\sum_{i=0}^{n} \lambda_i L_i$, et il vérifie (1) si, et seulement si : $\lambda_j = \alpha_j$ pour tout $j \in \{0,\ldots,n\}$.

$P_o = \sum_{i=1}^{n} \alpha_i L_i$ est donc l'unique élément de $K_n[X]$ qui vérifie (1).

Les éléments de $K[X]$ qui vérifient (1) sont ceux qui diffèrent de P_o par un polynôme s'annulant aux points a_j, à savoir les :

$$P_o + Q \cdot \prod_{i=o}^{n} (X-a_i), \quad Q \in K[X].$$

2° Soient $m \in \mathbb{N}^*$ et $n = 3m$. En adoptant $a_j = j$ pour tout $j \in \{0,\ldots,3m\}$, on constate aisément que les L_i, $i \in \{0,\ldots,3m\}$, s'écrivent :

$$L_i = \frac{(-1)^{3m-i}}{i!\,(3m-i)!} \prod_{j \neq i} (X-j).$$

D'après 1°, l'unique $P \in K_{3m}[X]$ qui vérifie i) et ii) est :

$$P = 2\sum_{k=o}^{m} L_{3k} + \sum_{k=1}^{m} L_{3k-2}.$$

Il s'agit de savoir si l'on peut choisir $m \in \mathbb{N}^*$ de façon à remplir la condition supplémentaire iii), qui s'écrit : $2A + B = 730$, avec

$$A = \sum_{k=o}^{m} L_{3k}(3m+1) \; ; \; B = \sum_{k=1}^{m} L_{3k-2}(3m+1).$$

On calcule :

$$L_{3k}(3m+1) = (-1)^{3m+3k} C_{3m+1}^{3k} \; ; \; L_{3k-2}(3m+1) = (-1)^{3m+3k-2} C_{3m+1}^{3k-2}.$$

On adjoint : $C = \sum_{k=1}^{m} (-1)^{3m+3k-1} C_{3m+1}^{3k-1}$

Par $(1-z)^{3m+1} = \sum_{\ell=o}^{3m+1} (-1)^{\ell} C_{3m+1}^{\ell} z^{\ell}$, et $z \in \{1,j,j^2\}$, on obtient :

$$A + (B-1) + C = 0 \quad ; \; A + (B-1)j + Cj^2 = \bar{u}$$

$$A + (B-1)j^2 + Cj = u \; ; \; u = (-1)^{3m} (\sqrt{3})^{3m+1} \exp\left[i\left(m\,\frac{\pi}{2} + \frac{\pi}{6}\right)\right]$$

ce qui fournit :

$$A = \frac{2}{3}(-1)^{3m}(\sqrt{3})^{3m+1} \cos\left(m\,\frac{\pi}{2} + \frac{\pi}{6}\right) \; ; \; B = 1 + \frac{2}{3}(-1)^{3m}(\sqrt{3})^{3m+1} \cos\left(m\,\frac{\pi}{2} + \frac{5\pi}{6}\right).$$

En utilisant $729 = 3^6$, on constate que iii) s'écrit :

$$(-1)^{3m}(\sqrt{3})^{3m}\left(\cos\frac{m\pi}{2} - \sqrt{3}\sin\frac{m\pi}{2}\right) = (\sqrt{3})^{12}$$

ce qui est vérifié si, et seulement si $3m = 12$, i.e. $m = 4$. □

2.1.8 Le corps commutatif K est de caractéristique 0. Soient a,b,c des éléments de K deux à deux distincts, et $k = (\alpha,\beta,\gamma,\alpha_1,\beta_1,\gamma_1,\alpha_2,\beta_2) \in K^8$.

Trouver tous les polynômes $P \in K[X]$ vérifiant :

$$P(a) = \alpha \; ; \; P(b) = \beta \; ; \; P(c) = \gamma \; ;$$

$$P'(a) = \alpha_1 \; ; \; P'(b) = \beta_1 \; ; \; P'(c) = \gamma_1 \; ; \; P''(a) = \alpha_2 \; ; \; P''(b) = \beta_2.$$

Il s'agit d'une extension de la formule d'interpolation de Lagrange.

On considère l'application $u : K[X] \to K^8$, visiblement linéaire :

$$P \mapsto \big(P(a),P(b),P(c),P'(a),P'(b),P'(c),P''(a),P''(b)\big).$$

Il s'agit de déterminer $\mathcal{T} = u^{-1}(k)$, et donc (si $\mathcal{T}$ n'est pas vide), de déterminer Ker u et un élément particulier de $\mathcal{T}$.

• On constate que Ker u est l'ensemble des polynômes divisibles par chacun des polynômes $(X-a)^3$, $(X-b)^3$, $(X-c)^2$, premiers entre eux deux à deux, et donc l'ensemble des polynômes divisibles par $(X-a)^3(X-b)^3(X-c)^2$.

Ceci nous conduit à introduire les polynômes :

$$C = \frac{(X-a)^3(X-b)^3}{(c-a)^3(c-b)^3} \; ; \; C_1 = (X-c)C \; ; \; C_2 = \frac{(X-c)^2}{2}C$$

dans lesquels les coefficients dominants ont été choisis de façon que :

$$C(c) = 1 \; ; \; C_1'(c) = 1 \; ; \; C_2''(c) = 1 \quad \text{(vérification aisée)}.$$

Ker u est l'ensemble des multiples de C_2.

- Par permutations circulaires sur a,b,c, on déduit de C, C_1, C_2 d'abord A, A_1, A_2 puis B, B_1, B_2.

On note que X-a divise A_1, que $(X-a)^2$ divise A_2, que $(X-a)^3$ divise B, B_1, B_2, C, C_1, C_2.

• Nous allons montrer que $\mathcal{T}$ contient un élément appartenant à $\mathrm{Vect}(\mathcal{F})$, où :

$$\mathcal{F} = \{A,B,C,A_1,B_1,C_1,A_2,B_2\}.$$

- En effet, pour que :

$$Q = \lambda A + \mu B + \nu C + \lambda_1 A_1 + \mu_1 B_1 + \nu_1 C_1 + \lambda_2 A_2 + \mu_2 B_2$$

appartienne à $\mathcal{T}$, il faut et il suffit qu'il vérifie :

$$\lambda = \alpha \quad ; \; \mu = \beta \quad ; \; \nu = \gamma$$

$$\lambda A'(a) + \lambda_1 = \alpha_1 \; ; \; \mu B'(b) + \mu_1 = \beta_1 \; ; \; \nu C'(c) + \nu_1 = \gamma_1$$

$$\lambda A''(a) + \lambda_1 A_1''(a) + \lambda_2 = \alpha_2 \; ; \; \mu B''(b) + \mu_1 B_1''(b) + \mu_2 = \beta_2.$$

conditions qui déterminent de manière unique $(\lambda,\mu,\nu,\lambda_1,\mu_1,\nu_1,\lambda_2,\mu_2)$ et donc Q.

• En conclusion $\mathcal{T}$ est Q + Ker u, ensemble des polynômes de la forme :

$$Q + C_2 R, \quad R \in K[X].$$

Remarque. L'étude montre que la restriction de u à $\mathrm{Vect}(\mathcal{F})$ est une bijection ce qui montre que $\mathrm{Vect}(\mathcal{F})$ est de dimension 8 et que $\mathcal{F}$ en est une base.

2.1.9 Par entier on entend : élément de $\mathbb{Z}$. On donne $n \in \mathbb{N}$.

1° A tout $a \in \mathbb{Z}$, on associe les n+1 polynômes $P_0 = 1$ et :

$$P_k = \frac{1}{k!} \prod_{\ell=0}^{k-1} (X - (a+\ell)),\ k \in \mathbb{N}_n.$$

a) Montrer que $(P_k)_{0 \leqslant k \leqslant n}$ est une base de $\mathbb{C}_n[X]$.

b) Vérifier : $P_k(i) \in \mathbb{Z}$ pour tous $k \in \{0,\ldots,n\}$ et $i \in \mathbb{Z}$.

2° a) Soit $P \in \mathbb{C}_n[X]$ tel qu'il existe n+1 entiers consécutifs en lesquels P prend des valeurs entières. Vérifier : $P(i) \in \mathbb{Z}$ pour tout $i \in \mathbb{Z}$.

b) Le résultat subsiste-t-il si P prend des valeurs entières en n+1 entiers deux à deux distincts ?

1° a) Dans le C-espace vectoriel $\mathbb{C}_n[X]$ de dimension (n+1), $(P_k)_{0 \leqslant k \leqslant n}$ est une famille de polynômes échelonnée en degrés, et donc une famille libre de n+1 éléments, i.e. une base. □

b) Il est clair que $P_o(i) = 1$ pour tout $i \in \mathbb{Z}$.

- Fixons maintenant $k \in \mathbb{N}_n$. Pour $i \in \mathbb{Z}$ nous avons :
  - Si $a \leqslant i \leqslant a+k-1$, $P_k(i) = 0$;
  - Si $i \geqslant a+k$, $P_k(i) = C^k_{i-a}$; en particulier $P_k(a+k) = 1$;
  - Si $i < a$, $P_k(i) = (-1)^k C^k_{a-i+k-1}$. □

2° a) Par hypothèse, il existe $a \in \mathbb{Z}$ tel que $P(a+j) \in \mathbb{Z}$ pour tout $j \in \{0,\ldots,n\}$. D'autre part on constate, en utilisant la base de $\mathbb{C}_n[X]$ associée à a (cf. 1° a)) qu'il existe $(\alpha_o,\ldots,\alpha_n) \in \mathbb{C}^{n+1}$ tel que :

$$P = \sum_{k=o}^{n} \alpha_k P_k.$$

Pour tout $j \in \{0,\ldots,n\}$, on a (en distinguant $j = 0$ et $j > 0$) :

$$P_j(a+j) = 1\ ;\ P_k(a+j) = 0 \text{ si } j+1 \leqslant k \leqslant n.$$

et donc : $$\sum_{k=o}^{j-1} \alpha_k P_k(a+j) + \alpha_j = P(a+j).$$

Pour $j = 0$ on obtient $\alpha_o \in \mathbb{Z}$. Compte tenu de ce résultat, pour $j = 1$ on obtient $\alpha_1 \in \mathbb{Z}$, et ainsi de suite jusqu'à $\alpha_n \in \mathbb{Z}$.

- Compte tenu du 1° b), on en déduit : $P(i) \in \mathbb{Z}$ pour tout $i \in \mathbb{Z}$. □

b) La réponse est négative (si $n \geqslant 1$). Contre-exemple :

$P = \frac{1}{(n+1)!} (X-1)\ldots(X-n)$, de degré n prend une valeur entière en chacun des n+1 entiers $1,\ldots,n$ et -1, mais $P(0)$ n'est pas entier.

Remarque. Soit $P \in \mathbb{C}_n[X]$ prenant une valeur entière en chacun des n+1 entiers deux à deux distincts $a_o,\ldots,a_n$. L'étude des polynômes d'interpolation de Lagrange permet de constater que P est à coefficients rationnels.

2.1.10 On se place dans $\mathbf{R}[X]$. Un polynôme est dit positif lorsque la fonction associée est positive. Montrer qu'un tel polynôme est la somme des carrés de deux polynômes de même degré.

• Comme la proposition est visiblement vraie pour le polynôme nul, et comme la fonction associée à un polynôme de degré impair n'est pas positive, il suffit de vérifier, par récurrence, qu'est vraie pour tout $n \in \mathbf{N}$ l'assertion :

(A_n) Tout polynôme positif de degré $2n$ est la somme des carrés de deux polynômes de même degré (nécessairement égal à n).

• Il est clair que (A_o) est vraie, tout polynôme positif de degré 0 s'écrivant $P^2 + P^2$, où P est un polynôme de degré 0.

• Soit $n \in \mathbf{N}^*$ pour lequel (A_{n-1}) est vraie. Considérons un polynôme P positif de degré $2n$. Deux cas sont possibles :

1er Cas : P n'a pas de zéro réel. Il existe alors un polynôme positif de degré 2, $S = X^2 + \alpha X + \beta$ avec $\alpha^2 - 4\beta < 0$, qui le divise. On a $P = ST$, avec $T(t) > 0$ pour tout $t \in \mathbf{R}$.

2ème Cas : P a au moins un zéro réel a. Celui-ci est d'ordre de multiplicité pair (sans quoi $t \mapsto P(t)$ changerait de signe en a) : $S = (X-a)^2$ est un polynôme positif de degré 2 qui divise P. On a $P = ST$, avec $T(t) \geqslant 0$ pour tout $t \in \mathbf{R} \setminus \{a\}$, et donc (par continuité) pour tout $t \in \mathbf{R}$.

Dans les deux cas, on peut écrire $P = ST$, où S et T sont des polynômes positifs de degrés 2 et $2n-2$. En utilisant l'hypothèse de récurrence, on obtient :

$$P = (A^2+B^2)(C^2+D^2) = (AC+BD)^2 + (AD-BC)^2 = U^2 + V^2.$$

Si U et V ne sont pas de même degré, on les remplace par :

$$\frac{1}{\sqrt{2}}(U+V) \text{ et } \frac{1}{\sqrt{2}}(U-V), \text{ qui sont alors de même degré.} \qquad \square$$

2.1.11 Déterminer tous les polynômes $P \in \mathbf{R}[X]$ qui vérifient :

$$P(X^2+1) = (P(X))^2 + 1 \quad \text{et} \quad P(0) = 0.$$

• Soit $(a_n)_{n \in \mathbf{N}}$ la suite d'entiers définie par :

$$a_o = 0, \text{ et } a_{n+1} = a_n^2 + 1 \text{ pour tout } n \in \mathbf{N}.$$

Il est clair qu'il s'agit d'une suite strictement croissante constituée d'entiers deux à deux distincts.

• On vérifie par récurrence que s'il existe une solution P, alors :

$$P(a_n) = a_n \text{ pour tout } n \in \mathbf{N}$$

et donc que $P = X$ puisque ces deux polynômes prennent la même valeur en tous les points d'un sous-ensemble infini de $\mathbf{R}$.

• D'autre part X est évidemment solution ; cette solution est donc unique. $\square$

2.1.12 Ici le corps commutatif K est de caractéristique 0. Trouver les polynômes $P \in K[X]$ tels que P' divise P.

Il est clair que le polynôme nul est solution, et qu'aucun polynôme de degré 0 n'est solution.

a) Soit $P \in K[X]$, de degré $n \geqslant 1$ tel que P' divise P.

Il existe $\alpha \in K$ tel que : $nP = (X-\alpha)P'$.

Si $n \geqslant 2$, on en déduit : $n(n-1)P = (X-\alpha)^2 P''$.

Plus généralement, on montre par récurrence que, pour tout $m \in \mathbb{N}_n$, on a : $n(n-1)\ldots(n-m+1)P = (X-\alpha)^m P^{(m)}$.

En particulier, pour $m = n$:

$$n!P = (X-\alpha)^n . an!$$

où a est le coefficient dominant de P.

Tout polynôme non nul divisible par son polynôme dérivée est donc de la forme : $a(X-\alpha)^n$, $a \in K^*$, $\alpha \in K$, $n \in \mathbb{N}^*$.

b) Inversement il est évident que tout polynôme de cette forme est divisible par son polynôme dérivé.

2.1.13 Trouver tous les polynômes $P \in \mathbb{C}[X]$ vérifiant :

$$P(X^2) = P(X)P(X+1) \qquad (1)$$

• Il est clair que les polynômes 0 et 1 sont solutions, et que toute solution non nulle est un polynôme normalisé (ce qui prouve que 0 et 1 sont les seules solutions constantes).

• Soit une solution P telle que $\deg P \geqslant 1$. P a au moins un zéro α.

De $P(\alpha^2) = P(\alpha)P(\alpha+1)$ et $P\big((\alpha-1)^2\big) = P(\alpha-1)P(\alpha)$, on déduit que α^2 et $(\alpha-1)^2$ sont zéros de P ; il en résulte (récurrence) que toutes les puissances 2^n, $n \in \mathbb{N}^*$, de α et $\alpha-1$ sont zéros de P.

Comme P n'a qu'un nombre fini de zéros, les familles des puissances 2^n de α et $\alpha-1$ sont nécessairement finies, ce qui s'écrit :

$$[(\alpha = 0) \vee (|\alpha| = 1)] \wedge [(\alpha = 1) \vee (|\alpha-1| = 1)] \qquad (2)$$

et conduit à considérer les cercles de $\mathbb{R}^2$ affine euclidien dont le rayon est 1 et dont les centres respectifs ont pour affixes 0 et 1 ; chacun contient le centre de l'autre, et ils ont en commun les points d'affixes $-j$ et $-j^2$, si bien que (2) s'écrit :

$$\alpha \in \{0, 1, -j, -j^2\}.$$

Ainsi : $P(X) = X^p(X-1)^q(X+j)^r(X+j^2)^s$, $(p,q,r,s) \in \mathbb{N}^4$.

On explicite $P(X+1)$ et $P(X^2)$ et on constate :

- que 0 est zéro d'ordre $p+q$ de $P(X)P(X+1)$, d'ordre $2p$ de $P(X^2)$,
- que $-j$ (resp. $-j^2$) est zéro d'ordre r (resp. s) de $P(X)P(X+1)$, mais n'est pas zéro de $P(X^2)$.

D'où, nécessairement, $p=q$, $r=s=0$, et $P(X) = (X^2-X)^p$, $p \in \mathbb{N}^*$.

- On constate qu'inversement $(X^2-X)^p$ vérifie (1) pour tout $p \in \mathbb{N}^*$.
- En conclusion, les solutions sont 0,1 et les $(X^2-X)^p$, $p \in \mathbb{N}^*$.

2.1.14 On donne $A \in \mathbb{C}[X]$, de degré $n \geqslant 1$, de zéros distincts $\alpha_1, \ldots, \alpha_n$. Trouver tous les $P \in \mathbb{C}[X]$ tels que $\deg P \leqslant n$, et que :

$$A^{(n)}P - A^{(n-1)}P' + \ldots + (-1)^n AP^{(n)} = 0 \quad \text{(polynôme nul)}.$$

L'ensemble des solutions est le noyau de $u \in \mathcal{L}(\mathbb{C}_n[X])$ défini par :

$$P \longmapsto A^{(n)}P - A^{(n-1)}P' + \ldots + (-1)^n AP^{(n)}.$$

Pour tout $P \in \mathbb{C}_n[X]$, le polynôme $u(P)$ a une dérivée nulle, et est donc constant. Pour $P=1$, on a $u(P) = A^{(n)} \neq 0$. D'où :

$$\dim(\operatorname{Im} u) = 1 \ ; \ \dim(\operatorname{Ker} u) = \dim(\mathbb{C}_n[X]) - 1 = n.$$

- Pour tout $i \in \{1, \ldots, n\}$, les dérivées d'ordres $0, 1, \ldots, n-1$ de $Q_i = (X-\alpha_i)^n$ prennent la valeur 0 au point α_i. D'où :

$$\big(u(Q_i)\big)(\alpha_i) = (-1)^n A(\alpha_i) Q_i^{(n)}(\alpha_i) \neq 0, \text{ et } u(Q_i) \text{ est constant}$$

ce qui entraîne : $Q_i \in \operatorname{Ker} u$.

- Nous avons ainsi : $\operatorname{Vect}(Q_1, \ldots, Q_n) \subset \operatorname{Ker} u$. Nous allons montrer que la famille $(Q_1, \ldots, Q_n)$ est libre ; compte tenu de $\dim(\operatorname{Ker} u) = n$, il en résultera : $\operatorname{Ker} u = \operatorname{Vect}(Q_1, \ldots, Q_n)$.

- La famille échelonnée en degrés $(C_n^n X^n, \ldots, C_n^1 X, 1)$ est une base de $\mathbb{C}_n[X]$; la famille $e = (Q_1, \ldots, Q_n, 1)$ a un déterminant dans cette base égal au déterminant de Vandermonde de $(-\alpha_1, \ldots, -\alpha_n)$, qui n'est pas nul puisque les α_i sont distincts ; e est donc une base de $\mathbb{C}_n[X]$. □

2.1.15 Soit $P \in \mathbb{C}[X]$, normalisé, de degré $n \geqslant 1$. Pour tout $k \in \{1, \ldots, n\}$, former le polynôme normalisé Q_k qui admet pour zéros, tous simples, les zéros d'ordre k de P, en convenant que $Q_k = 1$ si P n'a pas de zéro d'ordre k.

Exemple : $P = X^5 - 15X^3 + 10X^2 + 60X - 72$.

On a $P = Q_1 Q_2^2 \ldots Q_n^n$, avec Q_k et Q_ℓ premiers entre eux si $k \neq \ell$.

Une dérivation fournit : $P' = Q_2 Q_3^2 \ldots Q_n^{n-1} R$.

Soit a un zéro d'ordre k de P ; a est zéro simple de Q_k, et zéro d'ordre k-1 de P'. Si a était zéro de R, il serait zéro d'ordre au moins égal à k de $Q_k^{k-1} R$, et on aurait une contradiction. P et R sont donc premiers entre eux.

- En notant $A \wedge B$ le P.G.C.D. normalisé de A et B, on a :

$$P \wedge P' = Q_2 Q_3^2 \ldots Q_n^{n-1} \ ; \text{ or on sait calculer } P \wedge P' = P_1.$$

Il en résulte que $Q_1 Q_2 \ldots Q_n$ est le polynôme connu P/P_1.

- En remplaçant P par P_1, on obtient $Q_2 Q_3 \ldots Q_n = P_1/P_2$, où P_2 est le polynôme connu $P_1 \wedge P_1'$. Ainsi : $Q_1 = \frac{P}{P_1} / \frac{P_1}{P_2}$.

- En remplaçant encore P par P_1, on obtient : $Q_2 = \frac{P_1}{P_2} / \frac{P_2}{P_3}$, où P_3 est le polynôme connu $P_2 \wedge P_2'$, et, par récurrence ;

$$Q_k = \frac{P_{k-1}}{P_k} / \frac{P_k}{P_{k+1}} \text{ , où } P_{k+1} = P_k \wedge P_k'.$$

Exemple. On calcule 1/5. $P' = X^4 - 9X^2 + 4X + 12$. On en déduit :

$$P_1 = P \wedge P' = X^3 - X^2 - 8X + 12 \; ; \; P/P_1 = X^2 + X - 6.$$

On calcule : $P_1' = 3X^2 - 2X - 8$; on en déduit :

$$P_2 = P_1 \wedge P_1' = X - 2 \; ; \; P_1/P_2 = X^2 + X - 6.$$

D'où : $Q_1 = 1$; P n'a pas de zéro simple.

On calcule $P_2' = 1$; on en déduit $P_3 = 1$, et $P_2/P_3 = X-2$.

D'où : $Q_2 = X + 3$.

On calcule $P_3' = 0$; on en déduit $P_4 = 1$ et $P_3/P_4 = 1$.

D'où : $Q_3 = X - 2$.

A ce stade, P est divisible par $(X+3)^2(X-2)^3$. Compte tenu des degrés :

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

2.1.16 Soient un polynôme $P \in \mathbb{Q}[X]$ de degré $n \geqslant 1$, et a une racine complexe de P, de multiplicité m telle que $2m > n$. Vérifier : $a \in \mathbb{Q}$.

Exceptionnellement, nous donnerons deux solutions.

Première solution. L'ensemble J des éléments de $\mathbb{Q}[X]$ qui admettent la racine complexe a est visiblement un idéal de $\mathbb{Q}[X]$, non réduit à zéro puisque P lui appartient. Il s'agit donc des multiples d'un unique polynôme normalisé, $A \in \mathbb{Q}[X]$, de degré $p \geqslant 1$ (car $1 \notin J$).

Il est clair que $p = 1$, si et seulement si $a \in \mathbb{Q}$, (A est alors $X - a$).

- Supposons que a ne soit pas rationnel. Nous avons donc $p \geqslant 2$. Comme a ne peut être racine multiple de A (sans quoi A', de degré p-1, appartiendrait à J), A admet une racine complexe $b \neq a$.

Les polynômes $P, P', \ldots, P^{(m-1)}$ appartiennent à $\mathbb{Q}[X]$ et admettent a pour racine complexe ; ils appartiennent à J, et sont des multiples de A, ce qui entraîne qu'ils admettent b pour racine complexe : on en déduit que la multiplicité m' de la racine b de P vérifie $m' \geqslant m$. D'où $n \geqslant m+m' \geqslant 2m$, en contradiction avec $2m > n$. □

Deuxième solution. Nous allons montrer par récurrence qu'une assertion $(\mathcal{A}_n)$ est vraie pour tout $n \in \mathbb{N}^*$.

- $(\mathcal{A}_1)$ est vraie. En effet tout $P \in \mathbb{Q}[X]$, de degré 1, admet une unique racine complexe, et elle est rationnelle.

- Considérons $n \geqslant 2$ tel que $(\mathcal{A}_k)$ soit vraie pour tout $k \in \mathbb{N}_{n-1}$.

Soit $P \in \mathbb{Q}[X]$, de degré n, admettant une racine complexe a de multiplicité m telle que $2m > n$; on a $2m > 2$, i.e. $m-1 > 0$. Il en résulte que a est racine de multiplicité m-1 pour P', et aussi pour le PGCD de P et P' dans $\mathbb{C}[X]$, qui est noté Δ.

S'obtenant par divisions à partir de polynômes à coefficients rationnels, Δ est aussi le PGCD de P et P' dans $\mathbb{Q}[X]$. Le polynôme $Q \in \mathbb{Q}[X]$ défini par $P = \Delta Q$ admet a pour racine simple, et on a :

$$\deg \Delta + \deg Q = n, \quad \deg Q \geqslant 1.$$

Si $\deg Q = 1$, alors on constate $a \in \mathbb{Q}$ en appliquant $(\mathcal{A}_1)$ à Q.

Si $\deg Q \geqslant 2$, alors : $\deg \Delta \leqslant n-2 < 2(m-1)$, et on constate $a \in \mathbb{Q}$ en appliquant $(\mathcal{A}_k)$ à Δ, $(k = \deg \Delta)$. □

2.1.17 Soit $(a_0, \ldots, a_n)$ une famille de réels telle que $a_0 a_n \neq 0$, $(n \in \mathbb{N}^*)$. On dit que la famille présente un changement de signe à l'indice $i \in \mathbb{N}_n$ si, et seulement s'il existe $k \in \{0, \ldots, i-1\}$ tel que $a_k a_i < 0$ et que $a_\ell = 0$ pour tout ℓ tel que $k < \ell < i$.

Soit q le nombre des changements de signe de la famille .

1° Montrer que pour tout $\alpha \in \mathbb{R}_+^*$ le nombre q' des changements de signe de la famille $(-a_0\alpha, a_0 - a_1\alpha, a_1 - a_2\alpha, \ldots, a_{n-1} - a_n\alpha, a_n)$ vérifie $q' \geqslant q+1$.

2° Soit $P \in \mathbb{R}_n[X]$ le polynôme $a_0 + a_1 X + \ldots + a_n X^n$.

Montrer que le nombre m des racines strictement positives de P (comptées chacune avec sa multiplicité) vérifie $m \leqslant q$.

Pour $x \in \mathbb{R}$, on note $\operatorname{sgn} x = -1$ si $x < 0$, $\operatorname{sgn} 0 = 0$, $\operatorname{sgn} x = 1$ si $0 < x$.

1° Remarquons que $a_0 a_n \neq 0$ et $\alpha > 0$ entraînent $(-a_0\alpha)a_n \neq 0$.

1er cas : $q = 0$. On a $a_0 a_n > 0$ et donc $(-a_0\alpha)a_n < 0$. D'où $q' \geqslant 1$. □

2ème cas : $q = 1$. La famille initiale présente un unique changement de signe, à l'indice $i \in \mathbb{N}_n$. Puisque $a_i \neq 0$, on peut poser $\operatorname{sgn} a_i = \varepsilon$, $\varepsilon \in \{-1, 1\}$.

En adoptant les notations de la définition, on obtient :

$$\operatorname{sgn} a_k = -\varepsilon \ ; \ \operatorname{sgn} a_0 = -\varepsilon \ ; \ \operatorname{sgn}(-a_0\alpha) = \varepsilon \ ; \ \operatorname{sgn} a_n = \varepsilon.$$

Comme a_{i-1} est soit 0 soit a_k, il vient : $\operatorname{sgn}(a_{i-1} - \alpha a_i) = -\varepsilon$.

Pour la seconde famille, on a donc au moins un changement de signe entre $-a_0\alpha$ et $a_{i-1} - \alpha a_i$, ainsi qu'un changement de signe entre $a_{i-1} - \alpha a_i$ et a_n. D'où $q' \geqslant 2$. □

3ème cas : $q \geqslant 2$. Considérons deux changement de signes consécutifs, aux indices i et j, avec $i<j$. Posons encore $\operatorname{sgn} a_i = \varepsilon$. Il est clair que $\operatorname{sgn} a_j = -\varepsilon$, et, en raisonnant comme dans le cas précédent :

$$\operatorname{sgn}(a_{i-1} - \alpha a_i) = -\varepsilon, \quad \operatorname{sgn}(a_{j-1} - \alpha a_j) = \varepsilon.$$

On a ainsi un changement de signe (au moins) entre $a_{i-1} - \alpha a_i$ et $a_{j-1} - \alpha a_j$.

On dispose ainsi d'au moins q-1 changements de signe pour la seconde famille, auxquels il faut adjoindre deux changements de signe, l'un dans un intervalle d'origine $-a_o\alpha$, l'autre dans un intervalle d'extrêmité a_n (cf. 2ème cas). □

2° La première question joue le rôle d'un lemme servant à résoudre la seconde ; en effet la famille $(-a_o\alpha, \ldots, a_n)$ est celle des coefficients du polynôme $(a_o + \ldots + a_n X^n)(-\alpha + X)$, étant entendu que tous les polynômes qui interviennent sont ordonnés suivant les puissances croissantes de X.

Ecrivons alors $P = Q(-\alpha_1 + X)\ldots(-\alpha_m + X)$, où $\alpha_1, \ldots, \alpha_m$ sont les racines strictement positives de P (pas nécessairement distinctes).

Le nombre des changements de signe des coefficients du polynôme Q, qui est de la forme $\beta_o + \ldots + \beta_{n-m} X^{n-m}$ avec $\beta_o \beta_{n-m} \neq 0$, est noté r.

En utilisant 1°, on constate que les familles des coefficients de :

$$Q(-\alpha_1 + X),\ Q(-\alpha_1 + X)(-\alpha_2 + X), \ldots, P$$

ont respectivement un nombre de changements de signes au moins égal à r+1, r+2, ..., r+m.

D'où $r+m \leqslant q$ et $r \geqslant 0$, ce qui entraîne $m \leqslant q$.

2.1.18 Soit un polynôme $P \in \mathbf{R}[X]$ de degré $n \geqslant 2$, scindé sur $\mathbf{R}$ et de racines simples. On l'écrit $P = \sum_{k=o}^{n} a_k X^k$. Vérifier :

$$\forall k \in \mathbf{N}_{n-1} \quad a_{k-1} a_{k+1} < a_k^2 \qquad (1)$$

1° Etablissons le lemme suivant, que nous aurons à utiliser :

LEMME. *Soit* $Q \in \mathbf{R}[X]$ *de degré* $m \geqslant 1$, *scindé sur* $\mathbf{R}$ *et de racines simples. La fonction* $t \mapsto (Q'(t))^2 - Q(t)Q''(t)$ *ne prend que des valeurs strictement positives sur* $\mathbf{R}$.

- On peut écrire :

$$Q = a \prod_{i=1}^{m} (X - \alpha_i) \ ; \ a \in \mathbf{R}^* \ ; \ \alpha_i \neq \alpha_j \text{ si } i \neq j.$$

On en déduit les égalités de fractions rationnelles :

$$\frac{Q'}{Q} = \sum_{i=1}^{m} \frac{1}{X - \alpha_i}$$

et : $$\frac{Q'^2-QQ''}{Q^2} = \sum_{i=1}^{m} \frac{1}{(X-\alpha_i)^2} \qquad (2)$$

• Soit t un réel.

- Si t est racine de Q, alors $Q(t)=0$ et $Q'(t)\neq 0$ (sans quoi t serait racine multiple de Q) ; d'où :

$$\big(Q'(t)\big)^2 - Q(t)Q''(t) > 0 \qquad (3)$$

- Si t n'est pas racine de Q, alors (3) résulte de (2).

2° Venons-en à notre exercice. Dans chacun des n-1 intervalles ouverts de $\mathbb{R}$ dont les extrémités sont deux racines consécutives de P, le polynôme P' a au moins une racine (d'après le théorème de Rolle) et exactement une puisque son degré est n-1 ; P' est ainsi scindé sur $\mathbb{R}$ et de racines simples ; on montre par récurrence qu'il en est de même pour tout $P^{(k)}$, $k\in\mathbb{N}_{n-1}$.

Pour tout $k\in\mathbb{N}_{n-1}$, on a, en appliquant le lemme $Q = P^{(k-1)}$:

$$P^{(k-1)}(0)\ P^{(k+1)}(0) < \big(P^{(k)}(0)\big)^2$$

i.e. $$(k-1)!a_{k-1}\ (k+1)!\ a_{k+1} < (k!a_k)^2$$

et : $$a_{k-1}\ a_{k+1} < \frac{k}{k+1}\ a_k^2 \leqslant a_k^2.$$ □

2.1.19 Soit P un polynôme de $\mathbb{C}[X]$; montrer que toutes les racines de P' appartiennent à l'enveloppe convexe de l'ensemble des racines de P.

Désignons par $a_1,\ldots,a_p$ les racines de P de multiplicités respectives $m_1,\ldots,m_p$ ($m_j\geqslant 1$ pour $1\leqslant j\leqslant p$). On a l'égalité de fractions rationnelles :

$$\frac{P'}{P} = \sum_{j=1}^{p} \frac{m_j}{X-a_j}\ .$$

Soit a une racine de P' : si a est l'une des racines a_j, a est évidemment dans l'enveloppe convexe de ces racines. Dans le cas contraire on a :

$$\sum_{j=1}^{p} \frac{m_j}{a-a_j} = 0 \qquad (1)$$

Comme m_j est réel, (1) implique successivement :

$$\sum_{j=1}^{p} \frac{m_j}{\overline{a-a_j}} = 0 \quad \text{et} \quad \sum_{j=1}^{p} \frac{m_j}{|a-a_j|^2}\ (a-a_j) = 0.$$

Cette dernière relation prouve que a est barycentre de $a_1,\ldots,a_p$ affectés des coefficients strictement positifs $\frac{m_1}{|a-a_1|^2},\ldots,\frac{m_p}{|a-a_p|^2}$ □

Remarque. On retrouve le fait, établi directement dans l'exercice précédent, que si P est scindé sur $\mathbb{R}$, alors P' est scindé sur $\mathbb{R}$ et toutes les racines de P' appartiennent à l'intervalle : $[\min(a_j), \max(a_j)]$.

2.2. Fractions Rationnelles

2.2.1 1° Décomposer en éléments simples, la fraction rationnelle à coefficients réels :

$$F(X) = \frac{1}{(X-1)^m(X+1)^n}, \quad (m,n) \in (\mathbb{N}^*)^2.$$

2° Trouver les couples $\big(U(X),V(X)\big) \in (\mathbb{R}[X])^2$ vérifiant :

$$(X+1)^n U(X) + (X-1)^m V(X) = 1 \qquad (1)$$

1° La partie entière de F(X) étant nulle, F(X) est la somme des parties polaires $F_1(X)$ et $F_{-1}(X)$ relatives aux pôles 1 et -1, d'ordres m et n.

- Calculons $F_1(X)$. En posant $X-1=Y$, F(X) devient :

$$\frac{1}{Y^m} \cdot \frac{1}{2^n} \cdot \frac{1}{(1+Y/2)^n}.$$

Nous avons à calculer le quotient Q(Y) de la division suivant les puissances croissantes de 1 par $(1+Y/2)^n$ à l'ordre m-1. Or nous savons que Q(t) est le développement limité à l'ordre m-1 au voisinage de 0 de la fonction rationnelle $\frac{1}{(1+t/2)^n}$.

En utilisant :

$$(1+t/2)^{-n} = 1 + \sum_{k=1}^{m-1} (-1)^k \frac{n(n+1)\ldots(n+k-1)}{2^k k!} t^k + o(t^{m-1})$$

on constate que :

$$Q(Y) = 1 + \sum_{k=1}^{m-1} (-1)^k \frac{n(n+1)\ldots(n+k-1)}{2^k k!} Y^k.$$

On en déduit : $F_1(X) = \frac{A(X)}{(X-1)^m}$, où $A(X) = \frac{1}{2^n} Q(X-1)$

- Un calcul analogue conduit à :

$$F_{-1}(X) = \frac{B(X)}{(X+1)^n}, \text{ où } B(X) = \frac{1}{(-2)^m} R(X+1)$$

et : $$R(Y) = 1 + \sum_{k=1}^{n-1} \frac{n(n+1)\ldots(n+k-1)}{2^k k!} Y^k.$$

2° Les polynômes $(X+1)^n$ et $(X-1)^m$ sont premiers entre eux.

On en déduit l'existence et l'unicité d'une solution de (1) telle que deg U(X) <m et deg V(x) <n. On déduit du 1° que $\big(A(X),B(X)\big)$ est cette solution. Les autres solutions sont les :

$$\big(A(X) + (X-1)^m C(X),\ B(X) - (X+1)^n C(X)\big),\ C(X) \in \mathbb{R}[X]$$

Autre solution du 2°. De $2^{-m-n+1}[(X+1)-(X-1)]^{m+n-1} = 1$, on déduit par la formule du binôme de Newton :

$$A(X) = \frac{1}{2^{m+n-1}} \sum_{k=o}^{m-1} (-1)^k C_{m+n-1}^k (X-1)^k (X+1)^{m-1-k}$$

$$B(X) = \frac{1}{2^{m+n-1}} \sum_{k=o}^{n-1} (-1)^{m+k} C_{m+n-1}^{m+k} (X-1)^k (X+1)^{n-1-k}.$$

2.2.2 Soient $a_1,\ldots,a_n$ des nombres complexes deux à deux distincts, tels qu'aucun n'appartienne à $\{i,-i\}$. On leur associe :

$$P = \prod_{k=1}^{n} (X-a_k) \; ; \; F = \frac{(1+X^2)^n}{P^2} .$$

1° Décomposer la fraction rationnelle F en éléments simples.

2° Trouver, sous forme d'une relation entre P, P' et P'' une condition nécessaire et suffisante pour que F soit la dérivée d'une fraction rationnelle.

1° Les a_k, $1 \leqslant k \leqslant n$, dont aucun n'est racine de $1+X^2$, sont les pôles de F, chacun étant de multiplicité 2.

Les polynômes $(1+X^2)^n$ et P^2 étant de même degré 2n, et de même coefficient dominant 1, la partie entière de F est le polynôme constant 1.

La décomposition en éléments simples (unique) de F s'écrit donc :

$$F = 1 + \sum_{k=1}^{n} \left(\frac{\alpha_k}{(X-a_k)^2} + \frac{\beta_k}{X-a_k} \right)$$

Pour calculer α_k et β_k, k donné, on applique la formule de Taylor à $(1+X^2)^n$ et à P^2, et on constate que les polynômes $(1+X^2)^n$ et $P^2/(X-a_k)^2$ admettent les expressions respectives :

$$(1+a_k^2)^n + 2na_k(1+a_k^2)^{n-1}(X-a_k) + R(X-a_k)^2$$

et :
$$\left(P'(a_k)\right)^2 + P'(a_k)P''(a_k)(X-a_k) + S(X-a_k)^2$$

dans lesquelles R et S sont des éléments de $\mathbb{C}[X]$, et $P'(a_k) \neq 0$.

On calcule les deux premiers termes du quotient d'une division suivant les puissances croissantes de $X-a_k$, et on obtient :

$$\alpha_k = \left(P'(a_k)\right)^{-2}(1+a_k^2)^n$$

$$\beta_k = \left(P'(a_k)\right)^{-3}(1+a_k^2)^{n-1}\left[2na_kP'(a_k) - (1+a_k^2)P''(a_k)\right]$$

2° On vérifie aisément l'équivalence des assertions suivantes :

i) F est la dérivée d'une fraction rationnelle ;

ii) $\beta_k = 0$ pour tout $k \in \{1,\ldots,n\}$;

iii) Le polynôme $(1+X^2)P'' - 2nXP'$ s'annule en chacun des a_k ;

iv) Pour tout $\lambda \in \mathbb{C}$, le polynôme $P_\lambda = (1+X^2)P'' - 2nXP' + \lambda P$ s'annule en chacun des a_k.

• En remarquant que le coefficient de X^n dans P_λ est :

$$n(n-1) - 2n^2 + \lambda = \lambda - n(n+1)$$

et que deg $P_\lambda < n$ si $\lambda = n(n+1)$, on constate que iv), et par suite i) équivaut à l'assertion :

v) Le polynôme $(1+X^2)P'' - 2nXP' + n(n+1)P$ est nul.

En effet un polynôme de degré strictement inférieur à n, ayant n racines distinctes est nul.

2.2.3 1° On donne $p \in \mathbb{N}^*$, et les nombres complexes non nuls et deux à deux distincts $\rho_1, \ldots, \rho_p$. On note $P = \prod_{i=1}^{p} (X-\rho_i)$.

Montrer que, pour tout $n \in \mathbb{N}$, on peut écrire, de manière unique :

$$X^n = E_n P + \sum_{i=1}^{p} \alpha_{ni} P_i, \qquad P_i = \prod_{j \neq i} (X-\rho_j)$$

avec $E_n \in \mathbb{C}[X]$ et $(\alpha_{n1}, \ldots, \alpha_{np}) \in \mathbb{C}^p$.

2° Ici P est le polynôme : $pX^p - X^{p-1} - X^{p-2} - \ldots - X - 1$.

Montrer que P admet p racines simples, l'une étant 1, les autres étant de module strictement inférieur à 1.

3° Soit $a = (a_m)_{m \in \mathbb{N}}$ la suite définie par la donnée de $(a_0, \ldots, a_{p-1}) \in \mathbb{C}^p$ et de :

$$\forall m \in \mathbb{N} \quad a_{m+p} = \frac{a_m + a_{m+1} + \ldots + a_{m+p-1}}{p}.$$

Montrer que cette suite converge et a pour limite le barycentre de $(a_0, \ldots, a_{p-1})$ affecté des coefficients $(1, \ldots, p)$.

1° Soit $n \in \mathbb{N}$. Aucun des ρ_i n'étant nul, on dispose de la fraction rationnelle irréductible $\frac{X^n}{P}$ dont les pôles, tous simples, sont les ρ_i.

La théorie de la décomposition en éléments simples nous apprend l'existence et l'unicité d'une égalité de la forme :

$$\frac{X^n}{P} = E_n + \sum_{i=1}^{p} \alpha_{ni} \frac{1}{X-\rho_i}, \text{ où } \alpha_{ni} = \frac{\rho_i^n}{P'(\rho_i)} \qquad \square$$

2° Soit : $Q = (X-1)P = pX^{p+1} - (p+1)X^p + 1$.

On calcule : $Q' = p(p+1)\, X^{p-1}(X-1)$.

Les racines de Q' sont 0 et 1, celle-ci étant simple ; 0 n'est pas racine de Q ; 1 est racine de Q ; il en résulte que Q admet la racine double 1, et p-1 autres racines non nulles, toutes simples ; P admet ainsi p racines simples, non nulles, dont l'une est 1.

Soit ρ une racine de P autre que 1. On a :

$$p\rho^p = 1 + \rho + \ldots + \rho^{p-1} \qquad (1)$$

- On n'a pas $|\rho| > 1$, sans quoi on aurait :

$$|\rho^p| > |\rho|^k \text{ pour tout } k \in \{0, \ldots, p-1\}$$

et : $$|p\rho^p| > 1 + |\rho| + \ldots + |\rho|^{p-1} \geqslant |1 + \rho + \ldots + \rho^{p-1}|$$

en contradiction avec (1).

- On n'a pas $|\rho| = 1$, sans quoi, compte tenu de $\rho \neq 1$, on aurait :

$$|1+\rho| < 1 + |\rho| = 2, \text{ et } |\rho^2 + \ldots + \rho^{p-1}| \leqslant p-2$$

et, compte tenu de (1) et de $|p\rho^p| = p$:

$$p \leqslant |1+\rho| + |\rho^2 + \ldots + \rho^{p-1}| < p.$$

En conclusion : $|\rho| < 1$. □

Dans ce qui suit, P désigne le polynôme du 2°, dont les racines sont notées $\rho_1, \ldots, \rho_p$, avec $\rho_1 = 1$, et on utilise 1°.

3° Notons E le $\mathbb{C}$-espace vectoriel des suites complexes. Nous disposons de : $u \in \mathcal{L}(E)$, avec $(x_n) \mapsto (y_n)$, où $y_n = x_{n+1}$ pour tout $n \in \mathbb{N}$.

Nous constatons que, pour tout $k \in \mathbb{N}$, $u^k \in \mathcal{L}(E)$ est défini par :

$$(x_n) \mapsto (y_n), \text{ où } y_n = x_{n+k} \text{ pour tout } n \in \mathbb{N}.$$

• Soit $n \in \mathbb{N}$. On déduit du 1° l'égalité d'endomorphismes de E :

$$u^n = E_n(u) \circ P(u) + \sum_{i=1}^{p} \alpha_{ni} P_i(u) \qquad (2)$$

Ecrivons que les images de la suite a par les deux membres de (2) sont des suites égales. Comme : $pa_{m+p} - a_{m+p-1} - \ldots - a_m = 0$ pour tout $m \in \mathbb{N}$ entraîne $P(u)(a) = 0$, il vient :

$$u^n(a) = \sum_{i=1}^{p} \alpha_{ni} P_i(u)(a), \quad \alpha_{ni} = \rho_i^n / P'(\rho_i) \qquad (3)$$

Ecrivons que les termes d'indice 0 des deux membres de (3) sont égaux :

$$a_n = \sum_{i=1}^{p} \alpha_{ni} \beta_i$$

où $\beta_i = \big(P_i(u)(a)\big)_0$, terme d'indice 0 de $P_i(u)(a)$, ne dépend pas de n.

• En adoptant $\rho_1 = 1$ et $|\rho_i| < 1$ si $i \in \{2, \ldots, p\}$, on constate :

$$\lim_{n \to +\infty} a_n = \frac{1}{P'(1)} \big(P_1(u)(a)\big)_0$$

On calcule : $P'(1) = p(p+1)/2$.

En utilisant la division euclidienne de P par X-1, on constate :

$$P_1(X) = pX^{p-1} + (p-1)X^{p-2} + \ldots + 2X + 1$$

et on en déduit que la suite a est convergente, et a pour limite :

$$\frac{2}{p(p+1)} (a_0 + 2a_1 + \ldots + (p-1)a_{p-2} + pa_{p-1})$$ □

3. ESPACES VECTORIELS

3.1. GÉNÉRALITÉS

3.1.1 Soient $(a,b) \in \mathbf{R}^2$, $a<b$, et E l'ensemble des applications continues et affines par morceaux de $[a,b]$ dans $\mathbf{R}$ (à toute $f \in E$ on peut associer une subdivision $(a_i)_{0 \leqslant i \leqslant n}$ de $[a,b]$ telle que la restriction de f à chaque $[a_{i-1},a_i]$ soit affine).

1° Montrer que E est un $\mathbf{R}$-espace vectoriel.

2° A tout $c \in [a,b]$, on associe $f_c \in E$, telle que $f_c(t) = |t-c|$ pour tout $t \in [a,b]$.

Montrer que la famille $(f_c)_{c \in [a,b]}$ est une base de E.

3° Même question, en définissant ici f_c par :

- Si $c \in [a,b[$, alors $f_c(t) = 0$ pour tout $t \in [a,c]$, et $f_c(t) = t-c$ pour $t \in [c,b]$;
- Si $c = b$, alors $f_c(t) = 1$ pour tout $t \in [a,b]$.

1° Contenant l'application nulle de $[a,b]$ dans $\mathbf{R}$, E n'est pas vide.

- Soient $(\alpha,\beta) \in \mathbf{R}^2$ et $(f,g) \in E^2$. En réunissant des subdivisions de $[a,b]$ respectivement adaptées à f et à g, on obtient une subdivision $(a_i)_{0 \leqslant i \leqslant n}$ adaptée à la fois à f et à g ; les restrictions de f et g à chaque $[a_{i-1},a_i]$, $1 \leqslant i \leqslant n$, sont affines ; la restriction de l'application continue $\alpha f + \beta g$ à chaque $[a_{i-1},a_i]$ est donc affine, et on a : $\alpha f + \beta g \in E$.

- En conclusion, E est un sous-espace vectoriel de $\mathbf{R}^{[a,b]}$.

2° a) Soit $(\alpha_c)_{c \in [a,b]}$ une famille presque nulle de réels telle que :

$$\sum_{c \in [a,b]} \alpha_c f_c = 0 \quad \text{(application nulle de } [a,b] \text{ dans } \mathbf{R}) \qquad (1)$$

Faisons l'hypothèse : il existe $\gamma \in]a,b[$ tel que $\alpha_\gamma \neq 0$; $\alpha_\gamma f_\gamma$ est non dérivable en γ ; les $\alpha_c f_c$, $c \in [a,b] \setminus \{\gamma\}$ et l'application nulle sont dérivables en γ ; notre hypothèse conduit donc à une contradiction.

L'égalité (1) s'écrit ainsi : $\alpha_a f_a + \alpha_b f_b = 0$.

On a : $\alpha_a f_a(a) + \alpha_b f_b(a) = 0$, avec $f_a(a) = 0$ et $f_b(a) \neq 0$; d'où $\alpha_b = 0$. On a alors : $\alpha_a f_a(b) = 0$, avec $f_a(b) \neq 0$; d'où $\alpha_a = 0$.

Ainsi (1) exige la nullité de la famille (α_c) ; la famille (f_c) est donc libre.

b) Reste à montrer que la famille (f_c) est génératrice de E.

- Soit $f \in E$. Fixons une subdivision $(a_i)_{0 \leqslant i \leqslant n}$ adaptée à f. Soit E' l'ensemble des applications continues de [a,b] dans $\mathbf{R}$ dont la restriction à chaque $[a_{i-1}, a_i]$, $1 \leqslant i \leqslant n$, est affine. Il est clair que E' est un sous-espace vectoriel de E, qui contient f, et aussi chaque f_{a_i}, $0 \leqslant i \leqslant n$.

Comme l'application $g \mapsto \big(g(a_0), \ldots, g(a_n)\big)$ de E' dans $\mathbf{R}^{n+1}$ est visiblement un isomorphisme, E' est de dimension finie n+1.

La famille $(f_{a_i})_{0 \leqslant i \leqslant n}$ de n+1 éléments de l'espace vectoriel E' de dimension n+1 est libre $\big($sans quoi $(f_c)_{c \in [a,b]}$ serait liée dans E$\big)$; c'est donc une base de E'.

- Toute $f \in E$ s'exprime ainsi sous la forme d'une combinaison linéaire des éléments d'une sous-famille de (f_c), qui est ainsi génératrice de E. □

3° Le raisonnement du 2° peut être repris sans modification.

3.1.2 Soit E un K-espace vectoriel de dimension finie $n > 0$. On appelle <u>drapeau</u> de E toute famille de sous-espaces de E qui est de la forme $(E_i)_{0 \leqslant i \leqslant n}$ et vérifie :

i) $E_0 \subset E_1 \subset \ldots \subset E_n$;

ii) $\dim E_i = i$ pour tout $i \in \{0, \ldots, n\}$.

Soient $(E_i)_{0 \leqslant i \leqslant n}$ et $(E'_i)_{0 \leqslant i \leqslant n}$ deux drapeaux de E.

1° a) Soit $i \in \mathbf{N}_n$; on lui associe :

$$j = \sigma(i) = \inf\{k \in \{0, \ldots, n\} \mid E'_i + E_k = E'_{i-1} + E_k\}.$$

Vérifier que j existe et appartient à $\mathbf{N}_n$.

Vérifier que $E'_i \setminus E'_{i-1}$ et $E_j \setminus E_{j-1}$ ont un élément commun.

b) Montrer que l'application σ de $\mathbf{N}_n$ dans $\mathbf{N}_n$ définie en a) est une permutation.

2° Montrer qu'il existe une base $(e_1, \ldots, e_n)$ de E telle que, pour tout $i \in \mathbf{N}_n$, $(e_1, \ldots, e_i)$ soit une base de E_i et $\big(e_{\sigma(1)}, \ldots, e_{\sigma(i)}\big)$ une base de E'_i.

Deux remarques pour commencer.

α) Considérons le drapeau $(E_i)_{0\leqslant i\leqslant n}$ de E. On a : $E_o = \{0\}$ et $E_n = E$. D'autre D'autre part, pour tout $i \in \mathbf{N}_n$, E_{i-1} est un hyperplan de E_i. On choisit arbitrairement $e_i \in E_i \setminus E_{i-1}$, on a : $E_i = E_{i-1} \oplus Ke_i$; on vérifie (par récurrence) que $(e_1,\ldots,e_i)$ est une base de E_i ; en particulier, $(e_1,\ldots,e_n)$ est une base de E.

β) Inversement, si $(\varepsilon_1,\ldots,\varepsilon_n)$ est une base de E, en posant $F_o = \{0\}$, et $F_i = \mathrm{Vect}(\varepsilon_1,\ldots,\varepsilon_i)$ pour tout $i \in \mathbf{N}_n$, on obtient un drapeau $(F_i)_{0\leqslant i\leqslant n}$ de E.

1° a) • Défini comme le plus petit élément d'une partie de $\{0,\ldots,n\}$ qui contient n et ne contient pas 0, j existe et appartient à $\mathbf{N}_n$.

• Pour tout $k \in \{0,\ldots,n\}$ l'égalité $E'_i + E_k = E'_{i-1} + E_k$ entraîne $E'_i \subset E'_{i-1} + E_k$; inversement, cette inclusion entraîne $E'_i + E_k \subset E'_{i-1} + E_k$, et donc $E'_i + E_k = E'_{i-1} + E_k$. Il y a ainsi équivalence entre l'égalité et l'inclusion considérées.

- D'après la définition de j, E'_i est inclus dans $E'_{i-1} + E_j$ et n'est pas inclus dans $E'_{i-1} + E_{j-1}$. On dispose donc de $z \in E'_i$, appartenant à $E'_{i-1} + E_j$ mais pas à $E'_{i-1} + E_{j-1}$; on peut écrire :

$$z = x+y, \text{ avec } y \in E'_{i-1},\ x \in E_j \text{ et } x \notin E_{j-1}.$$

On a $x \notin E'_{i-1}$, sans quoi on aurait $z \in E'_{i-1}$ et $z \in E'_{i-1} + E_{j-1}$.

A cause de $z \in E'_i$ et $y \in E'_i$, on a $x \in E'_i$.

En conclusion, x appartient à $E'_i \setminus E'_{i-1}$ et à $E_j \setminus E_{j-1}$. □

b) En échangeant les rôles des deux drapeaux, nous pouvons définir une application τ de $\mathbf{N}_n$ dans $\mathbf{N}_n$ par :

$$\ell = \tau(j) = \inf\{k \in \{0,\ldots,n\} \mid E_j + E'_k = E_{j-1} + E'_k\}$$

- Considérons $i \in \mathbf{N}_n$, $j = \sigma(i)$, $\ell = \tau(j)$.

- Reprenant un vecteur x commun à $E'_i \setminus E'_{i-1}$ et $E_j \setminus E_{j-1}$ (cf. a)), nous avons : $E_j = E_{j-1} \oplus Kx \subset E_{j-1} + E'_i$, ce qui montre que $\ell \leqslant i$.

- D'autre part, on n'a pas $E_j \subset E_{j-1} + E'_{i-1}$, sans quoi on aurait $E'_{i-1} + E_j \subset E_{j-1} + E'_{i-1}$ et donc $E'_i \subset E'_{i-1} + E_{j-1}$, en contradiction avec $j = \sigma(i)$. Il en résulte $i-1 < \ell$, et finalement $\ell = i$.

• Nous avons ainsi prouvé que $\tau \circ \sigma$ est l'identité de $\mathbf{N}_n$; σ est ainsi une injection de $\mathbf{N}_n$ dans $\mathbf{N}_n$, et donc une permutation de $\mathbf{N}_n$; la permutation réciproque de σ est τ.

2° Pour tout élément $j = \sigma(i)$ de $\mathbf{N}_n$, nous pouvons (cf. 1°) choisir un vecteur e_j commun à $E'_i \setminus E'_{i-1}$ et à $E_j \setminus E_{j-1}$. Nous obtenons ainsi une famille $(e_1,\ldots,e_n)$.

D'après la remarque initiale α), pour tout $j \in \mathbf{N}_n$, $(e_1,\ldots,e_j)$ est une base de E_j et, en particulier, $(e_1,\ldots,e_n)$ est une base de E.

Comme $i = \tau(j)$ décrit $\mathbf{N}_n$ quand j décrit $\mathbf{N}_n$, pour tout $i \in \mathbf{N}_n$, $(e_{\sigma(1)}, \ldots, e_{\sigma(i)})$ est une base de E'_i. □

3.1.3 1° Ici le corps commutatif K est infini ; E est un K-espace vectoriel. Montrer que si $(F_i)_{1 \leqslant i \leqslant p}$ est une famille finie de sous-espaces vectoriels de E tous distincts de E, alors $\bigcup_{i=1}^{p} F_i$ est distinct de E.

2° Application. Soit $(a_i)_{1 \leqslant i \leqslant p}$ une famille finie de points de $\mathbf{R}^n$, $n \in \mathbf{N}^*$, dont aucun n'est nul. Montrer qu'il existe un hyperplan de $\mathbf{R}^n$ ne contenant aucun des a_i.

1° Il s'agit de montrer qu'une assertion $(\mathcal{A}_p)$ est vraie pour tout $p \in \mathbf{N}^*$. Raisonnons par récurrence.

- Il est clair que $(\mathcal{A}_1)$ est vraie.
- Soit $p \geqslant 2$, pour lequel $(\mathcal{A}_{p-1})$ a été vérifiée. Considérons une famille $(F_i)_{1 \leqslant i \leqslant p}$ de sous-espaces vectoriels de E tous distincts de E.

- D'après $(\mathcal{A}_{p-1})$, $A = \bigcup_{i=1}^{p-1} F_i$ est distinct de E. Si l'un des ensembles A ou F_p est inclus dans l'autre, $(\mathcal{A}_p)$ est donc vérifiée.

- Plaçons-nous maintenant dans le cas où aucun des ensembles A ou F_p n'est inclus dans l'autre. Nous disposons donc de $x \in A$ tel que $x \notin F_p$, et de $y \in F_p$ tel que $y \notin A$. Remarquons d'abord que :

i) Pour tout $\alpha \in K$, le point $x+\alpha y$ n'appartient pas à F_p (sinon, à cause de $y \in F_p$, on aurait $x \in F_p$) ;

ii) Pour tout $(\alpha, \beta) \in K^2$ tel que $\alpha \neq \beta$, les points $x+\alpha y$ et $x+\beta y$ ne peuvent appartenir à un même F_i, $1 \leqslant i \leqslant p-1$ (sinon on aurait $(\alpha-\beta)y \in F_i$, et $y \in F_i$ et $y \in A$).

Considérons alors une famille $(\alpha_i)_{1 \leqslant i \leqslant p}$ d'éléments deux à deux distincts de K, ce qui est possible puisque K est infini. En utilisant ii) nous constatons que, nécessairement, l'un des points $x+\alpha_i y$ n'appartient pas à A ; ce point n'appartenant pas à F_p d'après i), il n'appartient pas à $A \cup F_p$, qui est ainsi distinct de E ; $(\mathcal{A}_p)$ est donc vérifiée. □

Remarque. La proposition ne s'étend pas :
- au cas d'un corps K fini (si $K = \mathbb{Z}/2\mathbb{Z}$ et $E = K^2$, il est clair que E est la réunion des trois droites F_i définies par les couples de points $\{(0,0),(0,1)\}$, $\{(0,0),(1,1)\}$ et $\{(0,0),(1,0)\}$.
- au cas où (F_i) est une famille infinie (si $K = \mathbf{R}$ et $E = \mathbf{R}[X]$, il est clair que E est la réunion de la famille $(\mathbf{R}_n[X])_{n \in \mathbf{N}}$ de sous-espaces distincts de E).

2° Remarquons que : si a est un point non nul de $\mathbf{R}^n$, alors l'ensemble des formes linéaires sur $\mathbf{R}^n$ qui s'annulent en a est un hyperplan de $(\mathbf{R}^n)^*$.

En effet, d'après $a \neq 0$, il existe une base $(e_1,\ldots,e_n)$ de $\mathbf{R}^n$ telle que $e_1 = a$; soit $(e_1^*,\ldots,e_n^*)$ la base duale de $(\mathbf{R}^n)^*$; toute forme linéaire sur $\mathbf{R}^n$ s'écrit $\sum_{j=1}^{n} \beta_i e_i^*$, et elle s'annule en a si, et seulement si $\beta_1 = 0$.

• Appliquant ce résultat, nous pouvons associer à chacun des points donnés a_i, $1 \leqslant i \leqslant p$, l'hyperplan H_i^* de $(\mathbf{R}^n)^*$ ensemble des formes linéaires sur $\mathbf{R}^n$ qui s'annulent en a_i.

$\mathbf{R}$ étant infini, et $(H_i^*)_{1\leqslant i\leqslant p}$ étant une famille finie de sous-espaces du $\mathbf{R}$-espace vectoriel $(\mathbf{R}^n)^*$ tous distincts de $(\mathbf{R}^n)^*$, d'après le 1°, $\bigcup_{i=1}^{p} H_i^*$ est distinct de $(\mathbf{R}^n)^*$; il existe une forme linéaire x^* sur $\mathbf{R}^n$ qui ne s'annule en aucun des a_i ; elle est non nulle ; son noyau est un hyperplan de $\mathbf{R}^n$ qui ne contient aucun des a_i. □

3.1.4 Sans admettre l'existence d'un supplémentaire de tout sous-espace d'un espace vectoriel, montrer que, si E' est un sous-espace de codimension finie p d'un K-espace vectoriel E, alors il existe au moins un sous-espace E" de E supplémentaire de E' et dim E" = p.

Si dim $E < +\infty$, le résultat est classique. Nous ne faisons donc aucune hypothèse sur dim E.

• E/E', de dimension finie p, admet une base qui est nécessairement de la forme $b = \big(\varphi(e_1),\ldots,\varphi(e_p)\big)$, où φ est la surjection canonique de E sur E/E', et où $e = (e_1,\ldots,e_p)$ est une famille de vecteurs de E qui est libre (sans quoi son image par φ serait liée). On note E" le sous-espace de E dont une base est e.

• Soit x un élément de E. On dispose des coordonnées $(\xi_1,\ldots,\xi_p)$ de $\varphi(x)$ dans la base b, et donc du vecteur $x'' = \sum_{i=1}^{p} \xi_i e_i \in E''$, avec $\varphi(x) = \varphi(x'')$, ce qui s'écrit $x - x'' \in E'$.

• On a donc $E = E' + E''$.

• Par ailleurs, pour tout $x'' = \sum_{i=1}^{p} \xi_i e_i \in E''$, on a $x'' \in E'$ si, et seulement si $\varphi(x'') = \sum_{i=1}^{p} \xi_i \varphi(e_i)$ est nul, ce qui s'écrit $\xi_1 = \ldots = \xi_p = 0$, i.e. $x'' = 0$. D'où $E = E' \oplus E''$.

E" est ainsi un supplémentaire de E' dans E, et dim E" = p. □

3.1.5 Pour toute application linéaire u d'un K-espace vectoriel dans un autre, on note : $\nu(u) = \dim(\mathrm{Ker}\, u)$ et $\gamma(u) = \mathrm{codim}\,(\mathrm{Im}\, u)$; lorsque $\nu(u)$ et $\gamma(u)$ sont finis, on pose $\delta(u) = \gamma(u) - \nu(u)$.

Soient E,F,G trois K-espaces vectoriels, $u \in \mathcal{L}(E,F)$ et $v \in \mathcal{L}(F,G)$.

On note w l'élément vu de $\mathcal{L}(E,G)$.

1° Sans admettre que tout sous-espace d'un espace vectoriel admet un supplémentaire, montrer que :

a) Si $\nu(u)$ et $\nu(v)$ sont finis, alors $\nu(w)$ est fini ;

b) Si $\gamma(u)$ et $\gamma(v)$ sont finis, alors $\gamma(w)$ est fini.

2° Ici $\nu(u)$, $\nu(v)$, $\gamma(u)$, $\gamma(v)$ sont finis. Montrer :

$$\delta(w) = \delta(u) + \delta(v).$$

• Dans le cas particulier où E,F,G sont tous trois de dimension finie, le 1° est trivial ; quant au 2°, il se déduit de ce que, ici :

$$\delta(u) = \dim F - \dim E \quad \text{et} \quad \delta(v) = \dim G - \dim F.$$

• Dans la suite, nous ne faisons aucune hypothèse sur les dimensions de E,F,G. Le lecteur vérifiera que, dans tous les cas où nous aurons besoin de l'existence d'un supplémentaire, celle-ci sera assurée par le résultat de l'exercice précédent.

1° a) La restriction de u à Ker w admet pour noyau Ker u, et pour image $F_1 = \text{Ker } v \cap \text{Im } u$; on a $\dim F_1 \leqslant \dim(\text{Ker } v) = \nu(v)$.

Ker w/Ker u est ainsi isomorphe à F_1, et donc de dimension finie ; d'où l'existence de E' tel que $\text{Ker } w = \text{Ker } u \oplus E'$ et $\dim E' = \dim F_1$. On a :

$$\nu(w) = \nu(u) + \dim F_1 < +\infty. \qquad \square$$

b) De $\gamma(u) < +\infty$ on déduit $F = \text{Im } u \oplus F'$, avec $\dim F' = \gamma(u)$. D'où :

$$v(F) = v(\text{Im } u) + v(F'), \text{ i.e. } \text{Im } v = \text{Im } w + v(F'), \text{ et } \dim v(F') \leqslant \gamma(u).$$

De codimension finie dans Im v, Im w admet ainsi un supplémentaire G' dans Im v et $\dim G' \leqslant \gamma(u)$.

En outre, de $\gamma(v) < +\infty$ on déduit $G = \text{Im } v \oplus G''$, avec $\dim G'' = \gamma(v)$.

D'où : $G = \text{Im } w \oplus G' \oplus G''$ et $\gamma(w) = \dim G' + \gamma(v) < +\infty$. $\square$

2° Ici les résultats du 1° a) et du 1° b) s'appliquent.

Soit F_2 un supplémentaire de $F_1 = \text{Ker } v \cap \text{Im } u$ dans Ker v (de dimension finie) ; on a : $\dim F_1 + \dim F_2 = \nu(v)$, et $\text{Im } u \cap F_2 = \{0_F\}$.

On vérifie que la somme $\text{Im } u \oplus F_2$ est de codimension finie ; il existe donc F_3 tel que $F = \text{Im } u \oplus F_2 \oplus F_3$, avec $\dim F_3 = \gamma(u) - \dim F_2$.

En prenant les images par v, et compte tenu de $v(F_2) = \{0_G\}$:

$$\text{Im } v = \text{Im } w + v(F_3).$$

Cette dernière somme est directe car $v(y) = v(z)$, avec $y \in \text{Im } u$ et $z \in F_3$ exige $z \in \text{Im } u + \text{Ker } v$, i.e. $z \in \text{Im } u \oplus F_2$, et $z = 0_F$ et $v(z) = 0_G$.

D'autre part $F_3 \cap \operatorname{Ker} v = \{0_F\}$ entraîne $v(F_3) \simeq F_3$.

Reprenant $G = \operatorname{Im} v \oplus G''$ avec $\dim G'' = \gamma(v)$ nous avons :

$$G = \operatorname{Im} w \oplus v(F_3) \oplus G''$$

et : $\gamma(w) = \dim F_3 + \gamma(v) = \gamma(u) + \gamma(v) - \dim F_2$.

Or (cf. 1°a) : $\nu(w) = \nu(u) + \dim F_1 = \nu(u) + \nu(v) - \dim F_2$.

Par différence : $\delta(w) = \delta(u) + \delta(v)$. □

3.1.6 On donne $n \in \mathbb{N}^*$, et on note E au lieu de $\mathbb{R}_n[X]$.

1° Soient n+1 réels $h_0, \ldots, h_n$ deux à deux distincts. Montrer que la famille $\left((X+h_i)^n\right)_{0 \leqslant i \leqslant n}$ est une base de l'espace vectoriel E.

2° Montrer que l'ensemble & des $\varphi \in \mathcal{L}(E)$ vérifiant :

$$\forall h \in \mathbb{R} \quad \forall P \in E \quad \varphi\big(P(X+h)\big) = \big(\varphi(P)\big)(X+h)$$

est une sous-algèbre de $\mathcal{L}(E)$ de dimension n+1.

1° La famille donnée étant composée de n+1 éléments d'un espace vectoriel E de dimension n+1, montrer qu'elle est une base de E équivaut à montrer qu'elle est libre.

Soit $(\alpha_0, \ldots, \alpha_n) \in \mathbb{R}^{n+1}$ tel que : $\sum_{i=0}^{n} \alpha_i (X+h_i)^n = 0$ (polynôme nul).

En utilisant la formule du binôme de Newton, on obtient :

$$\forall k \in \{0, \ldots, n\} \quad \sum_{i=0}^{n} \alpha_i h_i^k = 0$$

ce qui montre que $(\alpha_0, \ldots, \alpha_n)$ est une solution d'un système linéaire et homogène de n+1 équations à n+1 inconnues ; on constate que le déterminant de ce système est le Vandermonde de la famille $(h_0, \ldots, h_n)$ dont les éléments sont deux à deux distincts ; ce déterminant est donc non nul et le système est cramérien, ce qui entraîne : $(\alpha_0, \ldots, \alpha_n) = (0, \ldots, 0)$. □

2° A tout $h \in \mathbb{R}$ on associe l'application $\theta_h : E \longrightarrow E$ telle que :

$$\sum_{k=0}^{n} a_k X^k \longmapsto \sum_{k=0}^{n} a_k (X+h)^k.$$

Il est clair que θ_h est un endomorphisme de E.

& est l'ensemble des $\varphi \in \mathcal{L}(E)$ vérifiant :

$$\forall h \in \mathbb{R} \quad \forall P \in E \quad \varphi\big(\theta_h(P)\big) = \theta_h\big(\varphi(P)\big)$$

i.e. $$\forall h \in \mathbb{R} \quad \varphi\theta_h = \theta_h\varphi.$$

Sous cette forme, il est évident que & est une sous-algèbre de $\mathcal{L}(E)$

contenant tous les θ_h, $h\in\mathbf{R}$ (car, pour tout $(h_1,h_2)\in\mathbf{R}^2$, θ_{h_1} et θ_{h_2} commutent).

En particulier & contient θ_1, noté désormais θ, et ses itérés $\theta^i = \theta_i$, $i\in\mathbf{N}$. Nous allons montrer que la famille $\varepsilon = (\theta^i)_{0\leqslant i\leqslant n}$ est une base de &, ce qui entraînera : dim & = n+1.

• *La famille* ε *est libre dans* $\mathcal{L}(E)$, *et donc dans* &. En effet, d'après 1°, la famille des $\theta^i(X^n) = (X+i)^n$, $i\in\{0,\dots,n\}$, est libre dans E ; a fortiori la famille ε est libre dans $\mathcal{L}(E)$.

• *La famille* ε *est génératrice de* &. En effet considérons un $\varphi\in$&. L'élément $\varphi(X^n)$ de E s'écrit dans la base $\big((X+j)^n\big)$, $j\in\{0,\dots,n\}$:

$$\varphi(X^n) = \sum_{j=0}^{n} \alpha_j (X+j)^n = \sum_{j=0}^{n} \alpha_j \theta^j(X^n).$$

Pour tout $i\in\{0,\dots,n\}$, on a :

$$\varphi\big((X+i)^n\big) = \varphi\big(\theta^i(X^n)\big) = \theta^i\big(\varphi(X^n)\big)$$
$$= \sum_{j=0}^{n} \alpha_j \theta^{i+j}(X^n) = \sum_{j=0}^{n} \alpha_j \theta^j\big((X+i)^n\big).$$

Donnant la même image de chacun des éléments de la base $(X+i)^n$, $i\in\{0,\dots,n\}$, de E, les deux endomorphismes φ et $\sum_{j=0}^{n} \alpha_j \theta^j$ de E coïncident. □

3.2. Applications Linéaires. Matrices

3.2.1 <u>Projecteurs</u>. Ici le corps commutatif K est de caractéristique nulle ; E est un K-espace vectoriel de dimension finie $n>0$.

1° Pour toute famille finie $(p_i)_{1\leqslant i\leqslant k}$ d'endomorphismes de E dont la somme est $I = Id_E$, vérifier l'équivalence des assertions :

i) $p_i p_j = 0$ pour tout $(i,j)\in\mathbf{N}_k^2$ tel que $i\neq j$, $(\mathbf{N}_k = \{1,\dots,k\})$;

ii) p_i est un projecteur pour tout $i\in\mathbf{N}_k$.

2° Pour toute famille finie $(p_i)_{1\leqslant i\leqslant k}$ de projecteurs de E, vérifier l'équivalence des assertions :

i) $p_i p_j = 0$ pour tout $(i,j)\in\mathbf{N}_k^2$ tel que $i\neq j$;

ii) $\sum_{i=1}^{k} p_i$ est un projecteur.

La notation $\sum_{j\neq i}$ est mise pour $\sum_{j\in\mathbf{N}_k\setminus\{i\}}$

1° Nous utiliserons le résultat suivant : *dans les conditions de l'énoncé, si* p *est un projecteur de* E *alors son rang est égal à sa trace.*

En effet E est la somme directe de Im p et de Ker p, et la matrice qui représente p dans une base de E obtenue en réunissant une base de Im p et

et une base de Ker p est de la forme diag(1,...,1,0,...,0), le nombre des 1 étant dim (Im p).

• Preuve de i) ⇒ ii). Par hypothèse, i) est vraie. Pour $i \in \mathbb{N}_k$ fixé :

$$p_i = p_i I = p_i \sum_{j=1}^{k} p_j = p_i^2. \qquad \square$$

• Preuve de ii) ⇒ i). Par hypothèse ii) est vraie. Fixons $i \in \mathbb{N}_k$.

Comme p_i est un projecteur, $I-p_i = \sum_{j\neq i} p_j$ est un projecteur dont l'image est le noyau F de p_i. On a :

$$F = \operatorname{Im}\left(\sum_{j\neq i} p_j\right) \subset \sum_{j\neq i} \operatorname{Im} p_j$$

et d'autre part

$$\dim F = \operatorname{tr}\left(\sum_{j\neq i} p_j\right) = \sum_{j\neq i} \operatorname{tr} p_j = \sum_{j\neq i} \dim(\operatorname{Im} p_j).$$

On en déduit que $F = \operatorname{Ker} p_i$ est la somme directe des $\operatorname{Im} p_j$, $j \in \mathbb{N}_k \setminus \{i\}$. Chacune de ces $\operatorname{Im} p_j$ est donc incluse dans $\operatorname{Ker} p_i$, ce qui montre que l'on a $p_i p_j = 0$ pour tout $j \in \mathbb{N}_k \setminus \{i\}$. $\square$

2° Preuve de i) ⇒ ii). L'hypothèse $p_i p_j = 0$ pour $i \neq j$ entraîne :

$(p_1+\ldots+p_k)^2 = p_1^2 +\ldots+ p_k^2$, et, les p_i étant ici des projecteurs:

$$(p_1 +\ldots+ p_k)^2 = p_1 +\ldots+ p_k,$$

ce qui montre que $p_1 +\ldots+ p_k$ est un projecteur. $\square$

• Preuve de ii) ⇒ i). L'hypothèse $\sum_{i=1}^{k} p_i$ est un projecteur entraîne : $I - \sum_{i=1}^{k} p_i$ est un projecteur ; on le note p_{k+1} et on a :

$$\sum_{i=1}^{k+1} p_i = I, \text{ où } p_i \text{ est un projecteur pour tout } i \in \mathbb{N}_{k+1}.$$

D'après 1°, il en résulte : $p_i p_j = 0$ pour tout $(i,j) \in \mathbb{N}_{k+1}^2$ tel que $i \neq j$ et, en particulier pour tout $(i,j) \in \mathbb{N}_k^2$ tel que $i \neq j$.

Complément. Si l'on n'impose à K que de ne pas être de caractéristique 2, et si E est un K-espace vectoriel de dimension finie ou infinie, alors pour tout couple (p,q) de projecteurs de E les assertions suivantes sont équivalentes :

i) p+q est un projecteur ;

ii) $pq + qp = 0$;

iii) $pq = qp = 0$.

Preuve. On a : $(p+q)^2 = p + q + pq + qp$.

L'équivalence de i) et ii) en résulte .

- De $pq + qp = 0$, on déduit d'une part $p^2q + pqp = 0$ et donc $pq + pqp = 0$, d'autre part $pqp + qp^2 = 0$ et donc $pqp + qp = 0$.

De $pq + qp = 0$, on déduit donc $pq = qp$, et $2pq = 0$, et (K n'étant pas de caractéristique 2) $pq = qp = 0$. D'où ii) $\Rightarrow$ iii).

- Inversement, il est clair que iii) $\Rightarrow$ ii). □

3.2.2 Soient E un K-espace vectoriel, et u un endomorphisme de E. On suppose qu'il existe un et un seul endomorphisme v de E tel que $uv = Id_E$. Montrer que u est un automorphisme.

En utilisant les règles de calcul dans l'anneau $\mathcal{L}(E)$, on obtient successivement : $uvu = u$, puis $uw = 0$, où $w = vu - Id_E$.

On en déduit : $u(v+w) = Id_E$. D'après l'unicité de l'inverse à droite de u dans $\mathcal{L}(E)$, il vient : $v+w = v$, i.e. $w = 0$.

Ainsi : $uv = vu = Id_E$, et donc $v \in GL(E)$. □

3.2.3 <u>Théorèmes de factorisation</u>. Soient E,F,G trois K-espaces vectoriels.

1° Soient $u \in \mathcal{L}(E,F)$ et $w \in \mathcal{L}(E,G)$. Montrer que les deux assertions suivantes sont équivalentes :

i) Il existe $v \in \mathcal{L}(F,G)$ telle que $w = v \circ u$;

ii) $\operatorname{Ker} u \subset \operatorname{Ker} w$.

2° Soient $v \in \mathcal{L}(F,G)$ et $w \in \mathcal{L}(E,G)$. Montrer que les deux assertions suivantes sont équivalentes :

i) Il existe $u \in \mathcal{L}(E,F)$ telle que $w = v \circ u$;

ii) $\operatorname{Im} w \subset \operatorname{Im} v$.

On admettra ici (résultat classique en dimension finie) que tout sous-espace d'un espace vectoriel admet un supplémentaire.

Comme d'habitude, nous écrirons vu pour $v \circ u$.

1° <u>Preuve de</u> i) $\Rightarrow$ ii). $w = vu$ entraîne $w(x) = 0$ pour tout $x \in \operatorname{Ker} u$. □

<u>Preuve de</u> ii) $\Rightarrow$ i). Par hypothèse : $\operatorname{Ker} u \subset \operatorname{Ker} w$.

Nous disposons d'un supplémentaire F_1 de Im u dans F. Pour obtenir une application linéaire v de F dans G, il est nécessaire et suffisant de se donner deux applications linéaires v_0 de Im u dans G, et v_1 de F_1 dans G ; v est alors l'application, visiblement linéaire, de F dans G dont v_0 et v_1 sont les restrictions à Im u et à F_1 respectivement.

Adoptons pour v_1 l'application nulle de F_1 dans G.

Nous constatons par ailleurs que, pour tout $y \in \operatorname{Im} u$, si x et x' sont deux éléments du sous-ensemble non vide $u^{-1}(\{y\})$ de E, alors $x - x'$ appartient à Ker u et donc à Ker w, ce qui entraîne $w(x) = w(x')$. Nous disposons donc de l'application $v_0 : \operatorname{Im} u \longrightarrow G$ définie par :

$$\forall y \in \operatorname{Im} u \quad v_o(y) = w(x),\ x \in u^{-1}(\{y\}) \text{ arbitrairement choisi.}$$

La linéarité de v_o résulte de ce que pour tous $(\alpha,\alpha') \in K^2$ et $(y,y') \in (\operatorname{Im} u)^2$, si x (resp. x') est un antécédent par u de y (resp. y') alors, par linéarité de u, $\alpha x + \alpha' x'$ est un antécédent de $\alpha y + \alpha' y'$ et :

$$v_o(\alpha y + \alpha' u') = w(\alpha x + \alpha' x') = \alpha w(x) + \alpha' w(x') = \alpha v_o(y) + \alpha' v_o(y').$$

L'application $v : F \longrightarrow G$ dont les restrictions à Im u et à F_1 sont v_o et v_1 est linéaire et, par construction :

$$\forall x \in E \quad v\big(u(x)\big) = v_o\big(u(x)\big) = w(x),\ \big(\text{car } x \in u^{-1}\big(\{u(x)\}\big)\big). \qquad \square$$

2° Nous pourrions procéder par dualité. Raisonnons directement.

Preuve de i) ⇒ ii). Pour tout $z \in \operatorname{Im} w$, il existe $x \in E$ tel que $z = w(x)$; puisqu'ici $w = vu$, on a $z = v\,u(x)$, ce qui montre : $z \in \operatorname{Im} v$. $\square$

Preuve de ii) ⇒ i). Par hypothèse $\operatorname{Im} w \subset \operatorname{Im} v$.

Nous disposons d'un supplémentaire F_2 de Ker v dans F. Nous savons que v induit un isomorphisme v_2 de F_2 sur Im v ; $x \mapsto v_2^{-1}\big(w(x)\big)$, considérée comme une application u de E dans F, est linéaire et, par construction :

$$\forall x \in E \quad v\big(u(x)\big) = v\big(v_2^{-1}(w(x))\big) = w(x). \qquad \square$$

3.2.4 Soient u,v et w trois endomorphismes d'un K-espace vectoriel E.

1° On suppose ici : $(\operatorname{Ker} u \cap \operatorname{Ker} v) \subset \operatorname{Ker} w$ (1)

Montrer qu'il existe $(a,b) \in \big(\mathcal{L}(E)\big)^2$ tel que $w = au + bv$.

2° On suppose ici : $\operatorname{Im} w \subset (\operatorname{Im} u + \operatorname{Im} v)$ (2)

Montrer qu'il existe $(a,b) \in \big(\mathcal{L}(E)\big)^2$ tel que $w = ua + vb$.

1° Soit v_1 et w_1 les restrictions de v et w à Ker u ; ce sont des applications linéaires de Ker u dans E de noyaux $\operatorname{Ker} u \cap \operatorname{Ker} v$ et $\operatorname{Ker} u \cap \operatorname{Ker} w$.

De (1) on déduit : $(\operatorname{Ker} u \cap \operatorname{Ker} v) \subset (\operatorname{Ker} u \cap \operatorname{Ker} w)$, i.e. $\operatorname{Ker} v_1 \subset \operatorname{Ker} w_1$.

D'après un théorème de factorisation, il existe $b \in \mathcal{L}(E)$ tel que $w_1 = bv_1$.

- L'endomorphisme w-bv de E vérifie :

$$\forall x \in \operatorname{Ker} u \quad (w-bv)(x) = w_1(x) - b\big(v_1(x)\big) = 0.$$

On a donc : $\operatorname{Ker} u \subset \operatorname{Ker}(w-bv)$, et, d'après le même théorème de factorisation, il existe $a \in \mathcal{L}(E)$ tel que : $w - bv = au$. $\square$

2° On raisonne par dualité en utilisant :

$$\forall f \in \mathcal{L}(E) \quad (\operatorname{Im} f)^{\perp} = \operatorname{Ker} {}^t f$$

D'aorès un résultat de dualité, on a :

$$(\mathrm{Im}\ u + \mathrm{Im}\ v)^{\perp} = (\mathrm{Im}\ u)^{\perp} \cap (\mathrm{Im}\ v)^{\perp}$$

et, compte tenu de (2) qui entraîne $(\mathrm{Im}\ u + \mathrm{Im}\ v)^{\perp} \subset (\mathrm{Im}\ w)^{\perp}$:

$$(\mathrm{Ker}\ {}^t u \cap \mathrm{Ker}\ {}^t v) \subset \mathrm{Ker}\ {}^t w.$$

D'après 1°, il existe $(\alpha,\beta) \in \left(\mathcal{L}(E^*)\right)^2$ tel que ${}^t w = \alpha\, {}^t u + \beta\, {}^t v$.

D'où : $w = ua + vb$, avec $a = {}^t\alpha$ et $b = {}^t\beta$. □

3.2.5 Soit E un K-espace vectoriel de dimension finie $n > 0$. On se propose de trouver tous les idéaux de $\mathcal{L}(E)$ (à gauche, à droite, bilatères).

1° A tout sous-espace V de E on associe :

$$g(V) = \{u \in \mathcal{L}(E) \mid V \subset \mathrm{Ker}\ u\}\ ;\ d(V) = \{u \in \mathcal{L}(E) \mid \mathrm{Im}\ u \subset V\}.$$

Montrer que ce sont des idéaux de $\mathcal{L}(E)$, respectivement à gauche et à droite.

2° Inversement, soient I un idéal à gauche de $\mathcal{L}(E)$, et $F = \bigcap_{u \in I} \mathrm{Ker}\ u$.

a) Montrer qu'il existe $u_o \in I$ tel que $F = \mathrm{Ker}\ u_o$. En déduire $I = g(F)$.

b) Montrer que pour tout $p \in \mathcal{L}(E)$ de noyau F, on a $I = \mathcal{L}(E)p$.

3° Etudier de même un idéal à droite de $\mathcal{L}(E)$.

4° Montrer que les seuls idéaux bilatères de $\mathcal{L}(E)$ sont $\{0\}$ et $\mathcal{L}(E)$.

Ce résultat subsiste-t-il si E n'est pas de dimension finie ?

5° Soit $\mathcal{J}$ l'ensemble des idéaux à gauche (resp. à droite ; resp. bilatères) de $\mathcal{L}(E)$. Trouver les éléments maximaux de $(\mathcal{J} \setminus \mathcal{L}(E), \subset)$.

1° Vérification aisée, laissée au lecteur.

2° a) Les noyaux des $u \in \mathcal{L}(E)$ sont des sous-espaces de E. L'ensemble $\{\dim(\mathrm{Ker}\ u) \mid u \in I\}$ est une partie de $\{0,\ldots,n\}$ non vide puisque $I \neq \phi$; il admet un plus petit élément n_o, et il existe $u_o \in I$ tel que $\mathrm{Ker}\ u_o$ soit de dimension n_o.

Il est clair que $F \subset \mathrm{Ker}\ u_o$. Montrons par l'absurde que $F = \mathrm{Ker}\ u_o$. Pour cela, faisons l'hypothèse : $F \neq \mathrm{Ker}\ u_o$. C'est qu'il existe $x \in \mathrm{Ker}\ u_o$ tel que $x \notin F$, ce qui entraîne qu'il existe $u_1 \in I$ tel que $x \notin \mathrm{Ker}\ u_1$.

Il en résulte que $\mathrm{Ker}\ u_1 \cap \mathrm{Ker}\ u_o$ est un sous-espace strict de $\mathrm{Ker}\ u_o$; considérons un endomorphisme w de E dont le noyau est ce sous-espace (par exemple un projecteur).

Puisque $(\mathrm{Ker}\ u_1 \cap \mathrm{Ker}\ u_o) \subset \mathrm{Ker}\ w$, d'après le 1° de l'exercice précédent il existe $(a,b) \in \left(\mathcal{L}(E)\right)^2$ tel que $w = au_1 + bu_o$, ce qui entraîne $w \in I$, en contradiction avec :

$$\dim(\mathrm{Ker}\ w) < \dim(\mathrm{Ker}\ u_o) = n_o.$$ □

• A ce stade, on a : $I \subset g(F)$.

• Inversement, soit $u \in g(F)$. De $\operatorname{Ker} u_o \subset \operatorname{Ker} u$ on déduit, par un théorème de factorisation, l'existence de $v \in \mathcal{L}(E)$ tel que $u = vu_o$; on a donc $u \in I$.

Ainsi $g(F) \subset I$ et, finalement : $I = g(F)$. □

b) Considérons $p \in \mathcal{L}(E)$ de noyau F. D'après ce qui précède on a $p \in I$ et donc $\mathcal{L}(E)p \subset I$.

D'autre part, pour tout $u \in I$, on a $\operatorname{Ker} p \subset \operatorname{Ker} u$, et il existe $v \in \mathcal{L}(E)$ tel que $u = vp$; on a donc $u \in \mathcal{L}(E)p$.

Ainsi $I \subset \mathcal{L}(E)p$ et, finalement $I = \mathcal{L}(E)p$. □

On dit que l'idéal à gauche I de $\mathcal{L}(E)$ est *principal*, et que les endomorphismes de E de noyau F en sont des *générateurs* ; on vérifie aisément que ce sont tous les générateurs de I. Parmi ceux-ci, les plus utilisés dans la pratique sont les projecteurs de noyau F.

3° *Soient* J *un idéal à droite de* $\mathcal{L}(E)$, et $G = \sum_{u \in J} \operatorname{Im} u$. *On a* $J = d(G)$; *pour tout* $q \in \mathcal{L}(E)$ *d'image* G, *on a* $J = q\mathcal{L}(E)$.

La démonstration, analogue à celle du 2°, est laissée au lecteur, qui commencera par montrer qu'il existe $v_o \in J$ tel que :

$$\forall v \in J \quad \dim(\operatorname{Im} v) \leqslant \dim(\operatorname{Im} v_o)$$

et en déduire $G = \operatorname{Im} v_o$, en utilisant cette fois le 2° de l'exercice précédent.

On peut aussi raisonner par dualité.

4° Il est clair que $\{0\}$ et $\{\mathcal{L}(E)\}$ sont des idéaux bilatères de $\mathcal{L}(E)$.

• Soit I un idéal bilatère non nul de $\mathcal{L}(E)$. S'agissant d'un idéal à droite non nul, il existe un sous-espace non nul G de E tel que :

$$I = \{u \in \mathcal{L}(E) \mid \operatorname{Im} u \subset G\}.$$

Soit $x \in G \setminus \{0\}$. A tout hyperplan H de E, on peut associer $u \in \mathcal{L}(E)$ de noyau H et d'image Kx, ce qui entraîne $u \in I$ (on choisit $y \in E \setminus H$ et on définit u par $u(H) = \{0\}$ et $u(y) = x$).

Il en résulte $\bigcap_{u \in I} \operatorname{Ker} u = \{0\}$ et, au titre d'idéal à gauche, I s'écrit ;

$$I = \{u \in \mathcal{L}(E) \mid \{0\} \subset \operatorname{Ker} u\} = \mathcal{L}(E).$$ □

• Le contre-exemple qui suit montre que le résultat ne subsiste pas si E n'est pas de dimension finie.

Soit $E = \mathbb{R}[X]$. L'ensemble J des endomorphismes de E dont le rang est fini est visiblement un idéal bilatère de $\mathcal{L}(E)$. L'identité de E n'appartenant pas à J on a $J \neq \mathcal{L}(E)$. D'autre part $J \neq \{0\}$; l'application qui à $P \in E$ associe le polynôme constant P(0) est en effet un endomorphisme non nul de rang fini, et donc un élément non nul de J. □

5° La notion d'idéal maximal d'un anneau commutatif est étendue aux anneaux non commutatifs.

• Le lecteur montrera que, pour tout couple (V,V') de sous-espaces de E, $g(V) \subset g(V')$ équivaut à $V' \subset V$. Un idéal à gauche de $\mathcal{L}(E)$ est donc maximal si et seulement s'il écrit g(V), avec dim V = 1.

• De même un idéal à droite de $\mathcal{L}(E)$ est maximal si et seulement s'il s'écrit d(V), avec codim V = 1.

• Il est clair que {0} est le seul idéal bilatère maximal.

3.2.6 Ici le corps commutatif K est de caractéristique nulle.

1° Soit $A \in \mathcal{M}_n(K)$ de diagonale nulle (i.e. formée de zéros). Montrer qu'il existe dans $\mathcal{M}_n(K)$ une matrice diagonale D et une matrice X telles que :

$$DX - XD = A.$$

2° Pour tout $n \in \mathbb{N}^*$, montrer qu'à tout endomorphisme u de trace nulle d'un K-espace vectoriel E de dimension n, on peut associer une base de E dans laquelle u est représenté par une matrice de diagonale nulle.

3° Soient E un K-espace vectoriel de dimension finie $n > 0$, et $\mathcal{C}(E)$ l'ensemble des *commutateurs* de $\mathcal{L}(E)$ (endomorphismes de E de la forme fg-gf).

Montrer que $\mathcal{C}(E)$ est un sous-espace vectoriel de $\mathcal{L}(E)$; en donner une base.

1° Ecrivons $A = [\alpha_{ij}]$, $(i,j) \in \mathbb{N}_n^2$, avec $\alpha_{ii} = 0$ pour tout $i \in \mathbb{N}_n$.

Soient $D = \mathrm{diag}(\eta_1, \ldots, \eta_n)$ et $X = [\xi_{ij}]$, $(i,j) \in \mathbb{N}_n^2$.

L'élément (i,j) de DX - XD est :

$$\sum_{k=1}^{n} \delta_{ik}\eta_i\xi_{kj} - \sum_{k=1}^{n} \xi_{ik}\delta_{kj}\eta_j = (\eta_i - \eta_j)\xi_{ij}$$

Un corps de caractéristique nulle étant un ensemble infini, nous pouvons choisir pour $\eta_1, \ldots, \eta_n$ des éléments deux à deux distincts de K (par exemple $1_K, \ldots, n1_K$) et, pour avoir DX-XD = A, il suffira d'adopter :

$$\xi_{ij} = (\eta_i - \eta_j)^{-1}\alpha_{ij} \text{ si } i \neq j \ ; \ \xi_{ij} \text{ quelconque si } i = j. \qquad \square$$

2° Vérifions par récurrence qu'une assertion $(\mathcal{A}_n)$ est vraie pour tout $n \in \mathbb{N}^*$.

- Il est clair que $(\mathcal{A}_1)$ est vraie.

- Soit $n \geqslant 2$ pour lequel $(\mathcal{A}_{n-1})$ a été vérifiée. Considérons un K-espace vectoriel E de dimension n, et $u \in \mathcal{L}(E)$ de trace nulle.

Si u = 0, il est clair que l'on peut représenter u par une matrice de diagonale nulle. Supposons maintenant $u \neq 0$. Une homothétie non nulle ayant

une trace non nulle (K est de caractéristique nulle), u n'est pas une homothétie. On en déduit aisément qu'il existe $e_n \in E$ tel que $(e_n, u(e_n))$ soit une famille libre ; en complétant cette famille en une base de E, on constate qu'il existe un hyperplan E' de E qui contient $u(e_n)$ et ne contient pas e_n ; soient p le projecteur sur E' parallèlement à Ke_n, et u' l'endomorphisme $x \mapsto p(u(x))$ de E'.

Pour toute base $e' = (e_1, \ldots, e_{n-1})$ de E', on dispose de la base e de E obtenue en adjoignant e_n à e', et on peut poser :

$$A = \mathrm{mat}(u;e) = [\alpha_{ij}],\ (i,j) \in \mathbb{N}_n^2.$$

On a : $\alpha_{nn} = 0$, tr A = 0 et :

$$A' = \mathrm{mat}(u';e') = [\alpha_{ij}],\ (i,j) \in \mathbb{N}_{n-1}^2$$

ce qui montre que A', et donc u' sont de trace nulle.

En utilisant $(\mathcal{A}_{n-1})$, on constate que l'on peut choisir e' de façon que A' soit de diagonale nulle ; A est alors de diagonale nulle. □

3° D'après tr(fg) = tr(gf) et la linéarité de la trace, tout commutateur de $\mathcal{L}(E)$ a une trace nulle.

Inversement, soit $u \in \mathcal{L}(E)$ de trace nulle. En utilisant 2°, on introduit une base e de E telle que A = mat(u;e) soit de diagonale nulle. En utilisant 1°, on écrit A sous la forme DX-XD, et on en déduit u = fg-gf, où f et g sont les endomorphismes de E représentés par D et X dans la base e ; u est donc un commutateur de $\mathcal{L}(E)$.

$\mathcal{C}(E)$ est ainsi l'ensemble des endomorphismes de E de trace nulle, i.e. le noyau de la forme linéaire non nulle $u \mapsto \mathrm{tr}\, u$ sur $\mathcal{L}(E)$. Il s'agit donc d'un sous-espace de $\mathcal{L}(E)$, de dimension n^2-1.

• Pour en obtenir une base, partons d'une base $(\varepsilon_1, \ldots, \varepsilon_n)$ arbitrairement choisie de E, et considérons la base (g_{ij}), $(i,j) \in \mathbb{N}_n^2$, de $\mathcal{L}(E)$ définie par :

$$\forall (i,j) \in \mathbb{N}_n \quad \forall k \in \mathbb{N}_n \quad g_{ij}(\varepsilon_k) = \delta_{jk}\varepsilon_i.$$

Nous disposons ainsi des n^2-n endomorphismes g_{ij}, $i \neq j$, et des n-1 endomorphismes $g_{ii}-g_{nn}$, $i \in \mathbb{N}_{n-1}$, tous de trace nulle, et, en tout, de n^2-1 commutateurs, qui sont linéairement indépendants puisque, la famille (g_{ij}) étant libre, l'égalité :

$$\sum_{i \neq j} \lambda_{ij} g_{ij} + \sum_{i=1}^{n-1} \mu_i (g_{ii} - g_{nn}) = 0$$

exige la nullité des λ_{ij} et celle des μ_i.

Nous avons donc trouvé une famille libre de n^2-1 éléments du sous-espace $\mathcal{C}(E)$ de dimension n^2-1 ; il s'agit d'une base. □

3.2.7 Soient A et B deux matrices carrées d'ordre n à coefficients réels, et C la matrice A+iB. Montrer que si A et C sont inversibles, alors $M = A+BA^{-1}B$ est inversible, et $C^{-1} = M^{-1} - iA^{-1}BM^{-1}$.

• De $CA^{-1} = I_n + iBA^{-1}$ on déduit : $\det(I_n + iBA^{-1}) = \det(C).\det(A^{-1}) \neq 0$, et, par conjugaison : $\det(I_n - iBA^{-1}) \neq 0$.

Il en résulte que la matrice produit $(I_n + iBA^{-1})(I_n - iBA^{-1})$ égale à $I_n + BA^{-1}BA^{-1}$ est inversible, et donc aussi $M = (I_n + BA^{-1}BA^{-1})A$.

• Un simple calcul fournit alors :

$$\begin{aligned} C(M^{-1} - iA^{-1}BM^{-1}) &= (A+iB)(M^{-1} - iA^{-1}BM^{-1}) \\ &= AM^{-1} + BA^{-1}BM^{-1} + i(BM^{-1} - AA^{-1}BM^{-1}) \\ &= (A + BA^{-1}B)M^{-1} = I_n. \end{aligned}$$ □

Remarque. Ce résultat permet, lorsque A est inversible, de calculer l'inverse de la matrice A+iB en utilisant des programmes de calcul approché de l'inverse d'une matrice (programmes fonctionnant en général pour des matrices réelles).

Lorsque B est inversible on se ramène au cas précédent en écrivant $C = i(B-iA)$.

3.2.8 Soient $n \geqslant 2$ et $A = [\alpha_{ij}]$ la n-n matrice réelle telle que $\alpha_{ii} = a$ et $\alpha_{ij} = b$ pour $i \neq j$ (a et b réels donnés). Calculer, pour $p \in \mathbb{N}$, la matrice A^p et, lorsque c'est possible, la matrice A^{-1}.

Introduisons la matrice J de terme général constant égal à 1. On constate aisément $J^2 = nJ$, puis par récurrence, $J^p = n^{p-1}J$ pour tout entier $p \geqslant 1$.

Ecrivons alors : $A = (a-b)I + bJ$. La formule du binôme de Newton, qui s'applique puisque I et J commutent, fournit :

$$A^p = (1/n)\left[\sum_{k=1}^{p} C_p^k (a-b)^{p-k}(bn)^k\right] J + (a-b)^p I$$

d'où :

$$A^p = (1/n)\left[(a-b+bn)^p - (a-b)^p\right] J + (a-b)^p I$$

Le terme général de A^p en résulte immédiatement ($p \geqslant 1$).

• Les valeurs propres de J sont 0 (ordre n-1) et n (ordre 1) (exercice classique ; on peut utiliser le fait que J est symétrique à coefficients réels). Pour $b \neq 0$, on peut écrire : $\det A = b^n \det((a-b)/b.I + J)$; A est donc inversible si et seulement si $-(a-b)/b$ n'est pas valeur propre de J, c'est-à-dire si et seulement si $a \neq b$ et $a-b+nb \neq 0$. Pour $b = 0$, ce résultat reste valable.

Nous supposons donc $a \neq b$ et $a-b+nb \neq 0$. En cherchant l'inverse sous la forme $xI + yJ$, nous constatons, compte tenu de $J^2 = nJ$:

$$A^{-1} = \frac{1}{a-b} I - \frac{b}{(a-b)(a-b+nb)} J$$

Remarque. La formule donnant A^p pour $p \geqslant 1$ est aussi valable pour $p = 0$ et $p = -1$.

3.2.9 Dans $\mathcal{M}_n(\mathbb{R})$, trouver les matrices M telles que $M^2 = I+J$, où $I = I_n$ et où l'élément (i,j) de J est 1 si $j = i+1$ et 0 sinon.

Indication. On montrera que toute solution commute avec J.

Notons que, pour tout $k \in \mathbb{N}$, J^k est la (n,n)-matrice dont l'élément (i,j) est 1 si $j = i+k$ et 0 sinon ; en particulier $J^k = 0$ pour $k \geqslant n$.

a) Supposons qu'il existe une solution A. De $J = A^2 - I$ on déduit $AJ = JA$ (la valeur commune étant $A^3 - A$).

Nous considérons comme acquis le résultat suivant, qui sera justifié au 4.3.11 (en montrant que J est "cyclique") : les $M \in \mathcal{M}_n(\mathbb{R})$ commutant avec J sont les $\sum_{k=0}^{n-1} \alpha_k J^k$, $\alpha_k \in \mathbb{R}$; la solution A est nécessairement de la forme :

$$A = \sum_{k=0}^{n-1} \alpha_k J^k .$$

Cette dernière égalité entraîne $A^2 = \alpha_o^2 I + B$, où $B \in \mathrm{Vect}(J,\ldots,J^{n-1})$, et on a même nécessairement $\alpha_o^2 = 1$.

b) Les "racines carrées" de I+J sont donc les matrices $\pm P(J)$ où $P \in \mathbb{R}_{n-1}[X]$ vérifie la condition :

$$\big(P(0) = 1\big) \wedge \big(P^2 = 1+X \pmod{X^n}\big) \qquad (1)$$

$P^2 = 1+X \pmod{X^n}$ s'écrit :

$$\big(P(t) + \sqrt{1+t}\big)\big(P(t) - \sqrt{1+t}\big) = o(t^{n-1}) \text{ au voisinage de 0.}$$

$P(0) = 1$ s'écrit : $\lim_{t \to o} \big(P(t) + \sqrt{1+t}\big) = 2$.

Pour tout $P \in \mathbb{R}_{n-1}[X]$, (1) s'écrit donc :

$$P(t) - \sqrt{1+t} = o(t^{n-1}) \text{ au voisinage de 0,}$$

i.e. $t \mapsto P(t)$ est le développement limité à l'ordre n-1 de $t \mapsto \sqrt{1+t}$ au voisinage de 0.

En conclusion, les racines carrées de I+J sont les deux matrices :

$$\pm \left(I + \frac{1}{2} J + \sum_{k=2}^{n-1} (-1)^{k-1} \frac{1.3\ldots(2k-3)}{2.4\ldots\ldots(2k)} J^k \right) .$$

3.2.10 1° Montrer que la partie G de $\mathcal{M}_n(K)$ formée des matrices triangulaires supérieures à éléments diagonaux non nuls est un groupe multiplicatif.

2° Montrer que la partie H de G formée des matrices à éléments diagonaux égaux à 1 est un sous-groupe distingué de G.

1° Toute $A \in G$ vérifie $\det A \neq 0$ et est donc inversible. En outre $I_n \in G$. G est donc une partie non vide de $GL_n(K)$, qui est un groupe multiplicatif.

Nous allons montrer que G est un sous-groupe de $GL_n(K)$ et, pour cela, que G est stable pour la multiplication et que, pour toute matrice de G, l'inverse dans $GL_n(K)$ appartient à G.

• Solution par le calcul. Soient $A = [\alpha_{ij}] \in G$ et $B = [\beta_{ij}] \in G$.

- On constate $AB = [\gamma_{ij}]$ avec $\gamma_{ij} = \sum_{k=1}^{j} \alpha_{ik}\beta_{kj}$.

On a $\gamma_{ij} = 0$ pour $i > j$, $\gamma_{jj} = \alpha_{jj}\beta_{jj} \neq 0$ pour tout j, et donc $AB \in G$.

- Ici $A \in G$ est fixé, et on cherche $B \in G$ telle que $AB = I_n$, i.e.

$$\forall j \in \mathbb{N}_n \quad \left(\beta_{jj} = (\alpha_{jj})^{-1}\right) \wedge \left(\sum_{k=i}^{j} \alpha_{ik}\beta_{kj} = 0 \text{ pour tout } i \in \mathbb{N}_{j-1}\right)$$

Pour $j \in \mathbb{N}_n$ donné, $\beta_{jj} \neq 0$ est déterminé sans ambiguïté ; la seconde condition, compte-tenu de la non nullité des α_{ii}, permet d'obtenir successivement, d'une façon et d'une seule : $\beta_{j-1,j}$, $\beta_{j-2,j}, \ldots, \beta_{1,j}$. □

• Autre solution. On commence par vérifier que, pour toute $A \in GL_n(K)$ il y a équivalence entre les assertions :

i) A appartient à G ;

ii) Pour toutes bases e et f de K^n telles que $A = P_e^f$, on a :

$$\forall k \in \mathbb{N}_n \quad \text{Vect}(f_1, \ldots, f_k) = \text{Vect}(e_1, \ldots, e_k).$$

La proposition s'en déduit immédiatement.

2° a) H, qui contient I_n, est une partie non vide de G.

- Si $A = [\alpha_{ij}]$ et $B = [\beta_{ij}]$ sont des éléments de H, on a $AB \in G$ et, par ailleurs, tous les éléments diagonaux de AB sont des 1 ; d'où $AB \in H$.

- Toute $A = [\alpha_{ij}] \in H$ a une inverse dans G, $B = [\beta_{ij}]$, avec :

$\beta_{jj} = (\alpha_{jj})^{-1} = 1$ pour tout $j \in \mathbb{N}_n$; d'où $B \in H$.

H est donc un sous-groupe de G.

b) Soient $A = [\alpha_{ij}] \in G$ et $M = [\mu_{ij}] \in H$; AMA^{-1} est une matrice de G dont le j-ème élément diagonal est $\alpha_{jj}\mu_{jj}(\alpha_{jj})^{-1}$, et donc 1.

On a ainsi $AMA^{-1} \in H$.

Il en résulte que le sous-groupe H de G est distingué. □

3.2.11 Soient A et B deux (n,n)-matrices à éléments réels, semblables au titre d'éléments de $\mathcal{M}_n(\mathbb{C})$. Sont-elles semblables au titre d'éléments de $\mathcal{M}_n(\mathbb{R})$?

Par hypothèse, il existe $P \in \mathcal{M}_n(\mathbb{C})$ inversible, telle que $PB = AP$.

Soient $\theta \in \mathbb{R}$, et $Q = e^{i\theta}P + e^{-i\theta}\overline{P}$. On écrit :

$$Q = e^{-i\theta}P(P^{-1}\overline{P} + e^{2i\theta}I_n).$$

On peut supposer que $\theta \in \mathbb{R}$ a été choisi de façon que $e^{2i\theta}$ ne soit pas racine du polynôme caractéristique de $-P^{-1}\overline{P}$, et ainsi :

$$\det Q = e^{-ni\theta}.\det P.\det(P^{-1}\overline{P} + e^{2i\theta}I_n) \neq 0.$$

En outre $\overline{Q} = Q$; la matrice Q est donc inversible, à éléments réels.

De $PB = AP$ on déduit : $\overline{P}B = A\overline{P}$, et par combinaisons linéaires :

$$(e^{i\theta}P + e^{-i\theta}\overline{P})B = A(e^{i\theta}P + e^{-i\theta}\overline{P})$$

ce qui s'écrit : $QB = AQ$.

A et B sont donc semblables au titre d'éléments de $\mathcal{M}_n(\mathbb{R})$.

3.2.12 Ici K est un corps commutatif infini ; L est un sur-corps commutatif de K. Soient A et B deux (n,n) matrices à éléments dans K qui sont semblables dans $\mathcal{M}_n(L)$; montrer qu'elles sont semblables dans $\mathcal{M}_n(K)$.

Il s'agit d'une extension de l'exercice précédent.

Soit $\mathcal{E}$ l'ensemble des $M \in \mathcal{M}_n(L)$ vérifiant : $AM = MB$ (1)

Remarquons que, A et B étant semblables dans $\mathcal{M}_n(L)$, $\mathcal{E}$ contient une matrice inversible, et donc non nulle.

En utilisant le calcul des éléments du produit de deux matrices, on constate qu'il existe un système linéaire et homogène (H) de n^2 équations à n^2 inconnues, à coefficients dans K, tel que $M \in \mathcal{M}_n(L)$ est solution de (1) si, et seulement si la famille des coordonnées de M dans la base canonique de $\mathcal{M}_n(L)$ est solution de (H).

Les solutions de (H) constituent un sous-espace vectoriel de L^{n^2}, de dimension $m = n^2 - r$, où r est le rang de (H) ; $\mathcal{E}$ contenant une matrice non nulle, (H) admet des solutions non nulles, et donc $m > 0$.

Pour résoudre (H) on peut procéder de la façon suivante.

- On recherche une matrice principale pour la matrice des coefficients de (H) ; on dispose ainsi de r équations principales, de r inconnues principales et de m inconnues non principales, que l'on note $y_1, \ldots, y_m$.

- Pour tout $k \in \mathbb{N}_m$, on donne, dans les équations principales, la valeur 1 à y_k et la valeur 0 aux autres inconnues non principales. On obtient ainsi un système de Cramer aux inconnues principales, qui fournit une solution M_k de (1). On remarque de M_k est à éléments dans K.

- & est le sous-espace de $\mathcal{M}_n(L)$ dont une base est $(M_1,\ldots,M_m)$.

• Considérons alors le polynôme : $\det\left(\sum_{k=1}^{m} X_k M_k\right) \in L[X_1,\ldots,X_m]$.

Puisqu'il existe dans $\mathcal{M}_n(L)$ une matrice inversible vérifiant (1), on dispose de $(\alpha_1,\ldots,\alpha_m) \in L^m$ tel que : $\det\left(\sum_{k=1}^{m} \alpha_k M_k\right) \neq 0$. Le polynôme considéré n'est donc pas nul. Or il est visiblement à coefficients dans K ; c'est donc un élément non nul de $K[X_1,\ldots,X_m]$.

Comme le corps K est infini, il existe un $(\beta_1,\ldots,\beta_m) \in K^m$ tel que :

$$\det\left(\sum_{k=1}^{m} \beta_k M_k\right) \neq 0.$$

La matrice $\sum_{k=1}^{m} \beta_k M_k$ est dans $\mathcal{M}_n(K)$, vérifie (!) et est inversible, ce qui prouve que A et B sont semblables dans $\mathcal{M}_n(K)$. □

3.2.13 1° Soient $p \in \mathbb{N}^*$ et Δ un endomorphisme de $\mathcal{M}_p(\mathbb{R})$ tel que :

$$\forall (U,V) \in \left(\mathcal{M}_p(\mathbb{R})\right)^2 \quad \Delta(UV) = \Delta(U).V + U.\Delta(V)$$

On suppose que H est un élément de $\mathcal{M}_p(\mathbb{R})$ tel que : $\Delta^2(H) = 0$.

Vérifier :

$$\forall n \in \mathbb{N}^* \quad \Delta^n(H^n) = n!\left(\Delta(H)\right)^n.$$

2° Soient A et H deux éléments de $\mathcal{M}_p(\mathbb{R})$, et $B = AH - HA$. On suppose que A et B commutent. Une norme étant choisie sur $\mathcal{M}_p(\mathbb{R})$, montrer :

$$\lim_{n\to+\infty} \|B^n\|^{1/n} = 0.$$

On dit que Δ est une *dérivation* sur l'algèbre $\mathcal{M}_p(\mathbb{R})$.

1° • En reprenant la démonstration de la formule de Leibniz sur la dérivée n-ième d'un produit, on vérifie par récurrence :

$$\forall n \in \mathbb{N}^* \quad \Delta^n(UV) = \sum_{k=o}^{n} C_n^k \Delta^k(U).\Delta^{n-k}(V)$$

(étant entendu que Δ^o désigne l'identité de $\mathcal{M}_p(\mathbb{R})$).

• Soit $H \in \mathcal{M}_p(\mathbb{R})$ tel que : $\Delta^2(H) = 0$.

a) Montrons par récurrence qu'est vraie pour tout $n \in \mathbb{N}^*$ l'assertion :

$(\mathcal{A}_n)$ $\quad \Delta^{n+1}(H^n) = 0$

- $(\mathcal{A}_1)$, qui s'écrit $\Delta^2(H) = 0$, est vraie par hypothèse.
- Soit $n \in \mathbb{N}^*$ pour lequel on a vérifié $(\mathcal{A}_n)$. On peut écrire :

$$\Delta^{n+2}(H^{n+1}) = \sum_{k=0}^{n+2} C_{n+2}^k \, \Delta^k(H).\Delta^{n+2-k}(H^n)$$
$$= H.\Delta^{n+2}(H^n) + (n+2)\Delta(H).\Delta^{n+1}(H^n)$$

(en effet, on a $\Delta^k(H) = 0$ pour tout $k \geqslant 2$).

Or $(\mathcal{A}_n)$ s'écrit $\Delta^{n+1}(H^n) = 0$ et entraîne $\Delta^{n+2}(H^n) = 0$; $(\mathcal{A}_{n+1})$ est donc vraie. □

b) Montrons par récurrence qu'est vraie pour tout $n \in \mathbb{N}^*$ l'assertion :

$(\mathcal{B}_n)$ $\quad \Delta^n(H^n) = n!\big(\Delta(H)\big)^n$.

- Il est clair que $(\mathcal{B}_1)$ est vraie.
- Soit $n \in \mathbb{N}^*$ pour lequel on a vérifié $(\mathcal{B}_n)$. On peut écrire :

$$\Delta^{n+1}(H^{n+1}) = \sum_{k=0}^{n+1} C_{n+1}^k \, \Delta^k(H).\Delta^{n+1-k}(H^n)$$
$$= H\Delta^{n+1}(H^n) + (n+1)\Delta(H).\Delta^n(H^n).$$

Compte-tenu de $(\mathcal{A}_n)$ et de $(\mathcal{B}_n)$, on en déduit que $(\mathcal{B}_{n+1})$ est vraie. □

2° Ici Δ désigne l'application $M \longmapsto AM-MA$ de $\mathcal{M}_p(\mathbb{R})$ dans lui-même, qui est visiblement linéaire, et vérifie :

$$\Delta(UV) = (AU-UA)V + U(AV-VA)$$
$$= \Delta(U).V + U.\Delta(V)$$

Δ est donc une dérivation sur l'algèbre $\mathcal{M}_p(\mathbb{R})$.

Comme $\Delta(H) = B$ et $\Delta^2(H) = AB-BA = 0$, on peut appliquer le 1° et écrire :

$$\forall n \in \mathbb{N}^* \quad \Delta^n(H^n) = n!\, B^n.$$

Les normes sur l'espace vectoriel $\mathcal{M}_p(\mathbb{R})$, de dimension finie, étant deux à deux équivalentes, on peut choisir une norme canoniquement associée à une norme sur $\mathbb{R}^p$. Comme Δ est continue, on a, pour tout $n \in \mathbb{N}^*$:

$$\|\Delta^n(H^n)\| \leqslant \|\Delta\|^n \, \|H\|^n$$

et donc : $\|B^n\|^{1/n} \leqslant a_n^{1/n} \, \|\Delta\| \, \|H\|$, où $a_n = 1/n!$

D'après une inégalité classique entre moyennes géométriques et arithmétiques, on a : $a_n^{1/n} \leqslant \frac{1}{n}\left(1 + \frac{1}{2} + \ldots + \frac{1}{n}\right)$. On en déduit :

$$\lim_{n \to +\infty} a_n^{1/n} = 0.$$ □

3.3. Déterminants. Equations Linéaires

3.3.1 Trouver les coefficients du polynôme $P_n \in K[X]$ défini par :

$$P_n = \det[\alpha_{ij}],\ (i,j) \in \{0,1,\ldots,n\}^2,$$

où $\alpha_{oj} = X^j$, et $\alpha_{ij} = (j+1)^{i-1}$ si $i \geqslant 1$.

Indication. On vérifiera que P_n est divisible par $(1-X)^n$.

On a $P_o = 1$ et $P_1 = 1-X$. On suppose dans ce qui suit : $n \geqslant 2$.

On ne change pas P_n en remplaçant les α_{io}, $i \in \{0,\ldots,n\}$, par les

$$\beta_{io} = \sum_{j=o}^{n} (-1)^j C_n^j \alpha_{ij}.$$

On a $\beta_{oo} = (1-X)^n$. On va montrer : $\beta_{io} = 0$ pour $i \geqslant 1$.

• Soient u l'endomorphisme $Q(X) \mapsto Q(X+1)$ de $K_{n-1}[X]$, et $v = I-u$ (où I est l'application identique de $K_{n-1}[X]$ dans lui-même). On constate que v transforme tout élément non nul de $K_{n-1}[X]$ en un polynôme de degré strictement inférieur ; on a donc $v^n = 0$, ce qui s'écrit :

$$\sum_{j=o}^{n} (-1)^j C_n^j u^j = 0.$$

Pour tout $Q \in K_{n-1}[X]$, le polynôme $\sum_{j=o}^{n} (-1)^j C_n^j Q(X+j)$ est nul.

On applique à $Q(X) = X^{i-1}$, $i \in \mathbb{N}_n$, et on fait $X = 1$. □

• En développant suivant la nouvelle première colonne, on obtient :

$$P_n = k_n(1-X)^n,\ n \geqslant 2,$$

où k_n est le déterminant de Vandermonde associé à $(2,3,\ldots,n+1)$, i.e.

$$k_n = (n-1)!(n-2)!\ \ldots 1!$$

3.3.2 Soit $n \in \mathbb{N}^*$. Pour tout $(i,j) \in \mathbb{N}_n^2$, on note α_{ij} le PGCD de i et j. Montrer que le déterminant de la (n,n)-matrice $A = [\alpha_{ij}]$ s'écrit :

$$\det A = \prod_{k=1}^{n} \varphi(k),$$ où φ est l'indicateur d'Euler (cf. 1.1.7).

A tout $(i,j) \in \mathbb{N}_n^2$, associons les deux entiers :

$$\begin{cases} m_{ij} = 1 \text{ si } i \text{ divise } j\ ;\ m_{ij} = 0 \text{ sinon} \\ n_{ij} = \varphi(j) \text{ si } j \text{ divise } i\ ;\ n_{ij} = 0 \text{ sinon.} \end{cases}$$

Nous disposons des (n,n)-matrices $M = [m_{ij}]$ et $N = [n_{ij}]$. Nous avons :

$$NM = [\beta_{ij}],\ \text{avec } \beta_{ij} = \sum_{k=1}^{n} n_{ik} m_{kj}.$$

- Donnons-nous $(i,j) \in \mathbb{N}_n^2$. Dans l'expression de β_{ij}, il suffit de considérer les indices k qui divisent à la fois i et j, i.e. les indices k qui divisent α_{ij} ; pour l'un de ces indices : $n_{ik}m_{kj} = \varphi(k)$; on a ainsi :

$$\beta_{ij} = \sum_{k \in \mathcal{T}_{ij}} \varphi(k), \text{ où } \mathcal{T}_{ij} \text{ est l'ensemble des diviseurs de } \alpha_{ij}.$$

et donc : $\beta_{ij} = \alpha_{ij}$, (cf. exercice 1.1.7 2°).

- D'où : NM = A, et det A = det N.det M.

Comme N et M sont triangulaires, on calcule aisément :

$$\det N = \varphi(1)\ldots\varphi(n) \; ; \; \det M = 1. \qquad \square$$

3.3.3 Soient $k \in \mathbb{N}^*$, $(n_1,\ldots,n_k) \in \mathbb{N}^k$ avec $n_1 < n_2 < \ldots < n_k$, et $(a_1,\ldots,a_k) \in (\mathbb{R}_+^*)^k$ avec $a_1 < a_2 < \ldots < a_k$.

On note D_k le déterminant de la matrice $A_k \in \mathcal{M}_k(\mathbb{R})$ dans laquelle l'élément (i,j) est $a_i^{n_j}$. Vérifier : $D_k > 0$.

Indication. On pourra commencer par montrer que $D_k \neq 0$.

Notons que l'étude du déterminant de Vandermonde fournit le résultat dans un cas particulier.

a) Commençons par montrer par l'absurde que $D_k \neq 0$.

Pour cela, faisons l'hypothèse (H) : $D_k = 0$. En considérant D_k comme le déterminant d'un système linéaire et homogène de k équations à k inconnues, on constate qu'il existe $(\alpha_1,\ldots,\alpha_k) \in \mathbb{R}^k$, non nul, tel que :

$$\forall i \in \mathbb{N}_k \quad \sum_{j=1}^{k} a_i^{n_j} \alpha_j = 0.$$

On dispose du polynôme non nul $P = \alpha_1 X^{n_1} + \ldots + \alpha_k X^{n_k}$, et celui-ci admet les k racines strictement positives (et distinctes) $a_1,\ldots,a_k$.

En factorisant X autant de fois que c'est possible dans P, on a :

$$P = X^r(\beta_0 + \ldots + \beta_s X^s), \text{ avec } \beta_0\beta_s \neq 0.$$

La famille $(\beta_0,\ldots,\beta_s)$ ayant au plus k éléments non nuls, elle présente au plus k-1 changements de signe. En utilisant l'exercice 2.1.17, on en déduit que P admet au plus k-1 racines strictement positives. L'hypothèse (H) conduit donc à une contradiction. $\square$

b) Nous allons maintenant vérifier par récurrence qu'une assertion $(\mathcal{T}_k)$ est vraie pour tout $k \in \mathbb{N}^*$.

- Il est clair que $(\mathcal{T}_1)$ est vraie.

- Soit $k \geqslant 2$, pour lequel $(\mathcal{T}_{k-1})$ a été vérifiée. Considérons $(n_1,\ldots,n_k) \in \mathbb{N}^k$ et $(a_1,\ldots,a_k) \in (\mathbb{R}_+^*)^k$ vérifiant les conditions de l'énoncé, et introduisons le polynôme ;

$$Q = \det \begin{bmatrix} \begin{bmatrix} & & \\ & A_{k-1} & \\ & & \end{bmatrix} & \begin{matrix} a_1^{n_k} \\ \\ a_{k-1}^{n_k} \end{matrix} \\ X^{n_1} \quad \dots & X^{n_k} \end{bmatrix}$$

Q a pour degré n_k et pour coefficient dominant $D_{k-1}X^{n_k}$, avec $D_{k-1} > 0$ d'après l'hypothèse de récurrence.

Pour tout réel $x > a_{k-1}$, $Q(x)$ peut être considéré comme le déterminant déduit de D_k en remplaçant a_k par x, et compte-tenu de :

$$a_1 < \dots < a_{k-1} < x$$

on a (cf 1°) : $Q(x) \neq 0$.

La restriction à $]a_{k-1}, +\infty[$ de la fonction associée au polynôme Q ne prend donc pas la valeur 0, et compte-tenu de $\lim_{x \to +\infty} P(x) = +\infty$, elle ne prend que des valeurs strictement positives. En particulier $D_k > 0$. $(\mathcal{T}_k)$ est donc vraie. □

3.3.4 Soient $n \geqslant 2$ et $A = [\alpha_{ij}] \in \mathcal{M}_n(K)$, non inversible ; on note A_{ij} le cofacteur de α_{ij} dans A. Vérifier :

$$\forall (i,j,k,\ell) \in (\mathbb{N}_n)^4 \quad A_{ij}A_{k\ell} = A_{kj}\,A_{i\ell}$$

• Si le rang de A n'excède pas n-2; la proposition est triviale (les A_{ij} étant alors tous nuls).

• Le cas rg A = n ne se posant pas (à cause de det A = 0), reste à étudier le cas rg A = n-1, dans lequel nous nous plaçons.

A étant identifié à un endomorphisme de K^n rapporté à sa base canonique, nous disposons de Ker A, qui est défini par :

$$\operatorname{Ker} A = \left\{ (\xi_1, \dots, \xi_n) \in K^n \mid \forall i \in \mathbb{N}_n \sum_{j=1}^{n} \alpha_{ij}\xi_j = 0 \right\}$$

et Ker A est un sous-espace de K^n de dimension 1.

Or, pour tout $(i,k) \in \mathbb{N}_n^2$ on a : $\sum_{j=1}^{n} \alpha_{ij}\, A_{kj} = 0$.

En effet $\sum_{j=1}^{n} \alpha_{ij}\, A_{kj}$ est un développement de det A si k = i, d'un déterminant dont deux lignes sont égales si $k \neq i$.

Il en résulte que, pour tout $k \in \mathbb{N}_n$, on a $(A_{k1}, \dots, A_{kn}) \in \operatorname{Ker} A$.

Pour tout $(i,k) \in \mathbb{N}_n^2$, $(A_{i1}, \dots, A_{in})$ et $(A_{k1}, \dots, A_{kn})$ sont donc des éléments colinéaires de K^n. □

3.3.5 Soient A,B,C,D quatre K-matrices carrées d'ordre $n \in \mathbb{N}^*$. On leur associe la K-matrice carrée d'ordre 2n :

$$M = \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right]$$

1° On suppose que C et D commutent. Vérifier :

$$\det M = \det(AD-BC). \qquad (1)$$

Indication : On étudiera d'abord le cas où D est inversible.

2° Que se passe-t-il si ce sont B et D (et non C et D) qui commutent ?

1° a) Ici D est inversible. Nous aurons à utiliser des matrices de la forme :

$$N = \left[\begin{array}{c|c} X & Y \\ \hline Z & T \end{array}\right]$$

où X,Y,Z,T sont des K-matrices carrées d'ordre n.

Rappelons que, pour une matrice de cette forme, si $Y=0$ ou si $Z=0$, alors : $\det N = \det X . \det T$.

- En multipliant à droite M par une matrice N, on a :

$$MN = \left[\begin{array}{c|c} AX+BZ & AY+BT \\ \hline CX+DZ & CY+DT \end{array}\right]$$

ce qui se simplifie si l'on adopte $X = D$, $Y = 0$, $Z = -C$, $T = D^{-1}$.

Compte-tenu de $CD = DC$, on a alors :

$$N = \left[\begin{array}{c|c} D & 0 \\ \hline -C & D^{-1} \end{array}\right] \quad \text{et} \quad NM = \left[\begin{array}{c|c} AD-BC & BD^{-1} \\ \hline 0 & I_n \end{array}\right]$$

D'où : $\det N = 1$, et $\det M = \det(AD-BC)$. □

Remarque. (1) peut être en défaut si C et D ne commutent pas. C'est ainsi que si :

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \; B = I_2, \; C = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \; D = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

on a : $\det M = 0$ et $\det (AD-BC) = \det \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = 1$.

b) Ici D n'est pas inversible. On peut supposer le corps K infini (quitte à le plonger dans l'un de ses sur-corps infini, par exemple le corps des fractions rationnelles de K).

On dispose des deux polynômes (éléments de $K[X]$) :

$$P = \det M(X) \; ; \; Q = \det \left(A(D-XI_n) - BC\right).$$

où :

$$M(X) = \left[\begin{array}{c|c} A & B \\ \hline C & D-XI_n \end{array}\right].$$

Comme C et $D-tI_n$ commutent pour tout $t \in K$, 1° montre que P et Q prennent la même valeur en tout point de K qui n'est pas valeur propre de D, et donc en une infinité de points de K. Il en résulte que P = Q, et qu'en particulier P(0) = Q(0), ce qui s'écrit (1). □

2° Nous utiliserons :

$$\det M = \det {}^tM = \det \left[\begin{array}{c|c} {}^tA & {}^tC \\ \hline {}^tB & {}^tD \end{array}\right].$$

La commutativité de B et D entraînant celle de ${}^tB$ et ${}^tD$, le 1° donne :

$$\det M = \det({}^tA{}^tD - {}^tC{}^tB) = \det {}^t({}^tA{}^tD - {}^tC{}^tB)$$

et : $$\det M = \det(DA-BC).$$

3.3.6 Soient A et B deux K-matrices (n,n) vérifiant :
i) A et B commutent ; ii) B est nilpotente.
Prouver : $\det(A+B) = \det A$ (1)

• Préambule. Nous allons prouver : $\det(I_n+B) = 1$.

B étant nilpotente, nous disposons d'une matrice B' semblable à B, triangulaire supérieure à diagonale de zéros (cf. 4.3.1).

On a : $B' = P^{-1}BP$, $P \in GL_n(K)$. Or : $I_n = P^{-1}I_nP$.

D'où : $I_n + B' = P^{-1}(I_n+B)P$, et :
$\det(I_n+B) = \det(I_n+B') = 1$. □

a) Preuve de (1) lorsque A est inversible. Ecrivons :

$$A + B = A(I_n+A^{-1}B).$$

Comme A et B, A^{-1} et B commutent. On en déduit que, puisque B est nilpotente, alors $A^{-1}B$ est nilpotente $\left[(A^{-1}B)^k = A^{-k}B^k\right]$. D'où :

$$\det(A+B) = \det A.\det(I_n+A^{-1}B) = \det A.$$ □

b) Preuve de (1) lorsque A est non inversible. Ici $\det A = 0$.

On sait qu'il existe $k \in \mathbb{N}^*$ tel que $B^k = 0$. Puisque A et B commutent on peut écrire, par la formule du binôme :

$$(A+B)^k = AM, \text{ où } M = \sum_{\ell=0}^{k-1} C_k^{\ell} A^{k-\ell-1}B^{\ell}$$

D'où : $\big(\det(A+B)\big)^k = \det A.\det M = 0.$

Tous deux nuls, det(A+B) et det A sont égaux. □

Autre solution de b). On peut se ramener au cas où le corps K est infini et prouver l'égalité des éléments $\det(A-XI_n+B)$ et $\det(A-XI_n)$ de $K[X]$. (cf. exercice précédent).

Remarque. On ne peut se passer de l'hypothèse i). Contre exemple :

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} ; B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} ; \det(A+B) = 0 \text{ et } \det A = 1.$$

3.3.7 1° Soit $A = [\alpha_{ij}]$ une (n,n) matrice réelle ou complexe telle que :

$$\forall i \in \mathbf{N}_n \quad |\alpha_{ii}| > \sum_{j \neq i} |\alpha_{ij}| \qquad (1)$$

Montrer que A est inversible (théorème d'Hadamard).

2° Soit $A = [\alpha_{ij}]$ une (n,n) matrice réelle telle que :

$\alpha_{ij} \leqslant 0$ pour $i \neq j$, et $\sum_{j=1}^{n} \alpha_{ij} > 0$ pour tout i.

Montrer que A est inversible.

1° Faisons l'hypothèse : A n'est pas inversible. Le système :

$$\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0, \quad 1 \leqslant i \leqslant n,$$

n'est pas cramérien : il admet une solution non nulle $(\xi_1,\ldots,\xi_n)$. On constate qu'il existe $k \in \mathbf{N}_n$ tel que $\xi_k \neq 0$ et $|\xi_j| \leqslant |\xi_k|$ pour tout $j \in \mathbf{N}_n$.

On a d'une part :

$$|\alpha_{kk}\xi_k| > |\xi_k| \sum_{j \neq k} |\alpha_{kj}|.$$

D'après $\alpha_{kk}\xi_k = - \sum_{j \neq k} \alpha_{kj}\xi_j$, on a d'autre part :

$$|\alpha_{kk}\xi_k| \leqslant \sum_{j \neq k} |\alpha_{kj}||\xi_j| \leqslant |\xi_k| \sum_{j \neq k} |\alpha_{kj}|$$

On aboutit donc à une contradiction. □

2° Pour tout $i \in \mathbf{N}_n$, on a :

$$\alpha_{ii} > - \sum_{j \neq i} \alpha_{ij} = \sum_{j \neq i} |\alpha_{ij}|$$

ce qui montre que la condition (1) est remplie. □

3.3.8 Soit $(\alpha,\beta,\gamma_1,\ldots,\gamma_n) \in K^{n+2}$. Calculer :

$$D = \det[a_{ij}], \quad (i,j) \in \{1,\ldots,n\}^2$$

où $a_{ii} = \gamma_i$; $a_{ij} = \alpha$ si $j > i$; $a_{ij} = \beta$ si $j < i$.

On considère $\Delta(X) \in K[X]$, défini par $\Delta(X) = \det[a_{ij}+X]$.

En retranchant la première colonne de toutes les autres, et en développant suivant la première colonne, on constate : deg $\Delta(X) \leqslant 1$, i.e. $\Delta(X) = kX + D$.

D'autre part $\Delta(-\alpha)$ et $\Delta(-\beta)$ sont les déterminants de matrices triangulaires, à savoir $\Delta(-\alpha) = P(\alpha)$ et $\Delta(-\beta) = P(\beta)$, avec :

$$P(X) = \prod_{i=1}^{n} (\gamma_i - X).$$

1er Cas : $\alpha \neq \beta$. En utilisant $\Delta(-\alpha) = -k\alpha + D$ et $\Delta(-\beta) = -k\beta + D$, on obtient :

$$D = \frac{\beta P(\alpha) - \alpha P(\beta)}{\beta - \alpha}.$$

2ème Cas : $\alpha = \beta$. En scindant chaque vecteur colonne de $[a_{ij}+X]$, $\Delta(X)$ apparaît comme la somme de 2^n déterminants. En supprimant ceux d'entre eux dont deux colonnes au moins sont formées de X, on obtient :

$$\Delta(X) = kX + D, \text{ avec } k = \sum_{j=1}^{n} D_j ;$$

où D_j est le déterminant obtenu à partir de D en remplaçant tous les éléments de la j-ième colonne par des 1 ; dans D_j, on retranche la j-ième ligne de toutes les autres, puis on développe suivant la j-ième colonne, ce qui fournit :

$$D_j = \prod_{i \neq j} (\gamma_i - \alpha)$$

En reprenant $D = P(\alpha) + k\alpha$, il vient :

$$D = \prod_{i=1}^{n} (\gamma_i - \alpha) + \alpha \sum_{j=1}^{n} \left(\prod_{i \neq j} (\gamma_i - \alpha) \right)$$

et : $$D = P(\alpha) - \alpha P'(\alpha).$$

3.3.9 Soient $(\alpha, \gamma_1, \ldots, \gamma_n) \in K^{n+1}$ et $A = [a_{ij}]$, $(i,j) \in \{1, \ldots, n\}^2$, avec :
$a_{ii} = \gamma_i$; $a_{ij} = \alpha$ si $i \neq j$.
Calculer la matrice A^{-1} lorsqu'elle est définie.

1° Si $\alpha = 0$, $A = \mathrm{diag}(\gamma_1, \ldots, \gamma_n)$ est inversible si, et seulement si aucun des γ_i n'est nul, et alors : $A^{-1} = \mathrm{diag}(\gamma_1^{-1}, \ldots, \gamma_n^{-1})$.

2° Dans la suite, on suppose $\alpha \neq 0$ et on écrit :

$$\alpha^{-1}A = J + \mathrm{diag}(\gamma_1' - 1, \ldots, \gamma_n' - 1), \ \gamma_i' = \alpha^{-1}\gamma_i,$$

où J est la (n,n)-matrice à éléments tous égaux à 1, ce qui ramène à étudier la possibilité d'inverser la matrice :

$$B = J + \mathrm{diag}(\beta_1, \ldots, \beta_n), \ \beta_i = \gamma_i' - 1.$$

Il s'agit donc de trouver à quelle condition, portant sur $(\beta_1, \ldots, \beta_n)$, le système de n équations linéaires :

$$x_1 + \ldots + x_n + \beta_i x_i = y_i, \quad 1 \leqslant i \leqslant n \qquad (L_y)$$

admet une solution unique pour tout $y = (y_1, \ldots, y_n) \in K^n$, et, le cas échéant, de calculer cette solution unique.

1er Cas : Deux des β_i sont nuls. Soit $\beta_p = \beta_q = 0$, avec $1 \leqslant p < q \leqslant n$. En considérant les p-ième et q-ième équations, on constate (par différence) que L_y n'a pas de solution pour un y tel que $y_p \neq y_q$; B n'est pas inversible.

2ème Cas : Un et un seul des β_i est nul. Soit par exemple :

$$\beta_1 = 0 \ ; \ \beta_2 \ldots \beta_n \neq 0.$$

On note : $\lambda_i = \beta_i^{-1}$ pour $2 \leqslant i \leqslant n$, et $1 + \lambda_2 + \ldots + \lambda_n = \lambda$.

On constate que, pour tout $y \in K^n$, L_y admet la solution unique :

$$x_i = \lambda_i (y_i - y_1) \text{ pour } 2 \leqslant i \leqslant n \ ; \ x_1 = \lambda y_1 - \sum_{j=2}^{n} \lambda_j y_j$$

ce qui montre que B est inversible et que :

$$B^{-1} = \operatorname{diag}(\lambda, \lambda_2, \ldots, \lambda_n) - \begin{bmatrix} 0 & \lambda_2 & \ldots & \lambda_n \\ \lambda_2 & & & \\ \vdots & & O & \\ \lambda_n & & & \end{bmatrix}$$

3ème Cas : Aucun des β_i n'est nul. On note :

$$\mu_i = \beta_i^{-1} \text{ pour } 1 \leqslant i \leqslant n, \text{ et } 1 + \mu_1 + \mu_2 + \ldots + \mu_n = \mu.$$

On écrit L_y sous la forme :

$$\begin{cases} x_i = \mu_i \left(y_i - y_1 + \dfrac{x_1}{\mu_1} \right), \ 2 \leqslant i \leqslant n \\ \dfrac{\mu}{\mu_1} x_1 = \mu y_1 - \mu_1 y_1 - \mu_2 y_2 - \ldots - \mu_n y_n \end{cases}$$

- Si $\mu = 0$, alors, pour $y = 0$, L_y admet une infinité de solutions ; B n'est pas inversible.

- Si $\mu \neq 0$, alors, pour tout y, L_y admet une solution unique ; B est inversible, et on constate que :

$$B^{-1} = \operatorname{diag}(\mu_1, \ldots, \mu_n) - \frac{1}{\mu} [b_{ij}], \text{ où } b_{ij} = \mu_i \mu_j.$$

Remarque. Nous n'avons pas eu recours aux déterminants. En utilisant 3.3.8 nous aurions pu constater a priori que B^{-1} existe si, et seulement si $\det B \neq 0$, où $\det B = \beta_1 \ldots \beta_n + \sum_{j=1}^{n} \left(\prod_{i \neq j} \beta_j \right)$.

3.3.10 Soient $(\alpha_i)_{1 \leqslant i \leqslant n}$ et $(\beta_j)_{1 \leqslant j \leqslant n}$ deux familles d'éléments de K telles que $\alpha_i + \beta_j \neq 0$ pour tout $(i,j) \in \{1, \ldots, n\}^2$.

Calculer : $D_n = \det [a_{ij}]$, où $a_{ij} = \dfrac{1}{\alpha_i + \beta_j}$.

On a $D_1 = (\alpha_1+\beta_1)^{-1}$. Soit $n \geqslant 2$. On retranche la dernière colonne de D_n de toutes les autres ; on factorise ensuite $(\alpha_i+\beta_n)^{-1}$ dans les éléments de la i-ième ligne, $1 \leqslant i \leqslant n$, et $\beta_n - \beta_j$ dans ceux de la j-ième colonne, $1 \leqslant j \leqslant n-1$; on obtient ainsi :

$$D_n = \frac{\prod_{j=1}^{n-1} (\beta_n-\beta_j)}{\prod_{i=1}^{n} (\alpha_i+\beta_n)} \Delta_n$$

où Δ_n se déduit de D_n en remplaçant les éléments de la dernière colonne par des 1. Dans Δ_n on retranche la dernière ligne de toutes les autres ; on factorise ensuite $\alpha_n-\alpha_i$ dans les éléments de la i-ième ligne, $1 \leqslant i \leqslant n-1$, et $(\alpha_n+\beta_j)^{-1}$ dans ceux de la j-ième colonne, $1 \leqslant j \leqslant n-1$; en développant suivant la dernière colonne, on obtient :

$$\Delta_n = \frac{\prod_{i=1}^{n-1} (\alpha_n-\alpha_i)}{\prod_{j=1}^{n-1} (\alpha_n+\beta_j)} D_{n-1}.$$

D'où :
$$D_n = \frac{\prod_{k=1}^{n-1} (\alpha_n-\alpha_k)(\beta_n-\beta_k)}{\prod_{k=1}^{n} (\alpha_k+\beta_n) \cdot \prod_{k=1}^{n-1} (\alpha_n+\beta_k)} D_{n-1}, \quad n \geqslant 2.$$

En raisonnant par récurrence, on en déduit :

$$D_n = \frac{\prod_{1 \leqslant k < \ell \leqslant n} (\alpha_\ell-\alpha_k)(\beta_\ell-\beta_k)}{\prod_{(k,\ell) \in \{1,\ldots,n\}^2} (\alpha_k+\beta_\ell)}.$$

On notera que le numérateur de D_n est le produit des déterminants de Vandermonde des familles $(\alpha_1,\ldots,\alpha_n)$ et $(\beta_1,\ldots,\beta_n)$; on a donc $D_n \neq 0$ si, et seulement si chacune de ces familles est composée d'éléments deux à deux distincts.

3.3.11 Soient $(\alpha_i)_{1 \leqslant i \leqslant n}$ et $(\beta_j)_{1 \leqslant j \leqslant n}$ deux familles d'éléments deux à deux distincts de K telles que $\alpha_i+\beta_j \neq 0$ pour tout $(i,j) \in (\mathbb{N}_n)^2$. Soit en outre $\gamma \in K$ tel que $\alpha_i+\gamma \neq 0$ pour tout $i \in \mathbb{N}_n$.

Résoudre et discuter sur K le système :

$$\frac{x_1}{\alpha_i+\beta_1} + \ldots + \frac{x_n}{\alpha_i+\beta_n} = \frac{1}{\alpha_i+\gamma}, \quad 1 \leqslant i \leqslant n \qquad (1)$$

Il s'agit d'un système de n équations linéaires à n inconnues. D'après l'expression de $\det\left[\frac{1}{\alpha_i+\beta_j}\right]$ trouvée au n°3.3.10 c'est un système de Cramer ;

(1) admet donc une solution unique.

• Nous allons retrouver ce résultat et calculer la solution en associant à tout $\xi = (\xi_1,\ldots,\xi_n) \in K^n$ la fraction rationnelle :

$$F_\xi = \frac{\xi_1}{X+\beta_1} + \ldots + \frac{\xi_n}{X+\beta_n} - \frac{1}{X+\gamma} \tag{2}$$

1er Cas : γ n'est égal à aucun des β_j ; F_ξ admet les n+1 pôles, tous simples, $-\beta_1,\ldots,-\beta_n, -\gamma$. Nous avons :

$$F_\xi = \frac{P_\xi}{(X+\beta_1)\ldots(X+\beta_n)(X+\gamma)}, \text{ où } P_\xi = (\xi_1+\ldots+\xi_n-1)X^n + \ldots$$

Il s'agit de trouver ξ tel que $P_\xi(\alpha_1) = \ldots = P_\xi(\alpha_n) = 0$, i.e. pour que P_ξ soit divisible par $X-\alpha_1$, $X-\alpha_2,\ldots,X-\alpha_n$, et donc pour que :

$$F_\xi = \frac{(\xi_1+\ldots+\xi_n-1)(X-\alpha_1)\ldots(X-\alpha_n)}{(X+\beta_1)\ldots(X+\beta_n)(X+\gamma)} .$$

En calculant la décomposition en éléments simples de cette dernière fraction rationnelle et en l'identifiant à (2), la condition s'écrit :

$$-1 = \frac{(\xi_1+\ldots+\xi_n-1)\prod_k(-\gamma-\alpha_k)}{\prod_k(-\gamma+\beta_k)} \tag{3}$$

et :
$$\xi_j = \frac{(\xi_1+\ldots+\xi_n-1)\prod_k(-\beta_j-\alpha_k)}{(-\beta_j+\gamma)\cdot\prod_{k\neq j}(-\beta_j+\beta_k)}, \quad 1\leqslant j\leqslant n \tag{4}$$

(Dans $\prod_k$, k décrit $\mathbb{N}_n$; dans $\prod_{k\neq j}$, k décrit $\mathbb{N}_n\setminus\{j\}$).

Par division, et compte tenu de $\xi_1+\ldots+\xi_n-1\neq 0$ (à cause de (3)), on obtient la solution unique $(\xi_1,\ldots,\xi_n)$ avec :

$$\forall j\in\mathbb{N}_n \quad \xi_j = \prod_k \frac{\beta_j+\alpha_k}{\gamma+\alpha_k}\cdot\prod_{k\neq j}\frac{\gamma-\beta_k}{\beta_j-\beta_k} \tag{5}$$

2ème Cas : $\gamma = \beta_\ell$, $\ell\in\mathbb{N}_n$. On a en évidence la solution :

$$\xi_\ell = 1 \ ; \ \xi_j = 0 \text{ pour tout } j\in\mathbb{N}_n\setminus\{\ell\}. \tag{6}$$

Cette solution est unique. En effet, ici :

$$F_\xi = \frac{\xi_\ell-1}{X+\beta_\ell} + \sum_{j\neq\ell}\frac{\xi_j}{X+\beta_j} = \frac{Q_\xi}{\prod_j(X+\beta_j)} , \ \deg Q_\xi < n$$

et pour que Q_ξ soit divisible par $X-\alpha_1,\ldots,X-\alpha_n$, il faut et il suffit que Q_ξ soit nul, i.e. que la fraction F_ξ soit nulle.

Remarque. Limitons nous à $K=\mathbb{C}$ ou $K=\mathbb{R}$. Les familles (α_i) et (β_j) étant fixées, notons $\varphi(\gamma)$ la solution du système (1) associé à $\gamma\in K\setminus\{-\alpha_1,\ldots,-\alpha_n\}$;

nous définissons ainsi une application φ qui, d'après (5) et (6) vérifie :

$$\forall \ell \in \mathbb{N}_n \quad \lim_{\gamma \to \beta_\ell} \varphi(\gamma) = \varphi(\beta_\ell).$$

L'application φ est donc continue.

3.3.12 Résoudre et discuter sur $\mathbb{R}$ le système :

$$\sum_{j=1}^{n} |\alpha_j - \alpha_i| x_j = 1, \quad 1 \leqslant i \leqslant n \tag{1}$$

dans lequel $(\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$ est un paramètre.

Il s'agit d'un système de n équations linéaires à n inconnues.

Il est évident que si $\alpha_1 = \ldots = \alpha_n$, alors (1) n'a pas de solution. Nous pouvons donc supposer que $\alpha_1, \ldots, \alpha_n$ ne sont pas tous égaux et, quitte à modifier la notation, que :

$$\alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_n \quad \text{et} \quad \alpha_1 < \alpha_n.$$

Par combinaisons linéaires (1) s'écrit :

$$\begin{cases} \sum_{j=1}^{n} (\alpha_j - \alpha_1) x_j = 1 \\ (\alpha_i - \alpha_{i-1})(x_1 + \ldots + x_{i-1} - x_i - \ldots - x_n) = 0, \quad 2 \leqslant i \leqslant n \end{cases}$$

1er Cas. *Les α_i sont deux à deux distincts.* Les $\alpha_i - \alpha_{i-1}$, $2 \leqslant i \leqslant n$, sont non nuls et, par nouvelles combinaisons linéaires, (1) s'écrit :

$$\begin{cases} \sum_{j=1}^{n} (\alpha_j - \alpha_1) x_j = 1 \\ (x_2 = \ldots = x_{n-1} = 0) \wedge (x_1 + \ldots + x_{n-1} - x_n = 0). \end{cases}$$

Il s'agit d'un système de Cramer qui admet la solution unique :

$$\left(\frac{1}{\alpha_n - \alpha_1}, 0, \ldots, \frac{1}{\alpha_n - \alpha_1} \right).$$

2ème Cas. *Les α_i ne sont pas deux à deux distincts.* Il existe des α_i consécutifs égaux. Soit $\alpha_k = \alpha_{k+1} = \ldots = \alpha_{k+p}$, $p \geqslant 1$. Dans (1) on peut supprimer les (k+1)-ième,...,(k+p)-ième équations et prendre pour inconnue auxiliaire $x_k + x_{k+1} + \ldots + x_{k+p}$, ce qui ramène à résoudre un système de la même forme que (1) dans lequel il y a n-p équations, n-p inconnues, le paramètre étant $(\alpha_1, \ldots, \alpha_k, \alpha_{k+p+1}, \ldots, \alpha_n) \in \mathbb{R}^{n-p}$. De proche en proche, on se ramène à un système de Cramer.

Exemple : $n = 6$; $\alpha_1 = \alpha_2 = \alpha_3 < \alpha_4 = \alpha_5 < \alpha_6$.

Le système (1) s'écrit ici :

$$\begin{cases} (\alpha_4-\alpha_1)(x_4+x_5) + (\alpha_6-\alpha_1)x_6 = 1 \\ (\alpha_4-\alpha_1)(x_1+x_2+x_3) + (\alpha_6-\alpha_4)x_6 = 1 \\ (\alpha_6-\alpha_1)(x_1+x_2+x_3) + (\alpha_6-\alpha_4)(x_4+x_5) = 1 \end{cases}$$

et encore, d'après l'étude du 1er cas :

$$\left(x_1+x_2+x_3 = x_6 = \frac{1}{\alpha_6-\alpha_1}\right) \wedge (x_4+x_5 = 0).$$

Les solutions de (1) sont donc les :

$$\left(\lambda, \mu, \frac{1}{\alpha_6-\alpha_1} - \lambda - \mu, \nu, -\nu, \frac{1}{\alpha_6-\alpha_1}\right), \ (\lambda,\mu,\nu) \in \mathbb{R}^3.$$

3.3.13 Dans $K = \mathbb{Z} / 13\,\mathbb{Z}$, résoudre le système :

$$(S) \begin{cases} \dot{6}x + \dot{2}y = \dot{1} \\ \dot{7}x + \dot{3}y = \dot{8} \end{cases}$$

Puisque 13 est premier, K est un corps commutatif ; la théorie des équations linéaires s'applique. On calcule le déterminant :

$$\begin{vmatrix} \dot{6} & \dot{2} \\ \dot{7} & \dot{3} \end{vmatrix} = \dot{4} \neq \dot{0}$$

(S) est cramérien. On calcule les déterminants :

$$\begin{vmatrix} \dot{1} & \dot{2} \\ \dot{8} & \dot{3} \end{vmatrix} = \dot{0} \ ; \ \begin{vmatrix} \dot{6} & \dot{1} \\ \dot{7} & \dot{8} \end{vmatrix} = \dot{2}$$

La solution, unique, de (S) est donnée par :

$$(x = \dot{0}) \wedge (\dot{4}y = \dot{2}), \text{ i.e. } (x,y) = (\dot{0},\dot{7}).$$

4. REDUCTION DES ENDOMORPHISMES

4.1. ELÉMENTS PROPRES

4.1.1 Soient u,v et w trois endomorphismes d'un $\mathbb{C}$-espace vectoriel E de dimension finie $n>0$, tels que :

$$w \neq 0 \quad \text{et} \quad uw = wv.$$

Montrer que u et v ont une valeur propre commune.

Nous donnerons exceptionnellement trois solutions de cet exercice.

Première solution. Le corps de base étant $\mathbb{C}$, v est trigonalisable : il existe une base $(e_1,\dots,e_n)$ de E telle que :

$$\forall j \in \mathbb{N}_n \quad v(e_j) = \alpha_{1j}e_1 + \dots + \alpha_{j-1,j}e_{j-1} + \alpha_{jj}e_j.$$

D'après $w \neq 0$, il existe $k \in \mathbb{N}_n$ tel que $w(e_k) \neq 0$ et $w(e_j) = 0$ pour $j < k$.

En écrivant : $u(w(e_k)) = w(v(e_k))$, on obtient :

$$u(w(e_k)) = \alpha_{kk}w(e_k).$$

Comme $w(e_k) \neq 0$, on en déduit que α_{kk} est valeur propre de u ; or il est clair que α_{kk} est valeur propre de v. □

Deuxième solution. Faisons l'hypothèse : u et v n'ont aucune valeur propre commune.

- Soit $\lambda \in \mathbb{C}$. On a : $(u-\lambda I)w = w(v-\lambda I)$, où $I = Id_E$, et, par une récurrence :

$$\forall p \in \mathbb{N} \quad (u-\lambda I)^p w = w(v-\lambda I)^p.$$

- Si λ est valeur propre de v, et n'est donc pas valeur propre de u, $u-\lambda I$ est injectif, et il en est de même pour $(u-\lambda I)^p$.

Pour $x \in \mathrm{Ker}(v-\lambda I)^p$, on a : $(u-\lambda I)^p(w(x)) = 0$, et donc $w(x) = 0$.

- Pour toute valeur propre λ de v, et pour tout $p \in \mathbb{N}$, Ker w contient ainsi

$\mathrm{Ker}(v-\lambda I)^p$; Ker w contient donc tous les sous-espaces spectraux de v; il contient donc leur somme E ; on a ainsi Ker w = E, et w = 0.

- Notre hypothèse conduit à une contradiction. □

Troisième solution. Il existe deux bases e et f de E telles que :

$$\mathrm{Mat}(w;e,f) = J = \mathrm{diag}(1,\ldots,1,0,\ldots,0)$$

et d'après $w \neq 0$, le rang r commun à w et à J vérifie $1 \leqslant r \leqslant n$.

Notons : A = Mat(u;f) et B = Mat(v;e) ; uw = wv s'écrit AJ = JB, et, chaque matrice étant décomposée en blocs :

$$\left[\begin{array}{c|c} A_1 & A_2 \\ \hline A_3 & A_4 \end{array}\right] \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] \left[\begin{array}{c|c} B_1 & B_2 \\ \hline B_3 & B_4 \end{array}\right]$$

ce qui se traduit par l'égalité des éléments A_1 et B_1 de $\mathcal{M}_r(\mathbb{C})$, et par la nullité de $A_3 \in \mathcal{M}_{n-r,r}(\mathbb{C})$ et de $B_2 \in \mathcal{M}_{r,n-r}(\mathbb{C})$.

Les polynômes caractéristiques de u et v sont ainsi :

$$\chi_u = \chi_A = \chi_{A_1} \cdot \chi_{A_4} \quad \text{et} \quad \chi_v = \chi_B = \chi_{B_1} \cdot \chi_{B_4}.$$

Ils ont en commun les racines du polynôme χ_{A_1}, de degré $r \geqslant 1$, et donc au moins une racine puisque le corps de base est $\mathbb{C}$. □

Remarque. Cette solution nous en apprend plus que les deux premières : le degré du PGCD de χ_u et χ_v est au moins égal au rang de w. En particulier si w est bijective (r = n), alors $\chi_u = \chi_v$ (ce qui résulte du fait que, dans toute base de E, u et v sont alors représentés par des matrices semblables).

4.1.2 Ici $K = \mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier. Montrer :

$$\forall M \in \mathcal{M}_n(K) \quad \mathrm{tr}\, M^p = (\mathrm{tr}\, M)^p .$$

• Nous utiliserons le résultat classique suivant :

Soient $P_1,\ldots,P_n$ des éléments deux à deux permutables d'un anneau A de caractéristique p. On a :

$$(P_1+\ldots+P_m)^p = P_1^p + \ldots + P_m^p . \qquad (1)$$

C'est trivial si m = 1. Pour m = 2, on utilise le binôme de Newton, en remarquant que C_p^k est divisible par p pour tout $k \in \mathbb{N}_{p-1}$. Pour $m > 2$, on raisonne par récurrence.

• De ce que K est de caractéristique p, on déduit que les anneaux K[X] et $\mathcal{M}_n(K[X])$ sont de caractéristique p.

• Nous partons de l'égalité d'éléments de K[X] :

$$\det(XI_n+M)^p = (\det(XI_n+M))^p.$$

Par (1), avec ici $A = \mathcal{M}_n(K[X])$, et compte tenu de ce que XI_n et M sont permutables :

$$(XI_n+M)^p = X^pI_n + M^p$$

et donc : $$\det(X^pI_n+M^p) = (\det(XI_n+M))^p. \qquad (2)$$

- Nous avons :

$$\det(XI_n+M) = X^n + a_1X^{n-1} + \ldots + a_n,\ a_i \in K,\ a_1 = \operatorname{tr} M,$$

et : $$\det(X^pI_n+M^p) = X^{pn} + b_1X^{p(n-1)} + \ldots + b_n,\ b_i \in K,\ b_1 = \operatorname{tr} M^p.$$

Par (1), avec ici $A = K[X]$, qui est un anneau commutatif :

$$(\det(XI_n+M))^p = X^{pn} + a_1^pX^{p(n-1)} + \ldots + a_n^p.$$

Par (2), égalité d'éléments de $K[X]$:

$$\forall i \in \mathbb{N}_n \quad b_i = a_i^p .$$

En particulier : $b_1 = a_1^p$. □

Remarque. Un autre aspect du résultat est le suivant : pour tout nombre premier p et toute matrice $M \in \mathcal{M}_n(\mathbb{Z})$, les entiers $\operatorname{tr} M^p$ et $(\operatorname{tr} M)^p$ sont égaux modulo p.

4.1.3 Soit E un K-espace vectoriel admettant une base dénombrable $e = (e_i)_{i\in\mathbb{N}}$.

On note a l'endomorphisme de E défini par $u(e_i) = e_{i+1}$, et φ l'application : $u \mapsto ua$ - au de $\mathcal{L}(E)$ dans $\mathcal{L}(E)$.

1° Montrer que φ est un endomorphisme surjectif et non injectif.

2° Trouver les valeurs propres de φ. Soient λ l'une d'elles et E_λ le sous-espace propre associé ; montrer qu'il existe un unique $f \in E_\lambda$ tel que $f(e_o) = e_o$ et expliciter $f(e_i)$, $i \in \mathbb{N}$; trouver une base de E_λ.

1° La linéarité de φ est évidente. Soit $v \in \mathcal{L}(E)$; pour que $u \in \mathcal{L}(E)$ vérifie $\varphi(u) = v$, il faut et il suffit que :

$$\forall i \in \mathbb{N} \quad u(e_{i+1}) = a(u(e_i)) + v(e_i)$$

ce qui détermine u (par les images des vecteurs de la base e de E) quand on se donne $u(e_o)$, arbitrairement choisi dans E.

Toute $v \in \mathcal{L}(E)$ admet donc une infinité d'antécédents par φ. □

2° Soit $\lambda \in K$. Pour tout $u \in \mathcal{L}(E) \setminus \{0\}$, $\varphi(u) = \lambda u$ s'écrit :

$$\forall i \in \mathbb{N} \quad u(e_{i+1}) = (\lambda I+a)(u(e_i)), \text{ où } I = Id_E$$

ce qui détermine u quand on se donne $u(e_o)$, arbitrairement choisi dans $E \setminus \{0\}$.

Il en résulte que tout $\lambda \in K$ est valeur propre de φ.

• Dans la suite, $\lambda \in K$ est fixé. Le sous espace propre E_λ associé à λ est $\{f_x \mid x \in E\}$, où f_x est défini (pour x donné) par :

$$\forall i \in \mathbb{N} \quad f_x(e_i) = (\lambda I + a)^i(x).$$

- En particulier, pour $x = e_o$, f_x, qui est alors noté f, s'écrit :

$$\forall i \in \mathbb{N} \quad f(e_i) = \sum_{k=o}^{i} C_i^k \lambda^{i-k} e_k.$$

- Pour tout $x \in E$, il existe une unique famille presque nulle d'éléments de K, $\alpha = (\alpha_j)_{j\in\mathbb{N}}$, telle que $x = \sum_{j\in\mathbb{N}} \alpha_j e_j = \sum_{j\in\mathbb{N}} \alpha_j a^j(e_o)$. On a :

$$\forall i \in \mathbb{N} \quad f_x(e_i) = \sum_{j\in\mathbb{N}} \alpha_j (\lambda I + a)^i a^j(e_o)$$

et, comme $(\lambda I+a)^i$ et a^j commutent :

$$\forall i \in \mathbb{N} \quad f_x(e_i) = \sum_{j\in\mathbb{N}} \alpha_j a^j f(e_i)$$

ce qui s'écrit :

$$f_x = \sum_{j\in\mathbb{N}} \alpha_j a^j f.$$

La famille $(a^j f)_{j\in\mathbb{N}}$ est donc génératrice de l'espace vectoriel E_λ. Comme, pour toute famille presque nulle α, $\sum_{j\in\mathbb{N}} \alpha_j a^j f$ n'est nul que si $\sum_{j\in\mathbb{N}} \alpha_j a^j f(e_o) = \sum_{j\in\mathbb{N}} \alpha_j e_j$ est nul, i.e. si α est nulle, la famille $(a^j f)_{j\in\mathbb{N}}$ est libre ; elle est donc une base (dénombrable) de E_λ.

Cas particulier. Pour $\lambda = 0$, E_o est Ker φ ; ici $f = I$; $(a^j)_{j\in\mathbb{N}}$ est base de Ker φ.

4.1.4 Soient a et b deux endomorphismes d'un $\mathbb{C}$-espace vectoriel E de dimension finie $n>0$. On leur associe l'endomorphisme $\varphi : u \mapsto au + ub$ de $\mathcal{L}(E)$.

Exprimer le polynôme caractéristique χ_φ de φ au moyen des racines $\alpha_1,\ldots,\alpha_n$ et $\beta_1,\ldots,\beta_n$ des polynômes caractéristiques χ_a et χ_b de a et b.

• Ici le corps de base est algébriquement clos ; on dispose d'une base (e_i), $i \in \mathbb{N}_n$, de E qui trigonalise b. On note :

$$\mathrm{mat}(a;(e_i)) = [a_{ij}] \ ; \ \mathrm{mat}(b;(e_i)) = [b_{ij}], \ b_{ij} = 0 \text{ si } i>j.$$

Soit (g_{ij}), $(i,j) \in \mathbb{N}_n^2$, la base de $\mathcal{L}(E)$ associée à (e_i) par :

$$\forall (i,j) \in \mathbb{N}_n^2 \quad \forall k \in \mathbb{N}_n \quad g_{ij}(e_k) = \delta_{jk} e_i .$$

Nous utiliserons : $g_{\ell m} g_{ij} = \delta_{mi} g_{\ell j}$.

• Ecrivons $\varphi = \varphi_1 + \varphi_2$, avec $\varphi_1 : u \mapsto au$ et $\varphi_2 : u \mapsto ub$.

En utilisant $a = \sum_{\ell,m} a_{\ell m} g_{\ell m}$, il vient, pour tout $(i,j) \in \mathbb{N}_n^2$:

$$\varphi_1(g_{ij}) = ag_{ij} = \sum_{\ell,m} a_{\ell m}\, g_{\ell m}\, g_{ij}$$

$$= \sum_{\ell,m} a_{\ell m}\, \delta_{mi}\, g_{\ell j} = \sum_{\ell} a_{\ell i}\, g_{\ell j}.$$

On calcule de même : $\varphi_2(g_{ij}) = \sum_{m} b_{jm}\, g_{im}$.

On ordonne la base (g_{ij}) de $\mathcal{L}(E)$ sous la forme :

$$g = (g_{11},\dots,g_{i1},\dots,g_{n1},\dots,g_{1j},\dots,g_{ij},\dots,g_{nj},\dots,$$

$$g_{1n},\dots,g_{in},\dots,g_{nn})$$

et on constate (c'est la partie la plus délicate de l'exercice) que $\mathrm{mat}(\varphi_1;g)$ et $\mathrm{mat}(\varphi_2;g)$, qui appartiennent à $\mathcal{M}_{n^2}(\mathbb{C})$, se présentent sous la forme de (n,n) matrices $P = [A_{kj}]$ et $Q = [B_{kj}]$ dont les éléments sont dans $\mathcal{M}_n(\mathbb{C})$, avec :

$A_{kj} = A$ si $k = j$, et 0 sinon ;

et : $B_{kj} = b_{jk}\, I_n$, et donc $B_{kj} = 0$ si $j > k$.

$P+Q = \mathrm{mat}(\varphi;g)$ est donc une matrice triangulaire inférieure de (n,n)-matrices ; les éléments diagonaux de P+Q sont (compte tenu de $b_{jj} = \beta_j$) les $A+\beta_j\, I_n$.

En utilisant une propriété classique des matrices triangulaires de matrices, on a :

$$\chi_\varphi(X) = \prod_{j=1}^{n} \det(XI_n - A - \beta_j I_n) = \prod_{j=1}^{n} \det((X-\beta_j)I_n - A)$$

et : $$\chi_\varphi(X) = \prod_{j=1}^{n} \chi_A(X-\beta_j).$$

En utilisant $\chi_A(X) = \prod_{i=1}^{n} (X-\alpha_i)$, il vient :

$$\chi_\varphi(X) = \prod_{i,j} (X-\beta_j-\alpha_i).$$

Remarque. Si le corps de base n'est pas $\mathbb{C}$, le calcul reste valable si b est trigonalisable, ce qui est toujours le cas si $b = 0$. Quel que soit le corps de base, le polynôme caractéristique de $u \mapsto au$ est donc $(\chi_a(X))^n$.

Il va de soi que a et b jouent des rôles symétriques.

4.1.5. Soient u et v deux endomorphismes d'un $\mathbb{C}$-espace vectoriel E de dimension finie $n > 0$. On suppose qu'il existe $(\alpha,\beta) \in \mathbb{C}^2$ tel que $uv - vu = \alpha u + \beta v$.

Montrer que u et v ont un vecteur propre commun.

Rappelons que tout endomorphisme d'un $\mathbb{C}$-espace vectoriel de dimension finie non nulle admet un sous-espace propre (et donc non nul).

Nous allons considérer trois cas, qui sont tous les cas possibles.

1er Cas : $\alpha = \beta = 0$. Soit $F \neq \{0\}$ un sous-espace propre de u. Comme ici u et

v commutent, F est stable par v. L'endomorphisme de F induit par v admet un vecteur propre, qui est a fortiori vecteur propre de v, et qui, au titre de vecteur non nul de F, est vecteur propre de u. □

2ème Cas : $\alpha \neq 0$ et $\beta = 0$. Il existe une valeur propre λ_0 de v tel que $\lambda_0 - \alpha$ ne soit pas valeur propre de v (sans quoi pour toute valeur propre λ de v et tout $m \in \mathbb{N}$, $\lambda - m\alpha$ serait valeur propre de v, en contradiction avec $\dim E < +\infty$).

Soit x_0 un vecteur propre de v associé à λ_0. Il vient :

$$v(u(x_0)) = (\lambda_0 - \alpha)u(x_0)$$

et donc $u(x_0) = 0$ (sans quoi $\lambda_0 - \alpha$ serait valeur propre de v) ; x_0 est vecteur propre commun à u et v. □

Autre solution. Ici $uv' - v'u = u$, où $v' = \alpha^{-1}v$, ce qui permet de montrer que u est nilpotent (cf. ci-dessous 4.3.3). On a donc $\operatorname{Ker} u \neq \{0\}$. On en déduit $u(v(x)) = 0$ pour tout $x \in \operatorname{Ker} u$, et $\operatorname{Ker} u$ est stable par v. On termine comme dans le 1er cas.

3ème Cas : $\beta \neq 0$. Posons : $w = uv - vu = \alpha u + \beta v$. Nous avons :

$$uw - wu = (\alpha u^2 + \beta uv) - (\alpha u^2 + \beta vu) = \beta w.$$

D'après le cas précédent, u et w ont un vecteur propre commun x_0. De $u(x_0) = \lambda x_0$ et $w(x_0) = \mu x_0$, on déduit : $v(x_0) = \beta^{-1}(\mu - \alpha\lambda)x_0$. □

4.1.6 Dans $\mathcal{M}_3(\mathbb{R})$ deux matrices sont dites "associées" si, et seulement si elles commutent et sont semblables. Soit E le sous-ensemble de $\mathcal{M}_3(\mathbb{R})$ formé par les matrices qui n'admettent qu'un nombre fini de matrices associées.

1° Soit $A \in \mathcal{M}_3(\mathbb{R})$ tel que le polynôme caractéristique de A n'a, sur $\mathbb{C}$, que des racines simples. Montrer que A appartient à E.

2° Déterminer E.

• La notion de matrices associées s'étend à $\mathcal{M}_n(K)$. Dans cet ensemble :

i) Si A et B sont associées, alors $A' = Q^{-1}AQ$ et $B' = Q^{-1}BQ$ le sont pour toute $Q \in GL_n(K)$.

Résulte de : $A'B' - B'A' = Q^{-1}(AB - BA)Q$ et de la transitivité de la similitude.

ii) Si A et B sont associées, alors $A'' = A + \lambda I_n$ et $B'' = B + \lambda I_n$ le sont pour tout $\lambda \in K$.

Résulte de : $A''B'' - B''A'' = AB - BA$, et de :

$$P^{-1}A''P = P^{-1}AP + \lambda I_n \text{ pour tout } P \in GL_n(K).$$

• Dans le cas de deux matrices de $\mathcal{M}_3(\mathbb{R})$ qui sont semblables (resp. qui se déduisent l'une de l'autre par addition d'une matrice scalaire), l'une d'elles appartient donc à E si, et seulement si l'autre appartient à E.

1° D'après l'hypothèse, A est diagonalisable dans $\mathcal{M}_3(\mathbb{C})$, ensemble dans lequel nous nous plaçons pour commencer : A est semblable à une matrice de la forme : $A' = \mathrm{diag}(\alpha_1,\alpha_2,\alpha_3)$, $\alpha_i \neq \alpha_j$ pour $i \neq j$.

Les matrices qui commutent avec A' sont les matrices diagonales (se vérifie aisément directement). Celles d'entre elles qui sont semblables à A', et donc associées à A', sont les : $\mathrm{diag}(\beta_1,\beta_2,\beta_3)$, où $(\beta_1,\beta_2,\beta_3)$ se déduit de $(\alpha_1,\alpha_2,\alpha_3)$ par une permutation ; elles sont au nombre de six ; d'après le préambule i), il existe, dans $\mathcal{M}_3(\mathbb{C})$, six matrices associées à A.

Les matrices associées à A dans $\mathcal{M}_3(\mathbb{R})$, qui figurent parmi ces six, sont évidemment en nombre fini, et on a : $A \in E$. □

2° E contient les matrices dont le polynôme caractéristique n'a, sur $\mathbb{C}$, que des racines simples, et les matrices scalaires (chacune de celles-ci n'ayant qu'une matrice associée, à savoir elle-même).

Nous allons montrer que E ne contient pas d'autre matrice.

• Considérons donc $A \in \mathcal{M}_3(\mathbb{R})$ vérifiant l'une des deux conditions :

- le polynôme caractéristique s'écrit $(X-\alpha)^3$, avec nécessairement $\alpha \in \mathbb{R}$ et $A \neq \alpha I_3$.

- le polynôme caractéristique s'écrit $(X-\alpha)^2(X-\beta)$, avec $(\alpha,\beta) \in \mathbb{R}^2$ et $\alpha \neq \beta$.

Nous allons montrer $A \notin E$. D'après le préambule ii), nous pouvons limiter la démonstration au cas où $\alpha = 0$. Soit $u \in \mathcal{L}(\mathbb{R}^3)$ représenté par A dans la base canonique de $\mathbb{R}^3$. On constate que u est non nul, et non injectif d'où :

$$1 \leqslant \dim(\mathrm{Ker}\ u) \leqslant 2.$$

En outre, lorsque $\chi_u = X^3$ et $u \neq 0$, on a les inclusions strictes :

$$\{0\} \subset \mathrm{Ker}\ u \subset \mathrm{Ker}\ u^2, \text{ avec } \dim(\mathrm{Ker}\ u^2) \in \{2,3\}.$$

Nous allons voir que les cas possibles sont au nombre de cinq. Dans chacun d'eux, nous trouverons une matrice A' semblable à A, et une famille infinie de matrices B_x associées à A' ; il en résultera : $A' \notin E$, et, d'après le préambule i) : $A \notin E$.

1er Cas : $\chi_u = X^3$ et $\dim(\mathrm{Ker}\ u) = 2$. Ici $\mathrm{Ker}\ u^2 = \mathbb{R}^3$.

On choisit $e_3 \in \mathbb{R}^3 \setminus \mathrm{Ker}\ u$; ainsi $e_2 = u(e_3)$ appartient à $\mathrm{Ker}\ u \setminus \{0\}$; on complète en une base (e_1,e_2) de Ker u ; (e_1,e_2,e_3) est une base de $\mathbb{R}^3$ et :

$$u(e_1) = 0 \ ; \ u(e_2) = 0 \ ; \ u(e_3) = e_2.$$

A est semblable à $A' = \mathrm{mat}(u;(e_1,e_2,e_3))$.

Pour tout $x \in \mathbb{R}^*$, on note $B_x = xA'$; A' et B_x commutent.

D'autre part on constate, en utilisant $x \neq 0$, que (e_1, e_2, xe_3) est une base de $\mathbb{R}^3$, et que :

$$B_x = \mathrm{mat}(u ; (e_1, e_2, xe_3)).$$

On en déduit que A' et B_x qui représentent u dans des bases différentes sont semblables.

Au total, A' et B_x sont associées.

On dispose donc d'une infinité de matrices B_x associées à A'. □

2ème Cas : $\chi_u = X^3$, $\dim(\mathrm{Ker}\ u) = 1$ et $\dim(\mathrm{Ker}\ u^2) = 2$. On utilise $\mathrm{Ker}\ u^3 = \mathbb{R}^3$. On choisit $e_3 \in \mathbb{R}^3 \setminus \mathrm{Ker}\ u^2$; ainsi $e_2 = u(e_3)$ appartient à $\mathrm{Ker}\ u^2 \setminus \mathrm{Ker}\ u$ et $e_1 = u(e_2)$ appartient à $\mathrm{Ker}\ u \setminus \{0\}$; (e_1, e_2, e_3) est une base de $\mathbb{R}^3$ et :

$$u(e_1) = 0 \ ; \ u(e_2) = e_1 \ ; \ u(e_3) = e_2.$$

A est semblable à $A' = \mathrm{mat}(u ; (e_1, e_2, e_3))$.

Pour tout $x \in \mathbb{R}^*$, on note $B_x = xA'$. On termine comme dans le 1er cas, après avoir remarqué que (e_1, xe_2, x^2e_3) est une base de $\mathbb{R}^3$ et que :

$$B_x = \mathrm{mat}(u ; (e_1, xe_2, x^2e_3)).$$ □

3ème Cas : $\chi_u = X^3$, $\dim(\mathrm{Ker}\ u) = 1$ et $\mathrm{Ker}\ u^2 = \mathbb{R}^3$.

On choisit une base (e_1) de $\mathrm{Ker}\ u$, et on complète en une base (e_1, e_2', e_3') de $\mathbb{R}^3$; on a $u(u(e_2')) = 0$ et $u(e_2') \neq 0$; d'où $u(e_2') = \lambda e_1$, $\lambda \neq 0$; de même $u(e_3') = \mu e_1$, $\mu \neq 0$; on pose $e_2 = \lambda^{-1} e_2'$ et $e_3 = \mu^{-1} e_3'$; (e_1, e_2, e_3) est une base de $\mathbb{R}^3$ et :

$$u(e_1) = 0 \ ; \ u(e_2) = e_1 \ ; \ u(e_3) = e_1.$$

A est semblable à $A' = \mathrm{mat}(u ; (e_1, e_2, e_3))$.

Pour tout $x \in \mathbb{R}^*$, on note $B_x = xA'$. On termine comme dans le 1er cas, après avoir remarqué que (e_1, xe_2, xe_3) est une base de $\mathbb{R}^3$ et que :

$$B_x = \mathrm{mat}(u ; (e_1, xe_2, xe_3)).$$ □

4ème Cas : $\chi_u = X^2(X-\beta)$, $\beta \in \mathbb{R}^*$, et $\dim(\mathrm{Ker}\ u) = 2$. Ici u est diagonalisable ; il existe une base (e_1, e_2, e_3) de $\mathbb{R}^3$ telle que :

$$u(e_1) = 0 \ ; \ u(e_2) = 0 \ ; \ u(e_3) = \beta e_3.$$

A est semblable à $A' = \mathrm{mat}(u ; (e_1, e_2, e_3)) = \mathrm{diag}(0, 0, \beta)$.

Pour tout $x \in \mathbb{R}$, on note v_x l'endomorphisme de E défini par :

$$v_x(e_1) = 0 \ ; \ v_x(e_2) = xe_1 + \beta e_2 \ ; \ v_x(e_3) = 0.$$

Soit $B_x = \mathrm{mat}(v_x ; (e_1, e_2, e_3))$. On constate que $(e_1, e_3, xe_1 + \beta e_2)$ est une base de $\mathbb{R}^3$ et que : $\mathrm{mat}(v_x ; (e_1, e_3, xe_1 + \beta e_2)) = \mathrm{diag}(0, 0, \beta) = A'$.

A' est donc semblable à B_x. En outre on vérifie $uv_x = v_x u = 0$. Au total, A' et B_x sont associées. □

5ème Cas : $\chi_u = X^2(X-\beta)$, $\beta \in \mathbb{R}^*$, et $\dim(\mathrm{Ker}\ u) = 1$. On a les inclusions strictes :

$$\{0\} \subset \mathrm{Ker}\ u \subset \mathrm{Ker}\ u^2, \text{ avec } \dim(\mathrm{Ker}\ u^2) = 2.$$

En effet $\mathrm{Ker}\ u^2$ et $E_\beta = \mathrm{Ker}(u-\beta Id_{\mathbb{R}^3})$ sont supplémentaires, et $\dim E_\beta = 1$.

On choisit $e_3 \in E_\beta \setminus \{0\}$ et $e_2 \in \mathrm{Ker}\ u^2 \setminus \mathrm{Ker}\ u$; ainsi $e_1 = u(e_2)$ appartient à $\mathrm{Ker}\ u \setminus \{0\}$; (e_1,e_2,e_3) est une base de $\mathbb{R}^3$ et :

$$u(e_1) = 0 \ ; \ u(e_2) = e_1 \ ; \ u(e_3) = \beta e_3.$$

A est semblable à $A' = \mathrm{mat}(u\ ;(e_1,e_2,e_3))$.

Pour tout $x \in \mathbb{R}^*$, on note v_x l'endomorphisme de E défini par :

$$v_x(e_1) = 0 \ ; \ v_x(e_2) = xe_1 \ ; \ v_x(e_3) = \beta e_3$$

Soit $B_x = \mathrm{mat}(v_x\ ;(e_1,e_2,e_3))$. On constate que $(e_1,x^{-1}e_2,e_3)$ est une base de $\mathbb{R}^3$ et que : $\mathrm{mat}(v_x\ ;(e_1,x^{-1}e_2,e_3)) = A'$.

A' est donc semblable à B_x. En outre on vérifie $uv_x = v_x u$. Au total, A' et B_x sont associées. □

Remarque. Le résultat vaut encore si l'on remplace $\mathcal{M}_3(\mathbb{R})$ par $\mathcal{M}_n(\mathbb{R})$, mais pour $n > 3$ la vérification est plus difficile.

4.1.7 Soient A et B des K-matrices (p,n) et (n,p), $1 \leq p \leq n$, et :

$$J = \left[\begin{array}{c|c} I_n & 0_{np} \\ \hline A & I_p \end{array}\right] \ ; \ L = \left[\begin{array}{c|c} XI_n - BA & B \\ \hline 0_{pn} & XI_p \end{array}\right] \ ; \ M = \left[\begin{array}{c|c} XI_n & B \\ \hline 0_{pn} & XI_p - AB \end{array}\right].$$

Comparer LJ et JM. En déduire une relation simple entre les polynômes caractéristiques χ_{AB} et χ_{BA}.

La multiplication des matrices par blocs montre que LJ et JM sont l'une et l'autre égales à : $\left[\begin{array}{c|c} XI_n & B \\ \hline XA & XI_p \end{array}\right]$.

J est une matrice triangulaire dont le déterminant est 1.

En développant p fois suivant la dernière ligne : $\det L = X^p \chi_{BA}$.

En développant n fois suivant la première colonne : $\det M = X^n \chi_{AB}$. D'où :

$$\chi_{BA} = X^{n-p} \chi_{AB}.$$

4.1.8 1° Soient E un $\mathbb{C}$-espace vectoriel de dimension finie $n > 0$, et u une application semi-linéaire de E dans E. Montrer que si u^2 admet une valeur propre $\lambda \in \mathbb{R}_-^*$, alors λ est racine d'ordre pair du polynôme caractéristique χ_{u^2}.

2° Soit $A \in \mathcal{M}_n(\mathbb{C})$. Montrer : $\det(I_n + A\overline{A}) \in \mathbb{R}_+$.

1° De $u(x+y) = u(x) + u(y)$ et $u(\alpha x) = \overline{\alpha} u(x)$, on déduit $u^2 \in \mathcal{L}(E)$.

Soit $(\lambda, a) \in \mathbb{R}^* \times (E \setminus \{0\})$ tel que $u^2(a) = \lambda a$.

• On a : $u^2(u(a)) = u(u^2(a)) = u(\lambda a) = \overline{\lambda} u(a)$

et, λ étant réel : $u^2(u(a)) = \lambda u(a)$.

Dans E, $(a, u(a))$ est libre, sinon (puisque $a \neq 0$) on aurait $u(a) = ka$ et :

$$\lambda a = u(u(a)) = u(ka) = \overline{k} u(a) = \overline{k} k a, \text{ et } \lambda = \overline{k} k \in \mathbb{R}_+.$$

Le sous-espace propre de u^2 associé à λ contient donc le plan $F = \mathrm{Vect}(a, u(a))$, qui est d'ailleurs stable par u ; en effet tout $x \in F$ s'écrit $\alpha a + \beta u(a)$ et vérifie : $u(x) = \overline{\beta}\lambda a + \overline{\alpha} u(a) \in F$.

• On a donc $n \geqslant 2$, et la proposition est acquise si $n = 2$.

• Sinon on introduit un supplémentaire G de F dans E, et on note p le projecteur d'image G et de noyau F. En considérant une base de E réunion de bases de F et G, on constate :

$$\chi_{u^2} = (X-\lambda)^2 \chi_v, \text{ où } v \in \mathcal{L}(G) \text{ est défini par :}$$

$$\forall x \in G \quad v(x) = pu^2(x) .$$

On vérifie aisément que l'application $w : x \mapsto pu(x)$ de G dans G est semi-linéaire. On va montrer $v = w^2$, ce qui permettra d'obtenir la proposition par récurrence.

- Pour tout $x \in G$, on a :

$$v(x) = pu(u(x)) = pu(w(x)+y) \text{ avec } y \in F.$$

Comme $y \in F$ entraîne $u(y) \in F$ et donc $pu(y) = 0$, il vient : $v(x) = pu(w(x))$. Or $w(x) \in G$ entraîne $pu(w(x)) = w(w(x))$. Finalement ;

$$\forall x \in G \quad v(x) = w^2(x). \qquad \square$$

2° On constate que $u : \mathbb{C}^n \to \mathbb{C}^n$ définie par :

$$\begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix} \longmapsto A \begin{bmatrix} \overline{\xi}_1 \\ \vdots \\ \overline{\xi}_n \end{bmatrix}$$

est semi-linéaire, et que $A\overline{A}$ représente $u^2 \in \mathcal{L}(\mathbb{C}^n)$ dans la base canonique.

D'après l'exercice précédent, on a $\chi_{A\overline{A}} = \chi_{\overline{A}A}$. Mais $\overline{A}A = \overline{A\overline{A}}$. D'où :

$$\chi_{A\overline{A}} \in \mathbb{R}[X] .$$

En notant $\lambda_1, \ldots, \lambda_r$ les racines réelles de $\chi_{A\overline{A}}$ et $k_1, \ldots, k_r$ leurs multiplicités, on peut écrire :

$$\chi_{A\bar{A}} = P \prod_{i=1}^{r} (X-\lambda_i)^{k_i}$$

où $P \in \mathbb{R}[X]$ est normalisé, de degré pair, sans racine réelle. D'où :

$$\det(I_n + A\bar{A}) = (-1)^n \chi_{A\bar{A}}(-1) = (-1)^{n+k} P(-1) \prod_{i=1}^{r} (1+\lambda_i)^{k_i}$$

avec $k = k_1 + \ldots + k_r$. Or $n-k = \deg P$ est pair, et aussi $n+k$.

En outre $P(-1) > 0$. Enfin, pour tout $i \in \mathbb{N}_r$, on a : $(1+\lambda_i)^{k_i} \geqslant 0$ (si $\lambda_i \geqslant 0$ c'est trivial, si $\lambda_i < 0$ alors k_i est pair d'après 1°). □

4.2. DIAGONALISATION

4.2.1 Soient $n \in \mathbb{N}^*$ et $A = [a_{ij}]$ une (n,n)-matrice sur K. On note B la matrice complémentaire de A, transposée de la comatrice de A (dans celle-ci l'élément (i,j) est le cofacteur A_{ij} de a_{ij} dans A).

1° Montrer que tout vecteur propre de A est vecteur propre de B.

2° On suppose ici que A est diagonalisable. Exprimer les valeurs propres de B en fonction de celles de A.

Un élément de K^n est identifié à une K-matrice $(n,1)$.

1°) On vérifie aisément : $AB = BA = (\det A) I_n$.

Distinguons trois cas.

1er Cas : A est inversible (i.e. de rang n).

Soit X un vecteur propre de A, associé à une valeur propre α (nécessairement non nulle). On a :

$$AX = \alpha X \; ; \; A^{-1}X = \frac{1}{\alpha} X \; ; \; BX = \frac{\det A}{\alpha} X.$$

X est vecteur propre de B associé à la valeur propre $\beta = (\det A)/\alpha$.

2ème Cas : Le rang de A est n-1, i.e. 0 est valeur propre de A et le sous-espace propre associé est de dimension 1.

Ici $AB = BA$ est la (n,n) matrice nulle 0.

Soit X un vecteur propre de A associé à une valeur propre α.

- Si $\alpha \neq 0$, de $AX = \alpha X$ on déduit $BAX = \alpha BX$, i.e. $BX = \alpha^{-1} 0X$.

BX est la matrice-colonne nulle ; X est vecteur propre de B associé à la valeur propre $\beta = 0$.

- Si $\alpha = 0$, on a $ABX = 0X$; $A(BX)$ est la matrice-colonne nulle ; BX appartient au sous-espace propre de A, associé à la valeur propre 0, et donc $BX = \beta X$; X est vecteur propre de B.

3ème Cas : Le rang de A est $r \leqslant n-2$, i.e. tous les A_{ij} sont nuls. On a : $B = 0$. Tout élément non nul de K^n, et en particulier tout vecteur propre de A, est vecteur propre de B, associé à la valeur propre 0.

2° Ici il existe une base $(X_1,\dots,X_n)$ de K^n formée de vecteurs propres de A, soit $AX_k = \alpha_k X_k$ pour tout $k\in\mathbf{N}_n$. D'après 1°, cette base est formée de vecteurs propres de B, qui est ainsi diagonalisable ; posons $BX_k = \beta_k X_k$ pour tout $n\in\mathbf{N}_n$. Reprenons les trois cas du 1°.

1er Cas. En utilisant 1°, on obtient : $\beta_k = \dfrac{\det A}{\alpha_k} = \prod_{i\neq k} \alpha_i$ pour tout $k\in\mathbf{N}_n$.

2ème Cas. Une, et une seule des α_k est nulle, par exemple $\alpha_n = 0$ et $\alpha_k \neq 0$ pour $k\neq n$. En utilisant 1°, on obtient : $\beta_k = 0$ pour tout $k\in\mathbf{N}_{n-1}$. La somme des racines du polynôme caractéristique de B étant tr B, il vient : $\beta_n = \operatorname{tr} B$. Pour toute matrice A, en développant $\det(XI_n-A)$ on constate que le coefficient de X dans le polynôme caractéristique χ_A est : $(-1)^{n-1}(A_{11}+\dots A_{nn})$ et donc $(-1)^{n-1}\operatorname{tr} B$, puisque les A_{ii} sont les éléments diagonaux de B.

Comme ici $\chi_A = X\prod_{i=1}^{n-1}(X-\alpha_i)$, on en déduit que ce coefficient est $(-1)^{n-1}\alpha_1\dots\alpha_{n-1}$. En conclusion : $\beta_n = \alpha_1\dots\alpha_{n-1}$.

3ème Cas. Ici deux des α_k au moins sont nulles. On a B = 0, et donc $\beta_k = 0$ pour tout $k\in\mathbf{N}_n$.

Remarque. Dans tous les cas : $\beta_k = \prod_{i\neq k} \alpha_i$ pour tout $k\in\mathbf{N}_n$.

4.2.2 Soit a un endomorphisme d'un K-espace vectoriel E de dimension finie $n>0$. On lui associe l'endomorphisme $\varphi : u \longmapsto$ au-ua de $\mathcal{L}(E)$.

1° On suppose ici que a est diagonalisable. Montrer que φ est diagonalisable ; en déterminer (par une base) le noyau et l'image.

Dans le cas où a admet n valeurs propres deux à deux distinctes, montrer que le noyau de φ est la sous-algèbre K[a] de $\mathcal{L}(E)$.

2° On suppose ici que a admet un vecteur propre x_o et que φ est diagonalisable. Montrer que a est diagonalisable.

3° On suppose ici que a est nilpotent. Montrer que φ est nilpotent.

(Les trois questions sont indépendantes).

1° On dispose ici d'une base (e_i), $i\in\mathbf{N}_n$, de E constituée de vecteurs propres de a ; on note $a(e_i) = \alpha_i e_i$ pour tout $i\in\mathbf{N}_n$.

Soit (g_{ij}), $(i,j)\in\mathbf{N}_n^2$, la base de $\mathcal{L}(E)$ associée à (e_i) par :

$$\forall (i,j)\in\mathbf{N}_n^2 \quad \forall k\in\mathbf{N}_n \quad g_{ij}(e_k) = \delta_{jk}e_i.$$

Pour (i,j) donné, on a : $\varphi(g_{ij})(e_k) = \delta_{jk}(\alpha_i-\alpha_k)e_i$, et donc :

$$\varphi(g_{ij}) = (\alpha_i-\alpha_j)g_{ij}\ .$$

Il en résulte que la base (g_{ij}) diagonalise φ, dont le polynôme caractéristique est :

$$\prod_{(i,j)\in\mathbb{N}_n^2} \left(X-(\alpha_i-\alpha_j)\right). \qquad \square$$

• Que a soit diagonalisable ou non, le noyau de φ est l'ensemble $\mathcal{C}$ des endomorphismes de E qui commutent avec a (*commutant* de a) ; il s'agit visiblement d'une sous-algèbre de $\mathcal{L}(E)$ qui contient $K[a]$.

Au titre de sous-espace propre de φ associé à la valeur propre 0, $\mathcal{C}$ admet ici la base (g_{ij}), $(i,j) \in \Omega$, où $\Omega = \{(i,j) \in \mathbb{N}_n^2 \mid \alpha_i = \alpha_j\}$. Notant $\lambda_1,\ldots,\lambda_p$ les racines distinctes du polynôme caractéristique de a et $m_1,\ldots,m_p$ leurs multiplicités on a : $\dim \mathcal{C} = \rho$, où $\rho = \sum_{j=1}^{p} m_j^2$.

De dimension $n^2-\rho$, Im φ, est visiblement engendré par (g_{ij}), $(i,j) \notin \Omega$, famille de cardinal $n^2-\rho$ qui en est ainsi une base.

Notons que, $m_j \geqslant 1$ entraînant $m_j^2 \geqslant m_j$, on a $\rho \geqslant \sum_{j=1}^{p} m_j$, i.e. $\rho \geqslant n$, la valeur minimale $\rho = n$ étant atteinte lorsque les α_i sont deux à deux distincts (ce qui garantit que a est diagonalisable).

• Etudions ce cas. Im φ, engendré par $(g_{ij})_{i\neq j}$ est l'ensemble des endomorphismes de E représentés dans la base (e_i) par les matrices à diagonale nulle (i.e. formée de zéros). $\mathcal{C}$ est l'ensemble des endomorphismes de E représentés dans la base (e_i) par les matrices diagonales. Nous avons vu $K[a] \subset \mathcal{C}$; nous allons montrer $\mathcal{C} \subset K[a]$ et donc $\mathcal{C} = K[a]$.

Soit $u \in \mathcal{C}$; on note $u(e_i) = \mu_i e_i$ pour tout $i \in \mathbb{N}_n$. Il suffit de montrer qu'il existe un $(\beta_0,\ldots,\beta_{n-1}) \in K^n$ tel que $u = \sum_{k=0}^{n-1} \beta_k a^k$, i.e. que le système linéaire à l'inconnue $(\xi_0,\ldots,\xi_{n-1})$:

$$\sum_{k=0}^{n-1} \alpha_i^k \xi_k = \mu_i, \quad i \in \mathbb{N}_n,$$

admet une solution, pour avoir $u \in K[a]$. Or le déterminant de ce système est le Vandermonde de la famille $(\alpha_1,\ldots,\alpha_n)$, non nul puisque les α_i sont deux à deux distincts ; le système considéré est cramérien. $\square$

2° L'existence d'un vecteur propre x_o de a (automatiquement acquise si K est algébriquement clos) permet de poser : $a(x_o) = \lambda x_o$.

Soit (f_{ij}), $(i,j) \in \mathbb{N}_n^2$, une base de $\mathcal{L}(E)$ qui diagonalise φ :

$$\forall (i,j) \in \mathbb{N}_n^2 \quad \varphi(f_{ij}) = \beta_{ij} f_{ij}.$$

Nous constatons que :

$$\forall (i,j) \in \mathbb{N}_n^2 \quad a(f_{ij}(x_o)) = (\beta_{ij}+\lambda) f_{ij}(x_o) \qquad (1)$$

• Montrons que la famille $(f_{ij}(x_o))$, $(i,j) \in \mathbb{N}_n^2$, engendre E. Il en résultera que l'on peut en extraite une base de E, et que cette base diagonalise a (d'après (1)).

Soit $y \in E$. Vecteur propre de a, x_o est non nul et on peut le considérer comme un vecteur d'une base de E ; il existe donc $u \in \mathcal{L}(E)$ tel que $u(x_o) = y$. Dans la base (f_{ij}) de $\mathcal{L}(E)$, u s'écrit $\sum_{i,j} \xi_{ij} f_{ij}$; d'où $y = \sum_{i,j} \xi_{ij} f_{ij}(x_o)$. □

3° Au départ, on ne suppose pas que a est nilpotent. Le calcul (laissé au lecteur) de $\varphi^2(u)$ et $\varphi^3(u)$ conduit à essayer de montrer par récurrence qu'est vraie pour tout $p \in \mathbb{N}^*$ l'assertion :

$$(\mathcal{A}_p) \qquad \forall u \in \mathcal{L}(E) \quad \varphi^p(u) = \sum_{k=o}^{p} (-1)^k \, C_p^k \, a^{p-k} u a^k$$

- Il est clair que $(\mathcal{A}_1)$ est vraie.
- Soit $p \in \mathbb{N}^*$ pour lequel $(\mathcal{A}_p)$ a été vérifiée. Pour tout $u \in \mathcal{L}(E)$, on a :

$$\varphi^{p+1}(u) = \varphi^p(\varphi(u)) = \varphi^p(au - ua)$$

et donc :

$$\varphi^{p+1}(u) = \sum_{k=o}^{p} (-1)^k \, C_p^k \, a^{p+1-k} \, ua^k + \sum_{k=1}^{p+1} (-1)^k \, C_p^{k-1} \, a^{p+1-k} \, ua^k.$$

Pour tout $k \in \mathbb{N}_p$, au second membre de l'égalité précédente, le coefficient de $(-1)^k \, a^{p+1-k} \, ua^k$ est : $C_p^k + C_p^{k-1} = C_{p+1}^k$.

On en déduit aisément que $(\mathcal{A}_{p+1})$ est vraie. □

- On ajoute maintenant l'hypothèse : a est nilpotent.

Soit $q \in \mathbb{N}$ tel que $a^q = 0$. On choisit $p = 2q-1$, et on écrit $(\mathcal{A}_p)$, en remarquant que $a^k = 0$ si $k \geqslant q$, et que $a^{p-k} = 0$ si $p-k \geqslant q$, i.e. $k \leqslant q-1$. On a donc : $\varphi^{2q-1} = 0$. □

4.2.3 Soient E un K-espace vectoriel de dimension finie ou infinie, u un endomorphisme diagonalisable de E, et F un sous-espace non nul de E stable par u.
Montrer que l'endomorphisme v de F induit par u est diagonalisable.

1° Commençons par un rappel et des remarques.

α) Dire que $u \in \mathcal{L}(E)$ est diagonalisable c'est dire que $E = \bigoplus_{\lambda \in Sp\, u} E_\lambda$, où Sp u est l'ensemble des valeurs propres de u, et où E_λ est le sous-espace propre de u associé à $\lambda \in Sp\, u$.

β) Soit v l'endomorphisme induit par u sur le sous-espace stable F.

Il est clair que toute valeur propre de v est valeur propre de u, et que, pour toute valeur propre λ de u, λ est valeur propre de v si et seulement si $E_\lambda \cap F$ n'est pas réduit à {0} ; lorsqu'il en est ainsi, $E_\lambda \cap F$ est le sous-espace propre de v associé à $\lambda \in Sp\, v$.

γ) Visiblement : $\bigoplus_{\lambda \in Sp\, u} E_\lambda \cap F \subset F$.

• Nous allons montrer : $F \subset \bigoplus_{\lambda \in Sp\, u} E_\lambda \cap F$ (1)

Compte tenu de γ), nous aurons : $F = \bigoplus_{\lambda \in Sp\, u} E_\lambda \cap F$,
et donc, compte tenu de β) :

$$F = \bigoplus_{\lambda \in Sp\, v} F_\lambda, \text{ où } F_\lambda = E_\lambda \cap F$$

est le sous-espace propre de v associé à $\lambda \in Sp\, v$; d'où la proposition.

• Preuve de (1). Soit $x \in E$. D'après α), on peut lui associer une famille presque nulle $(x_\lambda \in E_\lambda)_{\lambda \in Sp\, u}$ telle que $x = \sum_{\lambda \in Sp\, u} x_\lambda$.

Quitte à se restreindre au support de cette famille, on dispose de valeurs propres $\lambda_1, \ldots, \lambda_k$ deux à deux distinctes de u telles que :

$$x = \sum_{j=1}^{k} x_j, \; x_j \in E_{\lambda_j}$$

Considérons en particulier le cas où $x \in F$. Comme F est stable par u, à tout $i \in \mathbb{N}^*$ nous pouvons associer le vecteur $y_i = u^{i-1}(x)$ de F, et :

$$\forall i \in \mathbb{N}_k \quad y_i = \sum_{j=1}^{k} \alpha_{ij} x_j, \text{ où } \alpha_{ij} = \lambda_j^{i-1} \tag{2}$$

Soit M la matrice $[\alpha_{ij}]$, $(i,j) \in (\mathbb{N}_k)^2$; det M est le déterminant de Vandermonde de la famille $(\lambda_1, \ldots, \lambda_k)$ composée d'éléments deux à deux distincts ; on a donc det $M \neq 0$, et (2) s'écrit :

$$\forall j \in \mathbb{N}_k \quad x_j = \frac{1}{\det M} \sum_{i=1}^{k} A_{ij} y_i$$

où A_{ij} est le cofacteur de α_{ij} dans M.

Pour tout $j \in \mathbb{N}_k$, on a ainsi $x_j \in F$, et donc $x_j \in E_{\lambda_j} \cap F$.

Tout $x \in F$ appartient donc à $\bigoplus_{\lambda \in Sp\, u} E_\lambda \cap F$. D'où (1). □

2° Voici une autre solution qui ne vaut que dans le cas dim $E < +\infty$. On sait qu'alors un endomorphisme de E, ou du sous-espace F de E est diagonalisable si et seulement s'il annule un polynôme non nul scindé sur K, dont toutes les racines sont simples.

Ici, pour tout $P \in K[X]$, si P(u) est l'élément nul de $\mathcal{L}(E)$, alors P(v) est l'élément nul de $\mathcal{L}(F)$. □

4.2.4 Soient E un K-espace vectoriel de dimension finie $n > 0$, et $(u_i)_{i \in I}$ une famille finie ou infinie d'endomorphismes diagonalisables de E.

1° Prouver l'équivalence des assertions :

i) Les u_i commutent deux à deux ;

ii) Il existe une base de E qui diagonalise chacun des u_i.

2° Montrer que, lorsque ces assertions sont vraies, il existe un endomorphisme diagonalisable w de E et une famille $(P_i)_{i\in I}$ de polynômes de $K[X]$ tels que $u_i = P_i(w)$ pour tout $i \in I$.

1° Preuve de ii) ⇒ i). Par hypothèse, il existe une base (ε_ℓ), $\ell \in \mathbf{N}_n$, telle que chaque ε_ℓ soit vecteur propre pour chaque u_i.

Soit $(i,j) \in I^2$. On vérifie : $u_i(u_j(x)) = u_j(u_i(x))$ d'abord pour chacun des ε_ℓ, puis pour tout $x \in E$. □

Preuve de i) ⇒ ii). Procédons par récurrence sur $n = \dim E$. L'assertion i) ⇒ ii) est notée $\mathcal{A}_n$. Nous allons montrer qu'elle est vraie pour tout $n \in \mathbf{N}^*$.

• $\mathcal{A}_1$ est vraie car toute base d'un espace d'un espace vectoriel E de dimension un diagonalise tout endomorphisme de E.

• Soit $n \geqslant 2$, tel que $\mathcal{A}_1, \ldots, \mathcal{A}_{n-1}$ soient vraies. Considérons un K-espace vectoriel E de dimension n, et une famille $(u_i)_{i\in I}$ d'endomorphismes diagonalisables de E qui commutent deux à deux.

Si les u_i sont tous des homothéties, toute base de E diagonalise tout u_i.

Supposons maintenant que l'un des u_i, que nous notons u, ait au moins deux valeurs propres distinctes. Soient $\lambda_1, \ldots, \lambda_p$ les valeurs propres distinctes de u, et $E_1, \ldots, E_p$ les sous-espaces propres associés. Nous avons

$$E = E_1 \oplus E_1' \quad , \text{ où } \quad E_1' = \bigoplus_{k=2}^{p} E_k$$

avec : $1 \leqslant \dim E_1 \leqslant n-1$ et $1 \leqslant \dim E_1' \leqslant n-1$.

Pour tout $i \in I$, u_i commute avec u, et donc E_1 et E_1' sont stables par u_i, qui induit des endomorphismes v_i et v_i' de E_1 et E_1', diagonalisables d'après l'exercice précédent. Il est clair que, pour tout $(i,j) \in I^2$, v_i et v_j d'une part, v_i' et v_j' d'autre part commutent.

D'après l'hypothèse de récurrence, il existe une base e_1 de E_1 (resp. e_1' de E_1') formée de vecteurs propres communs à tous les v_i (resp. à tous les v_i') et donc à tous les u_i. En réunissant e_1 et e_1', on obtient une base e de E qui diagonalise chacun des u_i. □

2° Considérons cette base e et notons :

$$\forall i \in I \quad \mathrm{mat}(u_i;e) = \mathrm{diag}(\alpha_{i1}, \ldots, \alpha_{in}).$$

Choisissons arbitrairement des éléments $\mu_1, \ldots, \mu_n$ deux à deux distincts de K, et définissons $w \in \mathcal{L}(E)$ diagonalisable, par :

$$\mathrm{mat}(w;e) = \mathrm{diag}(\mu_1, \ldots, \mu_n).$$

Pour tout $P \in K[X]$, nous avons :

$$\mathrm{mat}(P(w);e) = \mathrm{diag}(P(\mu_1), \ldots, P(\mu_n)).$$

D'après l'étude des polynômes d'interpolation de Lagrange, à tout $i \in I$ nous pouvons associer un $P_i \in K[X]$, et un seul si l'on impose $\deg P_i \leqslant n-1$, tel que $P_i(u_k) = \alpha_{ik}$ pour tout $k \in \mathbb{N}_n$, ce qui entraîne $u_i = P_i(w)$. □

4.2.5 1° A quelle condition, nécessaire et suffisante, la $\mathbb{C}$-matrice

$$A = \begin{bmatrix} 0 & & \alpha_n \\ & \iddots & \\ \alpha_1 & & 0 \end{bmatrix}$$

est-elle diagonalisable ?

2° Le résultat s'étend-il à une $\mathbb{R}$-matrice de la même forme ?

Selon que n est impair ou pair, on note $n = 2p+1$ ou $n = 2p$.

1° Soit u l'endomorphisme de $\mathbb{C}^n$ qui est représenté par A dans la base canonique $(e_1,\dots,e_n)$ de $\mathbb{C}^n$. Nous pouvons écrire :

$$\mathbb{C}^n = \bigoplus_{i \in \mathbb{N}^*,\, 2i \leqslant n+1} E_i, \text{ où } E_i = \mathrm{Vect}(e_i, e_{n+1-i}) \qquad (1)$$

En utilisant : $u(e_i) = \alpha_i e_{n+1-i}$ et $u(e_{n+1-i}) = \alpha_{n+1-i} e_i$, nous constatons que chaque E_i est stable par u ; soit u_i l'endomorphisme de E_i induit par u.

En utilisant l'exercice 4.2.3, nous en déduisons qu'une condition nécessaire pour que u soit diagonalisable est que chaque u_i le soit ; cette condition est suffisante d'après (1).

Si $n = 2p+1$, nous avons $\dim E_{p+1} = 1$; u_{p+1} est diagonalisable.

Que $n = 2p+1$ ou $n = 2p$, il reste à écrire que, pour tout $i \in \mathbb{N}_p$,

$$A_i = \mathrm{mat}(u_i ; (e_i, e_{n+1-i})) = \begin{bmatrix} 0 & \alpha_{n+1-i} \\ \alpha_i & 0 \end{bmatrix}$$

est diagonalisable.

- Si $\alpha_i \alpha_{n+1-i} \neq 0$, A_i a deux valeurs propres distinctes, et est diagonalisable.

- Si $\alpha_i \alpha_{n+1-i} = 0$, A_i admet 0 pour valeur propre double, et A_i n'est diagonalisable que si elle est nulle, i.e. si $\alpha_i = \alpha_{n+1-i} = 0$.

En conclusion $A \in \mathcal{M}_n(\mathbb{C})$ est diagonalisable si, et seulement si :

$$\forall i \in \mathbb{N}_p \quad (\alpha_i = 0) \iff (\alpha_{n+1-i} = 0).$$

2° L'étude vaut sur $\mathbb{R}$ à condition de remarquer qu'ici A_i ne peut être diagonalisable que si son polynôme caractéristique est scindé sur $\mathbb{R}$, ce qui s'écrit : $\alpha_i \alpha_{n+1-i} \geqslant 0$ pour tout $i \in \mathbb{N}_p$.

Si la matrice A est réelle, elle est donc diagonalisable si, et seulement si :

$$\forall i \in \mathbb{N}_p \quad [\alpha_i \alpha_{n+1-i} \geqslant 0] \wedge [(\alpha_i = 0) \iff (\alpha_{n+1-i} = 0)].$$

4.2.6 1° Soient $p \in \mathbb{N}^*$, et $(\alpha_0,\dots,\alpha_{p-1}) \in \mathbb{C}^p$. Diagonaliser la "matrice circulante" :

$$A = \begin{bmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{p-1} \\ \alpha_{p-1} & \alpha_0 & \alpha_1 & \cdots & \alpha_{p-2} \\ \vdots & & & & \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_0 \end{bmatrix}$$

et calculer det A.

Cas particulier : $\alpha_0 = 1$, $\alpha_1 = 2,\dots,\alpha_{p-1} = p$.

2° Ici p est premier, et $\alpha_0,\dots,\alpha_{p-1}$ sont dans $\mathbb{Z}$. Vérifier :

$$\det A = \alpha_0 + \alpha_1 + \dots + \alpha_{p-1} \pmod p.$$

1° Dans la base canonique ε de $\mathbb{C}^p$, A représente $u \in \mathcal{L}(\mathbb{C}^p)$.

On constate que, pour toute racine p-ième t de 1, le vecteur non nul c(t) dont les coordonnées dans la base ε sont $1,t,\dots t^{p-1}$ est propre pour u, associé à la valeur propre P(t), ou $P(X) = \alpha_0 + \alpha_1 X + \dots + \alpha_{p-1} X^{p-1}$.

Les racines p-ièmes de 1 sont les ω^{j-1}, où $\omega = \exp\left(\frac{2i\pi}{p}\right)$ et $j \in \mathbb{N}_p$.

On dispose donc de la famille $e = \left(c(1),c(\omega),\dots,c(\omega^{p-1})\right)$ de vecteurs propres de u, d'ailleurs indépendante du choix de $\alpha_0,\dots,\alpha_{p-1}$. Soit Ω la matrice de la famille e dans la base ε ; det Ω est le déterminant de Vandermonde de la famille $(1,\omega,\dots,\omega^{p-1})$ dont les éléments sont deux à deux distincts ; d'où : det $\Omega \neq 0$; e est une base de $\mathbb{C}^p$, et Ω est la matrice de passage de ε à e.

Puisqu'il existe une base de $\mathbb{C}^p$ formée de vecteurs propres de u, cet endomorphisme est diagonalisable. On a :

$$\mathrm{Mat}(u;e) = D = \mathrm{diag}\left(P(1),P(\omega),\dots,P(\omega^{p-1})\right)$$

et : $$A = \Omega\, D\, \Omega^{-1}$$

D'où : $$\det A = \det D = P(1)P(\omega)\dots P(\omega^{p-1}).$$

Cas particulier. Ici $P(X) = 1 + 2X + \dots + pX^{p-1}$. On a : $P(1) = p(p+1)/2$. Dans $\mathbb{C}(X)$, P(X) est la dérivée de :

$$1 + X + X^2 + \dots + X^p = \frac{X^{p+1} - 1}{X - 1}$$

et on a : $$P(X) = \frac{pX^{p+1} - (p+1)X^p + 1}{(X-1)^2}.$$

Pour tout $z \in \mathbb{C} \setminus \{1\}$, on peut donc écrire :

$$P(z) = \frac{pz^{p+1} - (p+1)\, z^p + 1}{(z-1)^2}.$$

D'où : $$\forall k \in \mathbb{N}_{p-1} \quad P(\omega^k) = \frac{p}{\omega^k - 1},$$

et : $\det A = \frac{p(p+1)}{2}\ p^{p-1}\ \frac{1}{\beta}$, où $\beta = \prod_{k=1}^{p-1} (\omega^k - 1)$.

Les $\omega^k - 1$ sont les racines non nulles de $(z+1)^p - 1 = 0$, c'est-à-dire les racines de $z^{p-1} + C_p^1 z^{p-2} + \ldots + C_p^{p-1} = 0$; d'où $\beta = (-1)^{p-1} p$.

Finalement :

$$\det A = (-1)^{p-1}\ \frac{p+1}{2}\ p^{p-1}.$$

Remarque. Soit $\sigma \in \mathcal{L}(\mathbb{C}^p)$ défini par :

$$\sigma(\varepsilon_1) = \varepsilon_p\ ;\ \sigma(\varepsilon_2) = \varepsilon_1\ ;\ldots;\ \sigma(\varepsilon_p) = \varepsilon_{p-1}.$$

En convenant de noter $\varepsilon_m = \varepsilon_{m'}$ lorsque $m \equiv m' \pmod p$, on constate que, pour tout $k \in \mathbb{N}$, σ^k est défini par :

$$\forall j \in \mathbb{N}_p \quad \sigma^k(\varepsilon_j) = \varepsilon_{j-k}, \quad \text{(en particulier } \sigma^p = Id_{\mathbb{C}^p}).$$

On en déduit que, pour $k \in \{0,\ldots,n-1\}$, la matrice J^k qui représente σ^k dans la base ε est celle des matrices circulantes A dans lesquelles tous les coefficients sont nuls sauf les α_k, qui valent 1.

La matrice A s'écrit donc, dans le cas général :

$$A = \alpha_o I_p + \alpha_1 J + \ldots + \alpha_{p-1} J^{p-1} = P(J)\ .$$

D'où une variante de la diagonalisation de A, qui consiste à travailler d'abord sur J et à montrer, comme ci-dessus que :

$$J = \Omega.\mathrm{diag}(1,\omega,\ldots,\omega^{p-1}).\Omega^{-1}.$$

D'où : $$A = \Omega.\mathrm{diag}\big(P(1),\ P(\omega),\ldots,P(\omega^{p-1})\big).\Omega^{-1}.$$

2° Ici $p \geqslant 2$ est premier. Nous utiliserons :

- Pour tout $(a_1,\ldots,a_m) \in \mathbb{Z}^m$, $m \in \mathbb{N}^*$,

$$(a_1+\ldots+a_m)^p \equiv a_1^p + \ldots + a_m^p \pmod p \qquad (1)$$

Se prouve par récurrence sur m, en utilisant :

$$(a_1+a_2)^p - (a_1^p+a_2^p) = \sum_{k=1}^{p-1} C_p^k\ a_1^{p-k}\ a_2^k$$

égalité dans laquelle les C_p^k, $k \in \mathbb{N}_{p-1}$, sont des multiples de p.

- Pour tout $m \in \mathbb{Z}$, $m^p \equiv m \pmod p$ (2)

Pour $m = 0$, c'est trivial. Pour $m > 0$ (2), se déduit de (1). Pour $m < 0$, on utilise $(-1)^p = -1$, (mod p).

- Si $A_1,\ldots,A_m$ sont des (n,n) matrices à éléments dans $\mathbb{Z}$ qui commutent deux à deux, alors les éléments de la matrice :

$$(A_1 + \ldots + A_m)^p - (A_1^p + \ldots + A_m^p)$$

sont des multiples de p.

La justification est la même que celle de (1).

★ Venons-en à notre exercice. D'après la remarque du 1° :

$$A = \alpha_o I_p + \alpha_1 J + \ldots + \alpha_{p-1} J^{p-1}.$$

D'où : $$A^p = \sum_{k=o}^{p-1} (\alpha_k J^k)^p + B,$$

où les éléments de B sont des entiers multiples de p.

En utilisant $J^{kp} = I_p$ il vient :

$$A^p = sI_p + B, \text{ où } s = \alpha_o^p + \ldots + \alpha_{p-1}^p.$$

En utilisant l'expression du déterminant d'une matrice carrée à éléments dans $\mathbb{Z}$, on constate que, modulo p, celui-ci ne change pas lorsqu'on ajoute à chaque élément un multiple de p. On a donc :

$$\det(A^p) \equiv \det(sI_p) \pmod p.$$

Or : $$\det(A^p) = (\det A)^p, \text{ et } \det(sI_p) = s^p.$$

Compte tenu de ce que, modulo p : $(\det A)^p = \det A$, $s^p = s$ et $\alpha_k^p = \alpha_k$, on a :

$$\det A \equiv s \pmod p, \text{ avec } s \equiv \alpha_o + \ldots + \alpha_{p-1} \pmod p. \qquad \square$$

4.2.7 Soient $(a_1,\ldots,a_n) \in \mathbb{R}^n$, $n \in \mathbb{N}^*$, et $A = [\alpha_{ij}]$ la (n,n)-matrice réelle telle que $\alpha_{ij} = 0$ si $i \leqslant n-1$ et $j \leqslant n-1$, et que $\alpha_{in} = \alpha_{ni} = a_i$ pour tout $i \in \mathbb{N}_n$. Diagonaliser la matrice A.

Soit $\varepsilon = (\varepsilon_1,\ldots,\varepsilon_n)$ la base canonique de $\mathbb{R}^n$, et $u \in \mathcal{L}(\mathbb{R}^n)$ représenté par A dans la base ε. Il s'agit de trouver une base de $\mathbb{R}^n$ qui diagonalise u.

Il est clair que si $n = 1$, ou si le vecteur $a = a_1\varepsilon_1 + \ldots + a_{n-1}\varepsilon_{n-1}$ est nul, la base ε répond à la question (au départ, A est ici diagonale).

Nous nous limitons dorénavant au cas où $n \geqslant 2$ et $a \neq 0$.

• Calculons d'abord les valeurs propres non nulles de u.

Pour tout $\lambda \in \mathbb{R}^*$, le système :

$$(\forall i \in \mathbb{N}_{n-1} \quad a_i x_n = \lambda x_i) \wedge \left(\sum_{i=1}^{n-1} a_i x_i = (\lambda - a_n) x_n\right)$$

s'écrit :

$$(\forall i \in \mathbb{N}_{n-1} \quad x_i = (a_i/\lambda) x_n) \wedge \left((\lambda^2 - a_n\lambda - \sum_{i=1}^{n-1} a_i^2) x_n = 0\right)$$

et admet une solution non nulle si, et seulement si λ est racine de l'équation du second degré : $t^2 - a_n t - \sum_{i=1}^{n-1} a_i^2 = 0$.

Compte tenu de $\sum_{i=1}^{n-1} a_i^2 > 0$ cette équation admet deux racines réelles λ_1 et λ_2 telles que $\lambda_1 < 0 < \lambda_2$, à savoir :

$$\lambda_1 = \frac{1}{2}(a_n - \sqrt{\delta}) \text{ et } \lambda_2 = \frac{1}{2}(a_n + \sqrt{\delta}), \text{ où } \delta = a_n^2 + 4\sum_{i=1}^{n-1} a_i^2.$$

Les valeurs propres non nulles de u sont λ_1 et λ_2 ; les sous-espaces propres associés sont respectivement engendrés par $e_1 = a + \lambda_1 \varepsilon_n$ et $e_2 = a + \lambda_2 \varepsilon_n$.

Si n = 2, le calcul est terminé (0 n'est pas valeur propre ce que confirme d'ailleurs l'étude du noyau de u qui va suivre).

• Le noyau de u est donné dans la base ε par :

$$(\forall i \in \mathbb{N}_{n-1} \quad a_i x_n = 0) \wedge \left(\sum_{i=1}^{n} a_i x_i = 0\right)$$

et, compte tenu de $a \neq 0$, par :

$$(x_n = 0) \wedge \left(\sum_{i=1}^{n-1} a_i x_i = 0\right).$$

Il est de dimension n-2, et donc réduit à {0} pour n = 2. Pour $n \geqslant 3$, il est possible de choisir $k \in \mathbb{N}_{n-1}$ tel que $a_k \neq 0$, et on constate que les vecteurs $f_j = a_k \varepsilon_j - a_j \varepsilon_k$, $j \in \mathbb{N}_{n-1} \setminus \{k\}$ constituent une base du sous-espace propre Ker u associé à la valeur propre 0 de u. En adjoignant e_1 et e_2, on obtient une base $e = (e_1, e_2, e_3, \ldots, e_n)$ de $\mathbf{R}^n$ telle que :

$$A = PDP^{-1}, \text{ avec } P = P_{\varepsilon}^{e} \text{ et } D = \operatorname{diag}(\lambda_1, \lambda_2, 0, \ldots, 0).$$

Le lecteur explicitera les éléments de P au moyen des a_i, de λ_1 et de λ_2. □

Remarque. La matrice A étant symétrique à coefficients réels, on pouvait prévoir qu'elle était diagonalisable.

4.2.8 Soient $(\alpha, \beta, \gamma) \in \mathbb{C}^3$ et $A = [a_{ij}] \in \mathcal{M}_n(\mathbb{C})$, $n \geqslant 2$, avec :

$a_{ii} = \alpha$; $a_{ij} = \beta$ si $j - i = 1$; $a_{ij} = \gamma$ si $i - j = 1$;
$a_{ij} = 0$ si $|j - i| \notin \{0, 1\}$.

Trouver les valeurs propres de A, et, éventuellement, diagonaliser A.

Soit $B = A - \alpha I_n$. Les valeurs propres de A se déduisent de celles de B par addition de α, et une base de $\mathbb{C}^n$ diagonalise A si, et seulement si elle diagonalise B. On est donc ramené à étudier B.

a) Le cas $\beta\gamma = 0$ est trivial : B est alors triangulaire, à éléments diagonaux nuls ; les racines du polynôme caractéristique de B sont toutes nulles ; B est diagonalisable si, et seulement si B = 0, ce qui s'écrit $(\beta, \gamma) = (0, 0)$.

b) Dans toute la suite, nous supposons $\beta\gamma \neq 0$.

Le complexe λ est valeur propre de B si, et seulement si le système linéaire et homogène des n équations à l'inconnue $(x_1, \ldots, x_n)$:

$$\begin{cases} -\lambda x_1 + \beta x_2 = 0 \ ; \ \gamma x_{n-1} - \lambda x_n = 0 \\ \gamma x_{p-1} - \lambda x_p + \beta x_{p+1} = 0, \ 2 \leqslant p \leqslant n-1 \end{cases}$$

admet une solution non nulle, ou encore (en adjoignant les inconnues x_o et x_{n+1} et les équations $x_o = 0$ et $x_{n+1} = 0$) si, et seulement si le système linéaire et homogène des (n+2) équations à l'inconnue $(x_o, x_1, \ldots, x_n, x_{n+1})$:

$$(S_\lambda) \begin{cases} \gamma x_{p-1} - \lambda x_p + \beta x_{p+1} = 0, \ 1 \leqslant p \leqslant n \\ x_o = 0 \ ; \ x_{n+1} = 0 \end{cases}$$

admet une solution non nulle, i.e. telle que $x_1 \neq 0$.

On en déduit que le complexe λ est valeur propre de B si et seulement s'il existe une suite $(y_p)_{p \in \mathbb{N}}$ vérifiant les deux conditions :

$$\forall p \in \mathbb{N}^* \quad \gamma y_{p-1} - \lambda y_p + \beta y_{p+1} = 0 \tag{1}$$

et :
$$(y_o = 0) \wedge (y_1 \neq 0) \wedge (y_{n+1} = 0) \tag{2}$$

- L'étude des suites récurrentes linéaires nous conduit à associer à tout $\lambda \in \mathbb{C}$ les racines r_1 et r_2 de $\beta X^2 - \lambda X + \gamma$; notons que :

$$r_1 \neq 0 \ ; \ r_2 = \gamma/(\beta r_1) \neq 0.$$

Distinguons deux cas :

1er Cas. Soit $\lambda \in \mathbb{C}$ tel que $\lambda^2 = 4\beta\gamma$, i.e. $r_1 = r_2$.

Les suites qui vérifient (1) sont données par :

$$\forall p \in \mathbb{N} \quad y_p = (a+bp) r_1^p, \text{ avec } (a,b) \in \mathbb{C}^2.$$

La condition (2), qui s'écrit : $(a = 0) \wedge (b \neq 0) \wedge ((n+1)b = 0)$ n'est vérifiée par aucune de ces suites ; λ n'est pas valeur propre de B.

2ème Cas. Soit $\lambda \in \mathbb{C}$ tel que $\lambda^2 \neq 4\beta\gamma$, i.e. $r_1 \neq r_2$.

Les suites qui vérifient (1) sont données par :

$$\forall p \in \mathbb{N} \quad y_p = a r_1^p + b r_2^p, \text{ avec } (a,b) \in \mathbb{C}^2.$$

La condition (2) s'écrit : $(b = -a) \wedge (a \neq 0) \wedge (r_1^{n+1} = r_2^{n+1})$.

- En considérant les deux cas, on constate que $\lambda \in \mathbb{C}$ est valeur propre de B si, et seulement si :

$$(r_1 \neq r_2) \wedge (r_1^{n+1} = r_2^{n+1})$$

ce qui s'écrit, en désignant par δ une racine carrée arbitrairement choisie de $\gamma\beta^{-1}$:

$$(r_1^2 \neq \delta^2) \wedge (r_1^{2(n+1)} = \delta^{2(n+1)})$$

ou, encore, si, et seulement si r_1 est de la forme :

$$r_1 = \delta \exp(\pm i\theta_k), \text{ avec } \theta_k = \frac{k\pi}{n+1} \text{ et } k \in \mathbb{N}_n.$$

Compte tenu de : $\lambda = \beta(r_1+r_2) = \beta(r_1+\delta^2/r_1)$, on constate que B admet les n valeurs propres, visiblement deux à deux distinctes ;

$$\lambda_k = 2\mu \cos \theta_k, \text{ avec } \theta_k = \frac{k\pi}{n+1} \text{ et } k \in \mathbf{N}_n,$$

où $\mu = \beta\delta$ est une racine carrée arbitrairement choisie de $\beta\gamma$.

Il en résulte que B est diagonalisable.

Pour $k \in \mathbf{N}_n$ donné, les vecteurs propres de B associés à λ_k sont les vecteurs dont les composantes dans la base canonique $(\varepsilon_1,\ldots,\varepsilon_n)$ de $\mathbb{C}^n$ s'écrivent :

$$a(r_1^p - r_2^p) = a\left[r_1^p - (\delta^2/r_1)^p\right] = 2ia\delta^p \sin(\pm p\theta_k),\ a \neq 0,\ p \in \mathbf{N}_n.$$

Le sous-espace propre associé à λ_k est donc $\mathbb{C}e_k$ avec :

$$e_k = \sum_{p=1}^{n} \delta^p \sin(p\theta_k) \cdot \varepsilon_p \quad \text{et} \quad \theta_k = \frac{k\pi}{n+1}.$$

On a : $A = P D P^{-1}$, avec :

$$P = P_\varepsilon^e \quad \text{et} \quad D = \operatorname{diag}(\alpha+\lambda_1,\ldots,\alpha+\lambda_n).$$

Remarque. Le résultat s'étend au cas où α,β,γ sont des réels tels que $\beta\gamma > 0$, et où on considère $A \in \mathcal{M}_n(\mathbb{R})$.

4.2.9 1° Soit $n \in \mathbf{N}^*$. Trouver une base du sous-espace vectoriel E de $\mathbf{R}^{\mathbf{R}}$ engendré par la famille :

$$\mathcal{F} = \left(t \mapsto (\operatorname{ch} t)^{n-j} (\operatorname{sh} t)^j\right)_{j \in \{0,\ \ldots,n\}}.$$

2° En utilisant le 1°, diagonaliser la matrice $A = [\alpha_{ij}] \in \mathcal{M}_{n+1}(\mathbb{R})$ dans laquelle $\alpha_{ij} = 0$ pour tout $(i,j) \in \{0,\ldots,n\}^2$ sauf :

- si $j = i+1$, $j \in \mathbf{N}_n$, auquel cas $\alpha_{ij} = j$,
- si $i = j+1$, $i \in \mathbf{N}_n$, auquel cas $\alpha_{ij} = n+1-i$.

On explicitera les calculs pour $n = 3$.

Pour simplifier l'écriture, on utilise f(t) pour désigner une fonction (et non une valeur prise par une fonction).

1° Montrons que la famille $\mathcal{F}$ de n+1 éléments de $\mathbf{R}^{\mathbf{R}}$, qui engendre E, est libre ; il en résultera que $\mathcal{F}$ est une base de E et que dim E = n+1.

Soit $(\xi_0,\ldots,\xi_n)$ un élément non nul de $\mathbf{R}^{n+1}$. Associons-lui l'élément $\varphi(t) = \sum_{j=0}^{n} \xi_j (\operatorname{ch} t)^{n-j} (\operatorname{sh} t)^j$ de E. Il existe un unique $k \in \{0,\ldots,n\}$ tel que $\xi_k \neq 0$ et $\xi_j = 0$ si $j < k$. D'où l'équivalence :

$$\varphi(t) \sim \xi_k (\operatorname{sh} t)^k, \text{ au voisinage de } 0,$$

et donc : $\lim_{t\to 0, t\neq 0} \frac{\varphi(t)}{t^k} = \xi_k \neq 0$,

ce qui montre que la fonction $\varphi(t)$ n'est pas nulle. □

2° Il est clair que la dérivée d'un élément de $\mathcal{F}$ est un élément de E ; on dispose donc de l'application $d : \varphi \mapsto \varphi'$, visiblement linéaire, de E dans E.

On vérifie que A n'est autre que la matrice qui représente d dans la base $\mathcal{F}$.

- Soient $\varepsilon \in \{-1,1\}$ et $p \in \mathbb{N}$ tel que $2p \leqslant n$. Associons leur la fonction :

$$\varphi_{\varepsilon,p}(t) = \exp\big(\varepsilon(n-2p)t\big).$$

En utilisant : $\varphi_{\varepsilon,p}(t) = (\mathrm{ch}\, t + \varepsilon\, \mathrm{sh}\, t)^{n-p}(\mathrm{ch}\, t - \varepsilon\, \mathrm{sh}\, t)^p$, on constate qu'il s'agit d'un élément non nul de E. Par ailleurs, il est clair que sa dérivée est : $\varepsilon(n-2p)\varphi_{\varepsilon,p}(t)$. Il en résulte que $\varepsilon(n-2p)$ est une valeur propre de d [resp. A], et qu'un vecteur propre associé est $\varphi_{\varepsilon,p}(t)$ [resp. le vecteur-colonne dont la i-ième composante, $i \in \{0,\ldots,n\}$, est le coefficient de $X^{n-i}Y^i$ dans le développement du polynôme homogène :

$$(X+\varepsilon Y)^{n-p}(X-\varepsilon Y)^p .$$

Quelle que soit la parité de n, on a mis en évidence n+1 valeurs propres distinctes de la matrice A, d'ordre n+1, et, pour chacune d'elles trouvé un vecteur propre associé ; A est ainsi diagonalisable et nous savons la diagonaliser. Notons que A est non inversible si, et seulement si 0 est valeur propre, i.e. si, et seulement si n est pair.

• Pour n = 3, les valeurs propres de A sont 3, -3, 1, -1. Le lecteur vérifiera que l'on aboutit à : $P^{-1}AP = D$, où :

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & 3 \\ 0 & 0 & 1 & 0 \end{bmatrix} ; D = \begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} ; P = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 3 & -3 & 1 & -1 \\ 3 & 3 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} .$$

4.2.10 Ici $K = \mathbb{Z}/7\mathbb{Z}$. Soit $n \in \mathbb{N}^*$. Trouver toutes les $M \in \mathcal{M}_n(K)$ telles que $M^3 = I_n$.

Les éléments de K sont notés $\overline{0}, \overline{1}, \ldots, \overline{6}$.

• Il est clair qu'il existe des solutions diagonales, à savoir toutes les K-matrices (n,n) diagonales dont chaque élément diagonal a pour cube $\overline{1}$.

On les précise en calculant les cubes des éléments de K ; on obtient :

$$\forall x \in K \quad (x^3 = \overline{1}) \iff (x \in \{\overline{1}, \overline{2}, \overline{4}\}) \qquad (1)$$

• Les solutions diagonalisables sont donc les PDP^{-1}, où $P \in GL_n(K)$ et où $D \in \mathcal{M}_n(K)$ est diagonale, à éléments diagonaux dans $\{\overline{1},\overline{2},\overline{4}\}$.

• Montrons qu'il n'existe pas d'autre solution, i.e. que toute solution est diagonalisable.

Ceci résulte immédiatement de ce qu'une K-matrice carrée est diagonalisable si, et seulement si elle annule un polynôme non nul scindé sur K dont toutes les racines sont simples. Ici toute solution annule en effet le polynôme :

$$X^3 - \overline{1} = (X-\overline{1})(X-\overline{2})(X-\overline{4}).$$

4.2.11 Soient $A \in \mathcal{M}_n(\mathbb{R})$ et $B \in \mathcal{M}_{2n}(\mathbb{R})$ la matrice-bloc :

$$B = \left[\begin{array}{c|c} A & 0 \\ \hline A & A \end{array}\right]$$

A quelle condition la matrice B est-elle diagonalisable ?

• Par récurrence, on montre que, pour tout $i \in \mathbb{N}$ on a :

$$B^i = \left[\begin{array}{c|c} A^i & 0 \\ \hline iA^i & A^i \end{array}\right]$$

Par combinaisons linéaire, on a, pour tout $P = \sum \gamma_i X^i \in \mathbb{R}[X]$:

$$P(B) = \left[\begin{array}{c|c} P(A) & 0 \\ \hline AP'(A) & P(A) \end{array}\right] \qquad (1)$$

• On considère comme acquis qu'une K-matrice carrée est diagonalisable si, et seulement si elle annule un polynôme non nul scindé sur K dont toutes les racines sont simples.

• Supposons que B soit diagonalisable. Il existe $P \in \mathbb{R}[X]$ non nul, scindé sur $\mathbb{R}$ dont toutes les racines sont simples, et tel que $P(B) = 0$.

De (1), on déduit $P(A) = 0$ et $AP'(A) = 0$, ce qui signifie que les polynômes P et XP' sont divisibles par le polynôme minimal M de A. Puisque $P(A) = 0$, la matrice A est diagonalisable ; elle admet donc des valeurs propres ; celles-ci sont racines de M, et donc de P et de XP', et enfin de X car P et P' n'ont aucune racine commune (P n'a que des racines simples).

Diagonalisable et admettant 0 pour seule valeur propre, A est 0_n.

• Inversement, si $A = 0_n$, alors $B = 0_{2n}$ est diagonale, et donc diagonalisable.

4.3. Autres Réductions

Applications

4.3.1 Soit u un endomorphisme nilpotent d'un K-espace vectoriel de E de dimension finie $n>0$. Montrer qu'il existe une base de E dans laquelle u est représenté par une matrice triangulaire supérieure à diagonale nulle, et que le polynôme caractéristique de u est X^n.

Il s'agit d'un résultat classique, d'utilisation courante.

• Si u admet une valeur propre, celle-ci est nécessairement 0 ; il suffit donc de montrer que u est trigonalisable (ce qui est acquis si K est algébriquement clos).

• Pour tout $k\in\mathbb{N}$, nous notons $\operatorname{Ker} u^k = N_k$; r désignant l'indice de u, nous avons les inclusions strictes :

$$N_0 \subset N_1 \subset \ldots \subset N_{r-1} \subset N_r \text{ , avec } N_r = E,\ r \leqslant n.$$

A partir de la base vide de N_0, nous construisons une base $e = (e_1,\ldots,e_n)$ de $N_r = E$ par le procédé récurrent qui consiste, une fois obtenue une base de N_{k-1}, $k\in\mathbb{N}_r$, à lui adjoindre une base d'un supplémentaire de N_{k-1} dans N_k de façon à obtenir une base de N_k.

Pour tout $j\in\mathbb{N}_n$, il existe un unique $k\in\mathbb{N}_r$ tel que $e_j \in N_k \setminus N_{k-1}$; on a $N_{k-1} \subset \operatorname{Vect}(e_1,\ldots,e_j)$.

De $e_j \in N_k$ résulte $u(e_j) \in N_{k-1}$ et donc $u(e_j) \in \operatorname{Vect}(e_1,\ldots,e_j)$.

La base e trigonalise donc u. □

4.3.2 Soit u un endomorphisme d'un K-espace vectoriel E de dimension finie $n>0$. Pour tout $k\in\mathbb{N}$, on note $\operatorname{Ker} u^k = N_k$ et $\dim N_{k+1} - \dim N_k = \alpha_k$.

1° Montrer que la suite $(\alpha_k)_{k\in\mathbb{N}}$ est décroissante.

2° Montrer que, si u est nilpotent, les assertions suivantes sont équivalentes :

i) L'indice de u est n ;

ii) Pour tout $k\in\{0,\ldots,n\}$, $\dim N_k = k$;

iii) Il existe $k\in\mathbb{N}_{n-1}$ tel que $\dim N_k = k$;

iv) $\dim N_1 = 1$.

3° Montrer que si u est nilpotent d'indice n, il existe une base de E dans laquelle u est représenté par la K-matrice de Jordan d'ordre n, $J_n = [\alpha_{ij}]$ avec $\alpha_{ij} = 1$ si $j = i+1$ et $\alpha_{ij} = 0$ sinon.

1° Notons que $N_k \subset N_{k+1}$ entraîne $\alpha_k \geqslant 0$ pour tout $k \in \mathbb{N}$.

• Soient $k \geqslant 1$ et F_k un supplémentaire de N_k dans N_{k+1} ; nous avons $\dim F_k = \alpha_k$. Comme N_k contient $N_1 = \operatorname{Ker} u$, la restriction de u à F_k est injective, et donc : $\dim u(F_k) = \alpha_k$.

En remarquant que $x \in N_{k+1}$ entraîne $u(x) \in N_k$ et que $x \notin N_k$ entraîne $u(x) \notin N_{k-1}$, nous constatons :

$$u(F_k) \subset N_k \quad \text{et} \quad u(F_k) \cap N_{k-1} = \{0\}.$$

D'où : $$\left(u(F_k) \oplus N_{k-1}\right) \subset N_k \quad \text{et} \quad \dim\left(u(F_k)\right) \leqslant \alpha_{k-1}.$$ □

2° Ici u est nilpotent. Soit $r \in \mathbb{N}_n$ son indice. D'après la propriété des noyaux emboîtés, on a : $N_{r_{k-1}} = E$ et $\alpha_h \geqslant 1$ pour $0 \leqslant h \leqslant r-1$ (1)

D'où : $$k \leqslant \dim N_k = \sum_{h=o} \alpha_h \text{ pour tout } k \in \mathbb{N}_r. \quad (2)$$

• Preuve de i) ⇒ ii). Par hypothèse $r = n$. Par (2) et (1) :

$$n = \sum_{h=o}^{n-1} \alpha_h \quad \text{et} \quad \alpha_h \geqslant 1 \text{ pour } 0 \leqslant h \leqslant n-1$$

ce qui entraîne $\alpha_h = 1$ pour $0 \leqslant h \leqslant n-1$.

D'où, par (2) : $\dim N_k = k$ pour tout $k \in \mathbb{N}_n$. □

• ii) ⇒ iii) est trivial.

• Preuve de iii) ⇒ iv). Par hypothèse il existe $k \in \mathbb{N}_{n-1}$ tel que $\dim N_k = k$. Par (2) et (1), $\alpha_h = 1$ pour $0 \leqslant h \leqslant k-1$. En particulier, $\alpha_o = 1$. □

• Preuve de iv) ⇒ i). Par hypothèse $\alpha_o = 1$. La suite (α_k) étant décroissante, de (1) on déduit : $\alpha_h = 1$ pour $0 \leqslant h \leqslant r-1$. D'où, par (2) :

$$n = \dim E = \dim N_r = \sum_{h=o}^{r-1} \alpha_r = r.$$ □

3° Ici $E = N_n$ et $\dim N_k = k$ pour tout $k \in \{0, \ldots, n\}$.

Choisissons arbitrairement $e_n \in N_n \setminus N_{n-1}$ (i.e. e_n tel que $u^{n-1}(e_n) \neq 0$). Nous disposons, pour tout $k \in \mathbb{N}_n$, de $e_k = u^{n-k}(e_n)$, avec $e_k \in N_k \setminus N_{k-1}$, et nous avons $u(e_k) = e_{k-1}$ si $k \geqslant 2$ et $u(e_1) = 0$.

En raisonnant par récurrence, nous constatons que, pour tout $k \in \mathbb{N}_n$, $(e_1, \ldots, e_k)$ est une base de N_k ; en particulier $e = (e_1, \ldots, e_n)$ est une base de E, et $\operatorname{mat}(u; e) = J_n$. □

4.3.3 Soient E un $\mathbb{C}$-espace vectoriel de dimension finie $n > 0$, u et v deux endomorphismes de E vérifiant : $uv - vu = u$.

1° a) Montrer : $u^k v - v u^k = k u^k$ pour tout $k \in \mathbb{N}$.

b) En déduire que u est nilpotent.

2° On suppose ici que u est de rang n-1.

a) Montrer que v admet n valeurs propres simples de la forme :

$$\lambda_i = \alpha + i,\ i \in \mathbf{N}_n.$$

b) Soit e_n un vecteur propre de v associé à λ_n. Montrer que la famille $(e_i)_{1\leqslant i\leqslant n}$, avec $e_i = u^{n-i}(e_n)$ est une base de E.

Trouver les matrices de u et v dans cette base.

3° On revient au cas général.

a) Montrer que u et v admettent un vecteur propre commun.

b) Montrer qu'il existe une base de E dans laquelle u et v sont représentées par des matrices triangulaires supérieures.

Pour tout $k \in \mathbf{N}$, on note $N_k = \operatorname{Ker} u^k$.

1° a) Il s'agit de vérifier qu'une assertion $\mathcal{A}_k$ est vraie pour tout $k \in \mathbf{N}$.

- Il est clair que $\mathcal{A}_0$ et $\mathcal{A}_1$ sont vraies.
- Soit $k \in \mathbf{N}^*$ tel que : $u^k v - v u^k = k u^k$.

En composant à gauche par u, on en déduit :

$$u^{k+1} v - u v u^k = k u^{k+1}$$

et, compte tenu de $uv = vu + u$:

$$u^{k+1} v - v u^{k+1} = (k+1) u^{k+1}. \qquad \square$$

Remarque. Pour tout $k \in \mathbf{N}$, N_k est stable par v. En effet, compte tenu de $\mathcal{A}_k$, $u^k(y) = 0$ entraîne $u^k(v(y)) = 0$.

b) Puisque v est fixé on dispose de $\Phi : w \mapsto wv - vw$ qui est un endomorphisme de $\mathcal{L}(E)$. D'après $\mathcal{A}_k$, on a :

$$\forall k \in \mathbf{N} \quad \Phi(u^k) = k u^k$$

ce qui signifie que si $u^k \neq 0$, alors k est valeur propre de Φ. Comme $\mathcal{L}(E)$ est de dimension finie, Φ admet un nombre fini de valeurs propres, et il existe $k \in \mathbf{N}^*$ tel que $u^k = 0$; u est nilpotent.

2° Ici $\dim N_1 = 1$. D'après l'exercice précédent, l'indice de u est n, et $\dim N_k = k$ pour tout $k \in \{0, \ldots, n\}$.

a) Pour le moment, e_n est un élément arbitrairement choisi de $E \setminus N_{n-1}$.

Nous savons (toujours d'après l'exercice précédent) qu'en posant $e_k = u^{n-k}(e_n)$ pour tout $k \in \mathbf{N}_n$, $(e_1, \ldots, e_k)$ est une base de N_k et $e = (e_1, \ldots, e_n)$ est une base de E dans laquelle u est représenté par J_n, matrice nilpotente de Jordan d'ordre n.

- Compte tenu de la stabilité des N_k par v, $V = \operatorname{mat}(v; e)$ est triangulaire supérieure ; soient $\lambda_1, \ldots, \lambda_n$ ses éléments diagonaux.

- En écrivant que les éléments (i,j) où $j = i+1$ de $J_n V - V J_n$ et de J_n sont égaux nous obtenons : $\lambda_{i+1} - \lambda_i = 1$ pour tout $i \in \mathbb{N}_{n-1}$.

En posant $\alpha = \lambda_1 - 1$, nous constatons que v admet les n valeurs propres distinctes $\lambda_i = \alpha+i$, avec $i \in \mathbb{N}_n$.

Il en résulte que v est diagonalisable, et que, pour tout $k \in \mathbb{N}_n$, l'endomorphisme induit par v sur le sous-espace stable N_k est diagonalisable, de valeurs propres $\alpha+i$, avec $i \in \mathbb{N}_k$.

b) Choisissons arbitrairement un vecteur propre x de v associé à $\lambda_n = \alpha+n$.

Comme λ_n n'est pas valeur propre de l'endomorphisme de N_{n-1} induit par v, on a $x \notin N_{n-1}$. On peut donc considérer que tous les résultats obtenus en a) sont valables lorsque l'on adopte $e_n = x$.

• Montrons que, de plus, pour tout $i \in \mathbb{N}_n$, $e_i = u^{n-i}(e_n)$ est un vecteur propre de v associé à la valeur propre $\lambda_i = \alpha+i$.

Il s'agit de montrer qu'une assertion $\mathfrak{B}_i$ est vraie pour tout $i \in \mathbb{N}_n$. Nous allons opérer par récurrence descendante.

- $\mathfrak{B}_n$ est vraie d'après le choix de e_n.
- Soit $i \in \{2,\dots,n\}$, pour lequel : $v(e_i) = (\alpha+i)e_i$. On a :

$$v(e_{i-1}) = v(u(e_i)) = (uv-u)(e_i) = (\alpha+i-1)e_{i-1}.$$

Comme e_{i-1}, vecteur d'une base, n'est pas nul, c'est un vecteur propre de v associé à $\lambda_{i-1} = \alpha+i-1$. □

• La base e de E que nous venons d'obtenir est telle que :

$$\mathrm{mat}(v;e) = \mathrm{diag}(\alpha+1,\dots,\alpha+n) \text{ et } \mathrm{mat}(u;e) = J_n.$$

3°) a) $N_1 = \mathrm{Ker}\, u$ est non nul (car u est nilpotent) et stable par v (cf. 1°). L'endomorphisme du $\mathbb{C}$-espace vectoriel N_1 induit par v admet donc un vecteur propre y ; il est clair que y est vecteur propre de v, et aussi de u (puisque u(y) est nul).

b) Vérifions qu'est vraie pour tout $n \in \mathbb{N}^*$ ($n = \dim E$) l'assertion :

($\mathfrak{T}_n$) Si E est un $\mathbb{C}$-espace vectoriel de dimension n, pour tout couple (u,v) d'endomorphismes de E tel que uv-vu = u, il existe une base de E dans laquelle u et v sont représentés par des matrices triangulaires supérieures.

- Il est clair que $\mathfrak{T}_1$ est vraie.
- Soit $n \in \mathbb{N}^*$ pour lequel $\mathfrak{T}_n$ a été vérifiée. Considérons un $\mathbb{C}$-espace vectoriel E de dimension n+1, et $(u,v) \in (\mathcal{L}(E))^2$ tel que uv-vu = u.

On dispose de ε_1, vecteur propre commun à u et à v (cf. a)), tel que $u(\varepsilon_1) = 0$ et $v(\varepsilon_1) = \alpha\varepsilon_1$. Soit F, de dimension n, un supplémentaire de $\mathbb{C}\varepsilon_1$ dans E ; notons p le projecteur de E d'image F, de noyau $\mathbb{C}\varepsilon_1$.

On dispose des deux endomorphismes de F :

$$u_1 : x \mapsto p(u(x)) \; ; \; v_1 : x \mapsto p(v(x)).$$

Soit $\varepsilon = (\varepsilon_2,\ldots,\varepsilon_{n+1})$ une base arbitrairement choisie de F ; on dispose de la base $\omega = (\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{n+1})$ de E. On constate que, en notant :

$$U = \mathrm{mat}(u;\omega)\ ;\ V = \mathrm{mat}(v;\omega)\ :\ U_1 = \mathrm{mat}(u_1;\varepsilon)\ ;\ V_1 = \mathrm{mat}(v_1;\varepsilon)$$

on a :

$$U = \left[\begin{array}{c|ccc} 0 & \star & \cdots & \star \\ \hline 0 & & & \\ \vdots & & U_1 & \\ 0 & & & \end{array}\right] \quad ; \quad V = \left[\begin{array}{c|ccc} \alpha & \star & \cdots & \star \\ \hline 0 & & & \\ \vdots & & V_1 & \\ 0 & & & \end{array}\right]$$

et que : uv-vu = u implique $U_1V_1 - V_1U_1 = U_1$, et donc :

$$u_1v_1 - v_1u_1 = u_1 .$$

D'après $\mathfrak{T}_n$ appliquée à (F,u_1,v_1), il existe une base $(\varepsilon_2',\ldots,\varepsilon_{n+1}')$ de F dans laquelle les matrices de u_1 et v_1 sont triangulaires supérieures ; dans la base $(\varepsilon_1,\varepsilon_2',\ldots,\varepsilon_n')$ de E les matrices de u et v sont triangulaires supérieures.

Remarque. En utilisant la réduction de Jordan, on peut prolonger l'exercice par : u étant un endomorphisme de E, pour que tout $v \in \mathcal{L}(E)$ tel que uv-vu = u soit diagonalisable, il faut et il suffit que u soit de rang n-1.

4.3.4 Pour tout couple (A,B) de (n,n) matrices complexes, prouver l'équivalence des deux assertions :

i) Pour toute $M \in \mathcal{M}_n(\mathbb{C})$, AM et AM+B ont le même polynôme caractéristique.

ii) B est nilpotente et BA = 0.

1° Preuve de i) ⇒ ii). Par hypothèse i) est vraie.

- Par M = 0 on constate : $\chi_B = \chi_0 = X^n$; B est donc nilpotente.

- Pour toute $P \in \mathcal{M}_n(\mathbb{C})$ de polynôme caractéristique

$$X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \ldots = \prod_{k=1}^{n} (X-\lambda_k)$$

on a : $\mathrm{tr}\ P = \lambda_1 + \ldots + \lambda_n = \sigma_1$, et par trigonalisation

$$\mathrm{tr}\ P^2 = \lambda_1^2 + \ldots + \lambda_n^2 = \sigma_1^2 - 2\sigma_2 .$$

D'où :

$$\forall M \in \mathcal{M}_n(\mathbb{C}) \quad \mathrm{tr}(AM+B)^2 = \mathrm{tr}(AM)^2 .$$

En utilisant $\mathrm{tr}(U\,V) = \mathrm{tr}(V\,U)$, la linéarité de la trace, et $\mathrm{tr}\ B^2 = 0$ (conséquence de ce que B est nilpotente), il vient :

$$\forall M \in \mathcal{M}_n(\mathbb{C}) \quad \mathrm{tr}(BAM) = 0 \qquad (1)$$

ce qui s'écrit, en utilisant la base canonique (E_{ij}) de $\mathcal{M}_n(\mathbb{C})$:

$$\forall (i,j) \in \mathbb{N}_n^2 \quad \mathrm{tr}(BAE_{ij}) = 0 \qquad (2)$$

Or on vérifie que $tr(BAE_{ij})$ est l'élément (j,i) de la matrice BA ; (2) s'écrit donc BA = 0. □

2° Preuve de ii) ⇒ i). Par hypothèse, B est nilpotent et BA = 0.

Soient u et v les endomorphismes de $\mathbb{C}^n$ représentés par A et B dans la base canonique ; v est nilpotent et vu = 0.

Comme y = u(x) entraîne v(y) = vu(x) = 0, on a : Im u ⊂ Ker v.

On note r = dim(Im u) et p = dim(Ker v), avec $p \geqslant r$.

On peut donc partir d'une base de Im u, la compléter en une base de Ker v, et, par trigonalisation, compléter celle-ci en une base e de $\mathbb{C}^n$ dans laquelle v est représenté par une matrice B' triangulaire supérieure et nilpotente (la diagonale de B' est nulle et ses p premières colonnes sont nulles).

A' = mat(u;e) a ses n-r dernières lignes nulles. On a donc :

$$A' = \left[\begin{array}{c|c} A_1 & A_2 \\ \hline 0 & 0 \end{array}\right] \quad \text{et} \quad B' = \left[\begin{array}{c|c} 0 & B_2 \\ \hline 0 & B_4 \end{array}\right]$$

avec $A_1 \in \mathcal{M}_r(\mathbb{C})$, et $B_4 \in \mathcal{M}_{n-r}(\mathbb{C})$ triangulaire supérieure à diagonale nulle (les p-r premières colonnes de B_4 sont d'ailleurs nulles).

Il suffit d'établir que, pour toute $M' \in \mathcal{M}_n(\mathbb{C})$, les matrices A'M' et A'M' + B' ont le même polynôme caractéristique. On pose :

$$M' = \left[\begin{array}{c|c} M_1 & M_2 \\ \hline M_3 & M_4 \end{array}\right] \quad \text{avec } M_1 \in \mathcal{M}_r(\mathbb{C}) .$$

A'M' et A'M' + B' sont respectivement de la forme :

$$\left[\begin{array}{c|c} P & Q \\ \hline 0 & 0 \end{array}\right] \quad \text{et} \quad \left[\begin{array}{c|c} P & Q+B_2 \\ \hline 0 & B_4 \end{array}\right] \quad \text{avec } P \in \mathcal{M}_r(\mathbb{C}).$$

Leurs polynômes caractéristiques sont, l'un et l'autre : $\chi_P X^{n-r}$. □

• *Les deux exercices qui suivent sont des parties de problèmes de concours.*

4.3.5 On donne $A \in \mathcal{M}_n(\mathbb{R})$. Soit $\mathfrak{S}$ l'ensemble des $X \in \mathcal{M}_n(\mathbb{R})$ vérifiant :

i) $(AX = XA) \wedge (X^2A = X)$;

et : ii) Il existe $j \in \mathbb{N}$ tel que $A^{j+1}X = A^j$.

On se propose de justifier $\mathfrak{S} = \{A'\}$ et de calculer A'.

1° a) Etablir : $X^{\ell+1}A^{\ell} = X$ pour tous $X \in \mathfrak{S}$ et $\ell \in \mathbb{N}$.

b) Soit $(X,Y) \in \mathfrak{S}^2$. Pour m assez grand, comparer $X^{m+1}A^{m+1}Y$ et $YA^{m+1}X^{m+1}$. En déduire que $\mathfrak{S}$ a au plus un élément.

c) Déterminer $\mathfrak{A}$ lorsque A est nilpotente (resp. inversible).

2° Ici A n'est ni nilpotente, ni inversible. Soit $u \in \mathcal{L}(\mathbb{R}^n)$ représenté par A dans la base canonique de $\mathbb{R}^n$.

a) Montrer que la suite $(\operatorname{Ker} u^h)_{h\in\mathbb{N}}$ est stationnaire à partir d'un certain indice k, que $\mathbb{R}^n = \operatorname{Im} u^k \oplus \operatorname{Ker} u^k$, et que le rang s de u^k vérifie : $1 \leqslant s \leqslant n-k \leqslant n-1$.

b) Montrer qu'il existe $R \in GL_n(\mathbb{R})$ telle que

$$A = R \left[\begin{array}{c|c} C & 0 \\ \hline 0 & N \end{array}\right] R^{-1}, \text{ où } C \in GL_s(\mathbb{R}) \text{ et } N^k = 0_{n-s} \qquad (1)$$

En déduire que $\mathfrak{A} = \{A'\}$, où A' s'exprime au moyen de R et C (on pourra traiter d'abord le cas où k = 1).

c) Comparer les valeurs propres de A' à celles de A.

• Soit Q le polynôme caractéristique de C. Montrer qu'il existe $(U,V) \in (\mathbb{R}[X])^2$, tel que

$$UQ + VX^{k+1} = 1, \text{ avec } \deg V < s. \qquad (2)$$

• Montrer qu'il existe $P \in \mathbb{R}[X]$ tel que $P(A) = A'$ et exprime P à l'aide de V.

d) Décrire une méthode de calcul de A', et l'appliquer au cas de :

$$A = \left[\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{array}\right].$$

1° a) On fixe $X \in \mathfrak{A}$, et on vérifie qu'une assertion $\mathcal{A}_\ell$ est vraie pour tout $\ell \in \mathbb{N}$.

- Il est clair que $\mathcal{A}_0$, qui s'écrit $X = X$, est vraie.
- Supposant $\mathcal{A}_\ell$ vérifiée, on a (en utilisant $X^2A = X$) :

$$X^{\ell+2}A^{\ell+1} = X^\ell X^2 A\, A^\ell = X^{\ell+1}A^\ell = X$$

ce qui montre que $\mathcal{A}_{\ell+1}$ est vérifiée. □

b) Soient j et j' associés par ii) à $Y \in \mathfrak{A}$ et $X \in \mathfrak{A}$; en notant $m = \max(j,j')$ et en utilisant i), ii) et a), on obtient :

$$X^{m+1}A^{m+1}Y = X^{m+1}A^{m-j}A^{j+1}Y = X^{m+1}A^m = X \qquad (3)$$

et : $$YA^{m+1}X^{m+1} = A^{m-j}A^{j+1}YX^{m+1} = A^mX^{m+1} = X$$

et : $$X = YA^{m+1}X^{m+1} = Y^{m+1}A^{2m+1}X^{m+1} = Y^{m+1}A^{m+1}X.$$

En transposant X et Y dans (3) : $Y^{m+1}A^{m+1}X = Y$. D'où $X = Y$. □

c) Si A est nilpotente, i.e. s'il existe $j \in \mathbb{N}$ tel que $A^j = 0$, il est clair que $0 \in \mathfrak{G}$ et donc, compte tenu de l'unicité, que $\mathfrak{G} = \{0\}$.

• Si A est inversible, on a $A^{-1} \in \mathfrak{G}$ (avec j quelconque dans ii)) et $\mathfrak{G} = \{A^{-1}\}$.

2° a) Pour tout $u \in \mathcal{L}(E)$, où $\dim E < +\infty$, la théorie des noyaux itérés fournit l'existence de $k \in \mathbb{N}$ tel que, avec des inclusions strictes :

$$\{0\} \subset \operatorname{Ker} u \subset \ldots \subset \operatorname{Ker} u^k, \text{ et } \operatorname{Ker} u^h = \operatorname{Ker} u^k \text{ pour } h \geqslant k.$$

En utilisant $\dim(\operatorname{Ker} u^h) \geqslant 1 + \dim(\operatorname{Ker} u^{h-1})$ pour $1 \leqslant h \leqslant k$, il vient :

$$k \leqslant \dim(\operatorname{Ker} u^k) = n - s, \text{ où } n = \dim E \text{ et } s = \dim(\operatorname{Im} u^k).$$

• On a : $\operatorname{Im} u^k \cap \operatorname{Ker} u^k = \{0\}$; en effet si $x = u^k(y)$ et $u^k(x) = 0$, alors $u^{2k}(y) = 0$, et $u^k(y) = 0$ et $x = 0$. Compte tenu de la somme n des dimensions :

$$\operatorname{Im} u^k \oplus \operatorname{Ker} u^k = E.$$

• Ici $E = \mathbb{R}^n$; u est non nilpotent et donc $\operatorname{Im} u^k \neq \{0\}$, i.e. $1 \leqslant s$; en outre u est non inversible et donc $\operatorname{Ker} u \neq \{0\}$, i.e. $1 \leqslant k$. □

b) Comme u et u^k commutent, $\operatorname{Im} u^k$ et $\operatorname{Ker} u^k$ sont stables par u, qui induit donc des endomorphismes v et w de $\operatorname{Im} u^k$ et $\operatorname{Ker} u^k$. Soit e une base de $\mathbb{R}^n$ obtenue par réunion d'une base e' de $\operatorname{Im} u^k$ et d'une base e'' de $\operatorname{Ker} u^k$. On a :

$$\operatorname{mat}(u;e) = \left[\begin{array}{c|c} C & 0 \\ \hline 0 & N \end{array}\right], \text{ où } C = \operatorname{mat}(v;e') \text{ et } N = \operatorname{mat}(w;e'').$$

L'endomorphisme v^k de $\operatorname{Im} u^k$ est induit par u^k ; son noyau est nul, et il est bijectif ($\dim \operatorname{Im} u^k < +\infty$) ; sa matrice C^k est inversible ; comme $k \geqslant 1$, C est inversible, i.e. $C \in GL_s(\mathbb{R})$.

L'endomorphisme w^k de $\operatorname{Ker} u^k$ est induit par u^k, et donc nul ; d'où $N^k = 0_{n-s}$. On a ainsi (1), avec $R = P_\varepsilon^e$, où ε est la base canonique de $\mathbb{R}^n$.

• C étant inversible dans $GL_s(\mathbb{R})$, on dispose de l'ensemble $\mathcal{G} \subset \mathcal{M}_n(\mathbb{R})$ des matrices de la forme :

$$M_p = R \left[\begin{array}{c|c} C^p & 0 \\ \hline 0 & 0 \end{array}\right] R^{-1}, \quad p \in \mathbb{Z}.$$

Par multiplication de matrices blocs, on établit :

$$\forall (p,q) \in \mathbb{Z}^2 \quad M_p M_q = M_q M_p = M_{p+q} \tag{4}$$

On en déduit que $(\mathcal{G}, .)$ est un groupe commutatif isomorphe à $(\mathbb{Z}, +)$; ce n'est pas un sous-groupe de $GL_n(\mathbb{R})$ à cause de $s < n$.

D'autre part, on établit :

$$A^p = R \begin{bmatrix} C^p & 0 \\ 0 & N^p \end{bmatrix} R^{-1}, \quad p \in \mathbb{N}.$$

D'où $A^p = M_p$ pour $p \geqslant k$. Dans (4) on peut donc remplacer M_p par A^p pour $p \geqslant k$. On constate que le résultat ainsi obtenu s'étend sous la forme :

$$\forall (p,q) \in \mathbb{N} \times \mathbb{Z} \quad A^p M_q = M_q A^p = M_{p+q} \tag{5}$$

Le résultat du 1° c), conduit à étudier M_{-1} (qui est l'inverse de A dans $\mathcal{G}$ lorsque k = 1). *Quel que soit* k, on établit, grâce à (5) :

$$(AM_{-1} = M_{-1}A) \wedge \left((M_{-1})^2 A = M_{-1}\right)$$

et : $A^{k+1} M_{-1} = A^k$ (car $M_k = A^k$).

D'où : $M_{-1} \in \mathcal{E}$ (avec j = k dans ii)), et $\mathcal{E} = \{A'\}$, où $A' = M_{-1}$.

c) Le polynôme caractéristique de N, qui est nilpotente, est X^{n-s}.

Les polynômes caractéristiques de A et A' sont donc $X^{n-s}Q$ et $X^{n-s}Q_1$, où Q et Q_1 sont les polynômes caractéristiques de C et C^{-1} $\left(Q(0) \neq 0 \text{ et } Q_1(0) \neq 0\right)$.

Dans $\mathcal{M}_s(\mathbb{R}(X))$, où $\mathbb{R}(X)$ est un corps de fractions rationnelles, on a :

$$XI_s - C^{-1} = -C^{-1}X\left(\frac{1}{X} I_s - C\right).$$

D'où : $$Q_1(X) = (-1)^s \frac{1}{\det C} X^s Q\left(\frac{1}{X}\right).$$

Au total, A et A' admettent toutes deux la valeur propre 0 de même multiplicité n-s ; $\lambda \neq 0$ est valeur propre de multiplicité m de A' si, et seulement si λ^{-1} est valeur propre de multiplicité m de A.

• D'après $Q(0) \neq 0$, Q et X^{k+1} sont premiers entre eux ; le degré de Q est s. Le théorème de Bezout fournit l'existence et l'unicité de (U,V).

• De l'expression (déjà utilisée) de A^p pour $p \geqslant 0$, on déduit :

$$P(A) = R \begin{bmatrix} P(C) & 0 \\ 0 & P(N) \end{bmatrix} R^{-1} \text{ pour tout } P \in \mathbb{R}[X].$$

Il en résulte que P(A) = A' s'écrit : $\left(P(C) = C^{-1}\right) \wedge \left(P(N) = 0\right)$.

Cette dernière condition est vérifiée par $P(X) = X^k V(X)$. En effet on a alors P(N) = 0 à cause de $N^k = 0$; d'autre part, on a :

$$U(C)Q(C) + V(C)C^{k+1} = I_s$$

ce qui, associé à Q(C) = 0 (Cayley-Hamilton), fournit $P(C) = C^{-1}$.

En conclusion : $A' = A^k V(A)$, ce qui va permettre le calcul de A'.

d) Si $\det A \neq 0$, on sait calculer $A' = A^{-1}$. Sinon :

- On calcule le polynôme caractéristique χ de A, et on écrit, de façon unique, $\chi = X^{n-s}Q$, avec $Q(0) \neq 0$, ce qui fournit Q et $s \leqslant n-1$ $(\det A = 0)$.

Si $s = 0$, alors $\chi = X^n$, et $A^n = 0$, et $A' = \{0\}$ sinon :

- On détermine $k = \min\{h \in \mathbb{N} \mid \operatorname{rg} A^h = s\}$.
- On détermine le couple (U,V) qui vérifie (2). On a :

$$A' = A^k V(A). \qquad \square$$

• Dans le cas particulier considéré, il est clair que $\det A = 0$.

- On a (pratiquement sans calcul): $\chi = X^2(X-1)^2$; $s = 2$ et $Q = (X-1)^2$.
- De $\begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} \neq 0$, on déduit $\operatorname{rg} A = s+1$. D'où : $s \leqslant \operatorname{rg} A^2 \leqslant s$, et ici $k = s = 2$.
- Par identification, on trouve :

$$(3X^2+2X+1)(X-1)^2 + (-3X+4)X^3 = 1.$$

D'où : $V = -3X+4$, et $A' = -3A^3+4A^2$. On calcule :

$$A' = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 4 & 3 & 2 & 1 \\ -3 & -2 & -1 & 0 \end{bmatrix}.$$

Remarque. Le calcul de U et V peut aussi se faire par division suivant les puissances croissantes de 1 par Q.

4.3.6 On note J_n, $n \in \mathbb{N}^*$, la (n,n) matrice complexe dans laquelle l'élément (i,j) est 1 si $j = i+1$ et 0 sinon (matrice nilpotente de Jordan).

• Pour $A \in \mathcal{M}_n(\mathbb{C})$ donné, on cherche s'il existe $(B,C) \in (\mathcal{M}_n(\mathbb{C}))^2$ tel que :

$$(A = BC) \wedge (B^2 = C^2 = I_n) \qquad (1)$$

1° Ici A est $A_n = I_n + J_n$. Montrer qu'il existe une solution (B_n, C_n) avec :

$$C_n = [\gamma_{ij}], \text{ où } \gamma_{ij} = (-1)^i C_{n-i}^{n-j} \quad \text{(et donc 0 si } i > j).$$

2° Dans le cas général, montrer que si le problème admet une solution, alors A est inversible et semblable à A^{-1}.

3° Inversement soient $A \in \mathcal{M}_n(\mathbb{C})$ inversible et semblable à A^{-1}, et $u \in \mathcal{L}(\mathbb{C}^n)$ représenté par A dans la base canonique de $\mathbb{C}^n$.

a) On suppose ici que u admet une valeur propre unique λ et que le sous-espace propre associé E_λ est de dimension 1. Montrer que le problème admet une solution.

b) On suppose ici que u admet exactement deux valeurs propres distinctes λ et μ, que $\lambda^2 \neq 1$ et que le sous-espace propre E_λ associé à λ est de dimension 1.

En utilisant les restrictions de u aux sous-espaces caractéristiques W_λ et W_μ associés respectivement à λ et μ, montrer que A est semblable à une matrice qui s'exprime simplement en fonction de λ et de A_p, où p est un entier convenablement choisi, et où $A_p = I_p + J_p$.

Montrer qu'ici encore le problème admet une solution.

1° Commençons par montrer que le carré de C_n est I_n.

Pour tout vecteur de $\mathbb{C}^n$ de la forme $V_a = {}^t[a^{n-1}a^{n-2}\ldots 1]$, on a :

$$C_n V_a = {}^t[-(a+1)^{n-1}\ (a+1)^{n-2}\ldots(-1)^n]$$

et : $$(C_n)^2 V_a = {}^t[(a+1-1)^{n-1}\ (a+1-1)^{n-2}\ldots 1] = V_a.$$

L'endomorphisme de $\mathbb{C}^n$ représenté par $(C_n)^2$ dans la base canonique conserve donc la famille $(V_1,\ldots V_n)$ qui est une base de $\mathbb{C}^n$, puisque son déterminant dans la base canonique est (au signe près) le déterminant de Vandermonde du n-uple $(1,\ldots,n)$ dont les éléments sont deux à deux distincts ; cet endomorphisme est donc l'identité de $\mathbb{C}^n$, et $(C_n)^2 = I_n$.

- Compte tenu de $(C_n)^2 = I_n$, $A_n = BC_n$ équivaut à $B = A_n C_n$.

  Posant $B_n = A_n C_n$, nous avons donc à prouver $(B_n)^2 = I_n$.

- C'est vrai si $n=1$, car alors $A_n = [1]$, $C_n = [-1]$ et $B_n = [-1]$.

- Pour $n \geqslant 2$, on écrit : $B_n = [\beta_{ij}]$ avec $\beta_{ij} = (-1)^i\left(C_{n-i}^{n-j} - C_{n-i-1}^{n-j}\right)$.

  Si $i \leqslant n-1$ et $j \leqslant n-1$, $\beta_{ij} = (-1)^i\, C_{n-i-1}^{n-j-1}$ est l'élément de (i,j) de la matrice C_{n-1} ; si $(i,j) = (i,n)$ avec $i \leqslant n-1$, ou si $(i,j) = (n,j)$ avec $j \leqslant n-1$, alors $\beta_{ij} = 0$; enfin $\beta_{nn} = (-1)^n$. D'où :

$$B_n = \left[\begin{array}{c|c} C_{n-1} & 0 \\ \hline 0 & (-1)^n \end{array}\right] \text{ et donc : } (B_n)^2 = \left[\begin{array}{c|c} I_{n-1} & 0 \\ \hline 0 & 1 \end{array}\right] = I_n. \quad \square$$

2° S'il existe une solution (B,C), alors B et C sont leurs propres inverses, et il existe $A^{-1} = C^{-1}B^{-1} = CB$. On a :

$$C^{-1}A^{-1}C = C^{-1}CBC = BC = A$$

ce qui montre que A et A^{-1} sont semblables. $\square$

3° Soient λ une valeur propre de u ($\lambda \neq 0$ car u est inversible) et E_λ le sous-espace propre associé. Pour tout $x \in E_\lambda$, on a :

$$u(x) = \lambda x, \text{ et donc } u^{-1}(x) = \lambda^{-1}x,$$

et, comme $u^{-1} = p^{-1}up$, où $p \in GL(\mathbb{C}^n)$:

$$p^{-1}u(p(x)) = \lambda^{-1}x, \quad \text{et } u(p(x)) = \lambda^{-1}p(x).$$

On en déduit que λ^{-1} est valeur propre de u, et, compte tenu de $p \in GL(\mathbb{C}^n)$, que le sous-espace propre associé est $p(E_\lambda)$, dont la dimension est celle de E_λ.

a) Ici le polynôme caractéristique de u est $(X-\lambda)^n$. Par Cayley-Hamilton, on déduit que $v = \lambda^{-1}u - I$, où I est l'identité de $\mathbb{C}^n$, vérifie $v^n = 0$. En outre, il est clair que $\operatorname{Ker} v = E_\lambda$, de dimension 1.

D'après l'exercice 4.3.2, 3°, il existe une base e de $\mathbb{C}^n$ telle que (en reprenant les matrices J_n, A_n, B_n et C_n du 1°) : $\operatorname{mat}(v;e) = J_n$, et donc :

$$\operatorname{mat}(\lambda^{-1}u;e) = A_n \ ; \ \operatorname{mat}(u;e) = \lambda A_n.$$

P désignant la matrice de passage de la base canonique à la base e, on a :

$$A = \lambda P A_n P^{-1} = \lambda P B_n C_n P^{-1}, \text{ avec } (B_n)^2 = (C_n)^2 = I_n.$$

D'où : $A = BC$, avec $B = \lambda P B_n P^{-1}$ et $C = P C_n P^{-1}$.

On constate : $C^2 = I_n$. D'autre part, l'unicité de la valeur propre de A fait qu'ici $\lambda^{-1} = \lambda$, i.e. $\lambda^2 = 1$, ce qui entraîne $B^2 = I_n$. □

b) Ici $\lambda^2 \neq 1$ entraîne $\lambda^{-1} \neq \lambda$, et donc $\mu = \lambda^{-1}$.

Les endomorphismes u et u^{-1}, représentés dans la base canonique par des matrices semblables, ont un polynôme caractéristique commun :

$$\chi = (X-\lambda)^p (X-\mu)^q, \text{ avec } p+q = n.$$

En utilisant une base de $\mathbb{C}^n$ qui trigonalise u, et en remarquant que cette base trigonalise u^{-1}, on constate (ici très simplement) qu'au titre de polynôme caractéristique de u^{-1}, χ s'écrit : $(X-\lambda^{-1})^p (X-\mu^{-1})^q$.

Compte tenu de $\mu = \lambda^{-1}$, on en déduit : $p = q$ et $2p = n$ (ce qui montre qu'ici n est pair). Dans la suite, μ est mis pour λ^{-1}.

$\mathbb{C}^n$ est somme directe de $W_\lambda = \mathrm{Ker}(u-\lambda I)^p$ et $W_\mu = \mathrm{Ker}(u-\mu I)^p$, tous deux stables par u, ce qui permet d'introduire les endomorphismes induits u' et u" ; on a $(u'-\lambda I')^p = 0$ et $(u''-\mu I'')^p = 0$.

D'autre part les noyaux E_λ de $u-\lambda I$ et E_μ de $u-\mu I$, de dimension 1, sont respectivement inclus dans W_λ et W_μ, et sont ainsi les noyaux de $u'-\lambda I'$ et $u''-\mu I''$. Le raisonnement fait au début de a) s'applique à u' et à u". Il existe une base e' de W_λ et une base e" de W_μ telles que :

$$\mathrm{mat}(u';e') = \lambda A_p \ ; \ \mathrm{mat}(u'';e'') = \mu A_p.$$

Réunissant e' et e" en une base e de $\mathbb{C}^n$, on obtient :

$$\mathrm{mat}(u;e) = \left[\begin{array}{c|c} \lambda A_p & 0 \\ \hline 0 & \mu A_p \end{array}\right], \text{ avec } n = 2p \text{ et } \mu = \lambda^{-1}.$$

En utilisant $A_p = B_p C_p$, avec $B_p^2 = C_p^2 = I_p$, on constate :

$$\mathrm{mat}(u;e) = B'C', \text{ où } B' = \left[\begin{array}{c|c} 0 & \lambda B_p \\ \hline \mu B_p & 0 \end{array}\right] \text{ et } C' = \left[\begin{array}{c|c} 0 & C_p \\ \hline C_p & 0 \end{array}\right].$$

Compte tenu de $\lambda\mu = 1$, on calcule $B'^2 = C'^2 = I_n$.

P désignant la matrice de passage de la base canonique à la base e, on a :

$$A = BC, \text{ avec } B = PB'P^{-1}, \ C = PC'P^{-1}, \text{ et } B^2 = C^2 = I_n. \quad \square$$

4.3.7 Soit u un endomorphisme d'un K-espace vectoriel E de dimension finie $n>0$. A tout $x \in E$ on associe :

$$I_x = \{P \in K[X] \mid P(u)(x) = 0_E\}.$$

1° a) Soit $x \in E$. Montrer que I_x est un idéal non nul de $K[X]$; on dispose donc d'un unique polynôme normalisé μ_x tel que $I_x = \mu_x K[X]$.

b) Dans quels cas a-t-on $\mu_x = 1$ (resp. $\deg \mu_x = 1$) ?

2° Soit $(x,y) \in E^2$. Montrer que si $\mu_x \wedge \mu_y = 1$, alors $\mu_{x+y} = \mu_x \mu_y$.

3° Montrer qu'il existe $x \in E$ tel que $\mu_x = \mu$, où μ est le polynôme minimal de u.

1° a) $\varphi : P \longrightarrow P(u)$ est un morphisme d'algèbres de $K[X]$ dans $\mathcal{L}(E)$.

Pour $x \in E$ donné, $v \longmapsto v(x)$ est une application linéaire de $\mathcal{L}(E)$ dans E.

Par composition $P \longmapsto P(u)(x)$ est une application linéaire de $K[X]$ dans E.

I_x, qui en est le noyau, est ainsi un sous-groupe additif de $K[X]$.

Par ailleurs, pour tous $P \in I_x$ et $Q \in K[X]$:

$$(QP)(u)(x) = Q(u)[P(u)(x)] = Q(u)(0) = 0, \text{ et } QP \in I_x.$$

I_x est ainsi un idéal de $K[X]$; contenant l'idéal annulateur de u, I_x n'est pas réduit à zéro. □

Notons que les polynômes minimal et caractéristique de u sont des éléments de I_x, et donc des multiples de μ_x.

b) $\mu_x = 1$ s'écrit $I_x = K[X]$ et exige $u^0(x) = 0$, i.e. $x = 0$. Inversement, si $x = 0$, il est clair que $I_x = K[X]$ et donc que $\mu_x = 1$.

• Pour que $\mu_x = X - \lambda$, il faut et il suffit que :

$$[(u - \lambda Id_E)(x) = 0] \wedge [x \neq 0].$$

On a donc $\deg \mu_x = 1$ si, et seulement si x est vecteur propre de u.

2° Pour tout $(x,y) \in E^2$, on a :

$$(\mu_x \mu_y)(u)(x+y) = (\mu_y \mu_x)(u)(x) + (\mu_x \mu_y)(u)(y) = 0$$

et donc : μ_{x+y} divise $\mu_x \mu_y$. En outre :

$$(\mu_y \mu_{x+y})(u)(x) = (\mu_y \mu_{x+y})(u)(x+y-y)$$
$$= (\mu_{x+y} \mu_y)(-y) = 0$$

et donc : μ_x divise $\mu_y \mu_{x+y}$.

• Supposons maintenant que $\mu_x \wedge \mu_y = 1$. Il en résulte que μ_x divise μ_{x+y}. Symétriquement, μ_y divise μ_{x+y} ; et donc $\mu_x \mu_y$ divise μ_{x+y}. Compte tenu de :

μ_{x+y} divise $\mu_x \mu_y$, et de ce qu'il s'agit de polynômes normalisés :

$$\mu_{x+y} = \mu_x \mu_y.$$

3° Considérons la décomposition $\mu = \prod_{i=1}^{p} P_i^{r_i}$, $r_i \geqslant 1$, où les P_i sont des polynômes irréductibles, normalisés et deux à deux distincts. Les $P_i^{r_i}$ sont premiers entre eux deux à deux et, compte tenu de $\mu(u) = 0$, le lemme des noyaux donne :

$$E = \bigoplus_{i=1}^{p} N_i, \text{ où } N_i = \operatorname{Ker} P_i^{r_i}(u).$$

Pour $i \in \mathbb{N}_p$ donné, écrivons $\mu = P_i Q_i$, où $Q_i = P_i^{r_i-1} \prod_{j\neq i} P_j^{r_j}$.

En utilisant encore le lemme des noyaux, il vient :

$$\operatorname{Ker} Q_i(u) = \operatorname{Ker} P_i^{r_i-1}(u) \oplus G_i, \text{ où } G_i = \bigoplus_{j\neq i} N_j.$$

A cause de $\deg P_i \geqslant 1$, Q_i n'est pas un multiple de μ ; on a $Q_i(u) \neq 0$ et $\operatorname{Ker} Q_i(u) \neq E$; d'où l'inclusion stricte de $\operatorname{Ker} P_i^{r_i-1}(u)$ dans N_i.

Il existe donc $x_i \in \operatorname{Ker} P_i^{r_i}(u) \setminus \operatorname{Ker} P_i^{r_i-1}(u)$, ce qui implique $x_i \neq 0$. On a :

$$P_i^{r_i} \in I_{x_i} \quad \text{et} \quad P_i^{r_i-1} \notin I_{x_i}.$$

μ_{x_i} divise $P_i^{r_i}$ sans diviser $P_i^{r_i-1}$, ce qui entraîne $\mu_{x_i} = P_i^{r_i}$. D'où $\mu = \prod_{i=1}^{p} \mu_{x_i}$, les μ_{x_i} étant premiers entre eux deux à deux. En utilisant 2°, on en déduit par récurrence : $\mu = \mu_x$, où $x = x_1 + \ldots + x_p$.

Remarque. De $\mu_{x_i}(u)(x_i) = 0$ et $x_i \neq 0$, on déduit que $\mu_{x_i}(u) = P_i^{r_i}(u)$ est non injectif, ce qui exige que $P_i(u)$ soit non injectif (pour tout $i \in \mathbb{N}_n$).

• *Les résultats de l'exercice précédent seront utilisés dans l'exercice qui suit, lequel a de nombreuses applications.*

4.3.8 SOUS-ESPACES CYCLIQUES ; ENDOMORPHISMES CYCLIQUES. On considère un K-espace vectoriel E de dimension finie $n>0$ et un endomorphisme u de E.

1° Soit $x \in E \setminus \{0\}$. On lui associe $F_x = \operatorname{Vect}\left(u^i(x)\right)_{i\in\mathbb{N}}$ et on dit que F_x est le *sous-espace cyclique* de E associé à u et engendré par x.

On note : $k_x = \max\{r \in \mathbb{N}^* \mid (x, u(x), \ldots, u^{r-1}(x)) \text{ est libre}\}$.

a) Montrer que F_x admet la base $e_x = \left(u^i(x)\right)_{0\leqslant i<k_x}$ et qu'il est stable par u.

b) Exprimer le polynôme caractéristique de l'endomorphisme v_x de F_x induit par u en utilisant les coordonnées de $u^{k_x}(x)$ dans la base e_x. Le comparer au polynôme normalisé μ_x qui engendre l'idéal $I_x = \{P \in K[X] \mid P(u)(x) = 0\}$ de $K[X]$ étudié dans l'exercice précédent.

2° Déduire du 1° une démonstration du théorème de Cayley-Hamilton.

3° Prouver que les deux assertions suivantes sont équivalentes :

i) Il existe $x \in E \setminus \{0\}$ tel que E soit le sous-espace cyclique associé à u et engendré par x (on dit alors que u est un *endomorphisme cyclique*).

ii) Les polynômes caractéristique et minimal, χ et μ, de u sont égaux.

4° Montrer que tout polynôme irréductible de $K[X]$ qui divise χ divise μ.

1° Dans cette question, $x \in E \setminus \{0\}$ est fixé et on peut, pour alléger la notation, écrire k au lieu de k_x, qui existe au titre de plus grand élément d'une partie de $\mathbb{N}$ qui n'est pas vide (puisqu'elle contient 1) et qui est majorée par n (puisqu'une famille de n+1 éléments de E est liée). On a $k \in \mathbb{N}_n$.

a) D'après la définition de k, la famille e_x est libre et la famille $(u^i(x))_{0 \leqslant i \leqslant k}$ est liée ; $u^k(x)$ est donc une combinaison linéaire des éléments de e_x ; on vérifie par récurrence qu'il en est de même pour tout $u^i(x)$, $i \geqslant k$. Il en résulte que e_x est une base de F_x (qui est ainsi de dimension k) et que F_x est stable par u.

b) Posons $u^k(x) = \sum_{i=0}^{k-1} \alpha_i u^i(x)$ (1)

La matrice de v_x dans la base e_x de F_x s'écrit :

$$A = \begin{bmatrix} 0 & & & \alpha_0 \\ 1 & & 0 & \alpha_1 \\ & \ddots & & \vdots \\ & 0 & & \\ & & 0 & \alpha_{k-2} \\ & & 1 & \alpha_{k-1} \end{bmatrix} \qquad (2)$$

(On dit que A est une matrice-compagnon de Jordan).

Dans $\det(XI_k - A)$ on remplace la ligne L_1 par $\sum_{i=0}^{k-1} X^i L_{i+1}$, et on développe suivant la nouvelle première ligne, dont tous les éléments sont nuls, sauf le dernier. Le polynôme caractéristique de v_x est ainsi :

$$\chi_{v_x} = \chi_A = X^k - \sum_{i=0}^{k-1} \alpha_i X^i.$$

• Notons que, d'après (1), $\chi_A(u)(x) = 0$, et donc $\chi_A \in I_x$.

Comme la famille e_x est libre, aucun polynôme non nul de degré strictement inférieur à k n'appartient à I_x. On a donc $\deg \mu_x \geqslant k$. Comme en outre le polynôme normalisé μ_x divise le polynôme normalisé χ_A de degré k, on a $\chi_A = \mu_x$.

2° Il s'agit de prouver que, χ désignant le polynôme caractéristique de u, on a $\chi(u) = 0$, i.e. $\chi \in I_x$ pour tout $x \in E \setminus \{0\}$.

Soit $x \in E \setminus \{0\}$. On lui associe F_x, k_x (encore noté k) et e_x (cf. 1°)

• Supposons $F_x = E$. Ici $v_x = u$. D'après 1° b), on a $\chi = \mu_x$ et donc $\chi \in I_x$.

• Supposons $F_x \neq E$, i.e. $k < n$. Dans une base de E obtenue en complétant la famille libre e_x, la matrice de u est de la forme :

$$M = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} \qquad (3)$$

où A est la matrice-compagnon donnée par (2), et où $C \in \mathcal{M}_{n-k}(K)$.
D'où : $\chi = \chi_A \chi_C$, avec $\chi_A \in I_x$ d'après 1° b), et donc $\chi \in I_x$. □

3° Preuve de i) ⇒ ii). Par hypothèse, il existe $x \in E \setminus \{0\}$ tel que $F_x = E$ (notation du 1°). D'après 1° b), on a $\chi = \mu_x$; or μ_x, et donc χ, divisent le polynôme minimal μ de u (qui appartient à I_x) ; comme μ divise χ, et comme il s'agit de polynômes normalisés, on a $\chi = \mu$.

Preuve de ii) ⇒ i). Par hypothèse deg μ = n. Or on sait (exercice précédent) qu'il existe $x \in E$ tel que $\mu_x = \mu$; d'après $n > 0$, on a $x \neq 0$; on dispose de F_x et, d'après 1° b), on a : deg μ_x = dim F_x ; d'où dim F_x = n, et donc $F_x = E$. □

4° Procédons par récurrence sur dim E = n. Il s'agit de prouver qu'une assertion $\mathcal{A}_n$ est vraie pour tout $n \in \mathbb{N}^*$.

• Il est clair que $\mathcal{A}_1$ est vraie.

• Soit $n \geqslant 2$ tel que $\mathcal{A}_p$ ait été établie pour $1 \leqslant p \leqslant n-1$. Considérons un endomorphisme u d'un K-espace vectoriel E de dimension n ; soient χ et μ les polynômes caractéristique et minimal de u.

Prenons $x \in E \setminus \{0\}$ et associons-lui F_x, k_x (encore noté k) et e_x.

- Supposons k = n. On a $F_x = E$, et $\chi = \mu$ d'après 3°. Le résultat est acquis.

- Supposons $k < n$. Dans une base de E obtenue en complétant la famille libre e_x, la matrice M de u est de la forme (3) (cf. solution du 2°) et $\chi = \chi_A \chi_C$.

Soit $P \in K[X]$, irréductible, qui divise χ, et donc χ_A ou χ_C.

Comme $\chi_A = \mu_x$ (cf. 1°b) et comme μ_x divise μ, il est clair que si P divise χ_A, alors P divise μ.

Supposons maintenant que P divise χ_C ; alors P divise μ_C (hypothèse de récurrence). Nous avons par récurrence :

$$\forall m \in M \quad M^m = \begin{bmatrix} A^m & \star \\ 0 & C^m \end{bmatrix}$$

et, par combinaison linéaire :

$$\mu(M) = \begin{bmatrix} \mu(A) & \star \\ 0 & \mu(C) \end{bmatrix}$$

Comme $\mu(M) = 0$, il vient $\mu(C) = 0$; μ appartient à l'idéal annulateur de C, et est un multiple de μ_C et donc un multiple de P. □

Remarque. Le résultat du 4° a de nombreuses applications. En voici deux

• Soit la décomposition du polynôme caractéristique de u : $\chi = \prod_{i=1}^{p} P_i^{m_i}$, les P_i étant irréductibles, normalisés et distincts, avec $m_i \geqslant 1$.

Celle du polynôme minimal de u est : $\mu = \prod_{i=1}^{p} P_i^{r_i}$, $1 \leqslant r_i \leqslant m_i$, ce qui entraîne que les endomorphismes $P_i(u)$ sont non injectifs (cf. remarque à la fin de la solution de l'exercice précédent).

• D'autre part, si χ est scindé sur K et n'a que des racines simples, alors $\mu = \chi$.

• *Les quatre exercices qui suivent utilisent les définitions des sous-espaces cycliques et des endomorphismes cycliques données dans l'exercice précédent.*

4.3.9 On considère un K-espace vectoriel E de dimension finie $n > 0$, et un endomorphisme cyclique u de E.

Soit $G \neq \{0\}$, sous-espace de E stable par u. Montrer qu'il existe $y \in G$ tel que G soit le sous-espace cyclique de E associé à u et engendré par y.

Par hypothèse, nous disposons de $x \in E$ tel que $E = \mathrm{Vect}\left(u^i(x)\right)_{i \in \mathbb{N}}$.

Considérons $J = \{P \in K[X] \mid P(u)(x) \in G\}$. Il est clair que J est un sous-groupe additif de K[X]. D'autre part, pour tout $(P,Q) \in J \times K[X]$ nous avons $P(u)(x) \in G$ et, G étant stable par u, $u^i\left(P(u)(x)\right) \in G$ pour tout $i \in \mathbb{N}$; en écrivant $Q(u) = \sum_{i=0}^{+\infty} \xi_i u^i$, il en résulte $QP \in J$.

Finalement J est un idéal de l'anneau principal K[X] ; il contient l'idéal annulateur de u ; d'où $J \neq \{0\}$; il existe donc $R \in K[X] \setminus \{0\}$ qui engendre J. Posons $y = R(u)(x)$ et $F_y = \mathrm{Vect}\left(u^i(y)\right)_{i \in \mathbb{N}}$.

- Par $R \in J$, nous obtenons $y \in G$; comme G est stable par u, nous en déduisons $F_y \subset G$.

- Inversement, soit $z \in G$. D'après $z \in \mathrm{Vect}\left(u^i(x)\right)_{i \in \mathbb{N}}$, il existe $S \in K[X]$ tel que $z = S(u)(x)$; compte tenu de $z \in G$, il vient $S \in J$, et il existe donc $Q \in K[X]$ tel que $S = QR$. Nous avons :

$$z = (QR)(u)(x) = Q(u)(y) \text{ et } z \in F_y.$$

Nous avons ainsi $G \subset F_y$, et, au total $G = F_y$, ce qui exige $y \neq 0$. □

4.3.10 Soient E un K-espace vectoriel de dimension finie $n>0$, et u un endomorphisme de E, nilpotent d'indice r.

1° Montrer qu'il existe un sous-espace cyclique de E associé à u dont la dimension est r.

2° Montrer qu'il existe une décomposition $E = F \oplus G$, où F est cyclique associé à u, de dimension r, et où G est stable par u (on utilisera ${}^t u$).

1° Par définition de r, $\mathrm{Ker}\, u^r = E$, et $\mathrm{Ker}^{r-1} \subset E$ strictement. Il existe donc $x' \in E$ tel que $u^{r-1}(x') \neq 0$ et $u^i(x') = 0$ pour tout $i \geqslant r$.

La famille $(x', u(x'), \ldots, u^{r-1}(x'))$ est donc génératrice de $F' = \mathrm{Vect}(u^i(x'))_{i\in\mathbb{N}}$.

Montrons qu'elle est libre, ce qui entraînera qu'il s'agit d'une base de F' et fournira la proposition.

Soit $(\alpha_0, \alpha_1, \ldots, \alpha_{r-1}) \in K^r$ tel que $\sum_{i=0}^{r-1} \alpha_i u^i(x') = 0$; en prenant les images successivement par $u^{r-1}, \ldots, u^0$, on constate $\alpha_0 = 0, \ldots, \alpha_{r-1} = 0$. □

2° Pour tout $k \in \mathbb{N}$, on a $({}^t u)^k = {}^t(u^k)$; en outre, par identification de E et de son bidual, ${}^t({}^t u) = u$. Il en résulte que ${}^t u$ est nilpotent d'indice r.

En raisonnant comme au 1°, on constate qu'il existe $y^* \in E^*$ tel que $({}^t u)^{r-1}(y^*) \neq 0$, et que le sous-espace cyclique G^* de E^*, associé à ${}^t u$ et engendré par y^*, est de dimension r.

Notons G l'orthogonal $(G^*)^\circ$ de G^* dans E. On a $\dim G = n-r$.

• Comme G^* est stable par ${}^t u$, G est stable par u ; en effet, pour tout $\xi \in G$, on a :

$$\forall z^* \in G^* \quad \langle z^*, u(\xi)\rangle = \langle {}^t u(z^*), \xi\rangle = 0$$

et donc : $u(\xi) \in (G^*)^\circ$.

• D'après $({}^t u)^{r-1}(y^*) \neq 0$, il existe $x \in E$ tel que :

$$\langle ({}^t u)^{r-1}(y^*), x\rangle = \langle y^*, u^{r-1}(x)\rangle \neq 0 \qquad (1)$$

En particulier : $u^{r-1}(x) \neq 0$; comme $u^i(x) = 0$ pour tout $i \geqslant r$, le raisonnement du 1° montre que le sous-espace cyclique $F = \mathrm{Vect}(u^i(x))_{i\in\mathbb{N}}$ est de dimension r.

• Soit $z \in F \cap G$. D'après $z \in F$, on a : $z = \sum_{i=0}^{r-1} \alpha_i u^i(x)$.

D'après $z \in G$, pour tout $j \in \{0, \ldots, r-1\}$, on a : $\langle ({}^t u)^j(y^*), z\rangle = 0$,

i.e. : $\sum_{i=0}^{r-1} \alpha_i \langle ({}^t u)^j(y^*), u^i(x)\rangle = 0$,

et : $\sum_{i=0}^{r-1} \alpha_i \langle ({}^t u)^{j+i}(y^*), x\rangle = 0$.

En faisant successivement $j = r-1, \ldots, 0$, compte tenu de (1) et de $({}^t u)^k(y^*) = 0$ pour $k \geqslant r$, on constate : $\alpha_0 = 0, \ldots, \alpha_{r-1} = 0$, et donc $z = 0$.

On a ainsi $F \cap G = \{0\}$, et grâce aux dimensions : $E = F \oplus G$. □

Remarque. L'endomorphisme induit par u sur le sous-espace stable F admet pour matrice dans la base $(u^{r-1}(x),\dots,x)$ la matrice $J_r = [\xi_{ij}]$, avec $\xi_{ij} = 1$ si $j = i+1$, et $\xi_{ij} = 0$ sinon (matrice nilpotente de Jordan d'ordre r).

Comme G est stable par u, on dispose de l'endomorphisme induit par u sur G, qui est nilpotent d'indice $r' \leqslant r$. Par récurrence sur les dimensions, cet exercice prouve l'existence d'une base de E dans laquelle la matrice de u est : $\mathrm{diag}(J_r, J_{r_1}, \dots, J_{r_k})$, où les J_{r_i} sont des matrices nilpotentes de Jordan d'ordres r_i tels que : $r \geqslant r_1 \geqslant \dots \geqslant r_k$. C'est sur ce résultat que se base la réduction de Jordan d'un endomorphisme quelconque de E.

4.3.11 Soient E un K-espace vectoriel de dimension finie $n > 0$, et u un endomorphisme de E. On appelle *commutant* de u l'ensemble $\mathcal{C}$ des endomorphismes de E qui commutent avec u.

1° Déterminer $\mathcal{C}$ dans le cas où u est cyclique (cf. 4.3.8).

Exemple : E est $K_{n-1}[X]$, u est la dérivation $P \mapsto P'$.

2° Ici le polynôme caractéristique de u est scindé sur K ; on l'écrit :

$$\chi = \prod_{i=1}^{p} (X-\lambda_i)^{m_i},\ m_i \in \mathbb{N}^*,\ \lambda_i \neq \lambda_j \text{ si } i \neq j.$$

Montrer : $\dim \mathcal{C} \leqslant m_1^2 + \dots + m_p^2$; peut-il y avoir égalité ?

3° Déterminer $\mathcal{C}$ dans le cas où u admet n valeurs propres distinctes.

Il est clair que $\mathcal{C}$ est une sous-algèbre de $\mathcal{L}(E)$, et que $K[u] \subset \mathcal{C}$.

1° Par hypothèse, il existe $x \in E$ tel que $e = (x,\dots,u^{n-1}(x))$ soit une base de E.

Soit $v \in \mathcal{C}$. On peut écrire : $v(x) = \sum_{i=0}^{n-1} \alpha_i u^i(x)$.

Commutant avec u, v commute avec tout u^k, $k \in \mathbb{N}$, et l'on a :

$$v(u^k(x)) = u^k(v(x)) = \sum_{i=0}^{n-1} \alpha_i u^{i+k}(x) = \left(\sum_{i=0}^{n-1} \alpha_i u^i\right)(u^k(x)).$$

Les deux endomorphismes v et $\sum_{i=0}^{n-1} \alpha_i u^i$ donnent la même image de tout élément de la base e de E ; ils sont donc égaux. D'où : $v \in K[u]$.

On a donc $\mathcal{C} \subset K[u]$, et finalement : $\mathcal{C} = K[u]$.

Exemple.- Il s'agit d'un cas particulier d'un endomorphisme $u \in \mathcal{L}(E)$ nilpotent d'indice n ; celui-ci est cyclique d'après 4.3.2, 3°, et, compte tenu de $u^k = 0$ pour $k \geqslant n$, $\mathcal{C}$ est l'ensemble des $\sum_{k=0}^{n-1} \alpha_k u^k$.

En utilisant encore 4.3.1, 3°, on en déduit que les $M \in \mathcal{M}_n(K)$ qui commutent avec J_n, matrice nilpotente de Jordan d'ordre n, sont les $\sum_{k=0}^{n-1} \alpha_k J_h^k$.

2° Utilisons l'étude des sous-espaces caractéristiques. Pour tout $i \in \mathbf{N}_p$ notons r_i l'indice de l'endomorphisme $u - \lambda_i \mathrm{Id}_E$, E_i l'espace $\mathrm{Ker}(u-\lambda_i \mathrm{Id}_E)^{r_i}$, u_i l'endomorphisme induit par u sur E_i (qui est stable par u puisque $(u - \lambda_i \mathrm{Id}_E)^{r_i}$ commute avec u), et $\mathcal{C}_i$ le commutant de u_i dans $\mathcal{L}(E_i)$.

On sait que $\dim E_i = m_i$ pour tout $i \in \mathbf{N}_p$, et que $E = \bigoplus_{i=1}^{p} E_i$.

• Notons que l'on peut caractériser $\mathcal{C}$ de la façon suivante :

- Soit $v \in \mathcal{C}$. Pour tout $i \in \mathbf{N}_p$, E_i est stable par v (puisque $(u-\lambda_i \mathrm{Id}_E)^{r_i}$ commute avec v) et l'endomorphisme v_i de E_i induit par v appartient à $\mathcal{C}_i$ dans $\mathcal{L}(E_i)$.

- Réciproquement, si pour tout $i \in \mathbf{N}_p$ on choisit un $v_i \in \mathcal{C}_i$, l'endomorphisme v de E défini par :

$$\forall i \in \mathbf{N}_p \quad \forall x \in E_i \quad v(x) = v_i(x)$$

appartient à $\mathcal{C}$.

• Il en résulte aisément : $\dim \mathcal{C} = \sum_{i=1}^{p} \dim \mathcal{C}_i$.

Or : $\dim \mathcal{C}_i \leqslant \dim(\mathcal{L}(E_i)) = m_i^2$, avec égalité si, et seulement si $\mathcal{C}_i = \mathcal{L}(E_i)$, ce qui s'écrit : u_i est dans le centre de $\mathcal{L}(E_i)$, i.e. u_i est une homothétie, i.e. $E_i = \mathrm{Ker}(u-\lambda_i \mathrm{Id}_E)$.

En conclusion : $\dim \mathcal{C} \leqslant m_1^2 + \ldots + m_p^2$, avec égalité si, et seulement si u est diagonalisable.

3° L'hypothèse implique que le polynôme minimal de u coïncide avec le polynôme caractéristique de u ; il en résulte (cf. 4.3.8,3°) que u est cyclique, et donc, d'après 1°, que $\mathcal{C} = K[u]$.

Notons que ce résultat a été obtenu au n°4.2.2,1° par un procédé qui n'utilise pas la notion d'endomorphisme cyclique.

4.3.12 Soient un corps commutatif K, et un entier $n \geqslant 2$. Pour toute permutation $\sigma \in \mathfrak{S}_n$ de $(1,\ldots,n)$ on note A_σ la K-matrice (n,n) dont l'élément (i,j) est $\delta_{i,\sigma(j)}$.

1° Montrer que $S_n = \{A_\sigma \mid \sigma \in \mathfrak{S}_n\}$ est un groupe isomorphe à $\mathfrak{S}_n$.

2° Soit $A_\sigma \in S_n$. Déterminer son polynôme caractéristique χ_σ et son polynôme minimal μ_σ (on décomposera σ en produit de cycles).

3° Ici K est algébriquement clos, de caractéristique p. Soit σ un cycle d'ordre n. Trouver une condition nécessaire et suffisante (liant p et n) pour que A_σ soit diagonalisable, et, lorsqu'elle est remplie, diagonaliser A_σ.

1° Remarquons que, pour toute base $e = (e_1,\ldots,e_n)$ de K^n, A_σ est la matrice de passage de e à la base $e' = (e'_1,\ldots,e'_n)$ dans laquelle $e'_j = e_{\sigma(j)}$ pour tout $j \in \mathbf{N}_n$ (les éléments de e' sont ceux de e, dans un ordre différent).

A_σ appartient donc au groupe linéaire $GL_n(K)$ des K-matrices (n,n) inversibles ; S_n est ainsi une partie de $GL_n(K)$; montrons que c'est un sous-groupe.

• Preuve de la stabilité de S_n. Nous allons prouver :

$$\forall(\sigma,\tau)\in(\mathfrak{S}_n)^2 \quad A_\sigma A_\tau = A_{\sigma\tau} \cdot \tag{1}$$

Par le calcul c'est immédiat : l'élément α_{ij} de $A_\sigma A_\tau$ est la somme $\sum_{k=1}^{n} \delta_{i,\sigma(k)}\delta_{k,\tau(j)}$ dont le terme général n'est non nul (et alors il vaut 1) que si $i=\sigma(k)$ et $k=\tau(j)$, i.e. si $i=\sigma\tau(j)$ et $k=\tau(j)$. □

Une méthode plus élégante consiste à adjoindre aux bases e et e' déjà considérées la base $e'' = (e''_1,\ldots,e''_n)$, avec $e''_k = e'_{\tau(k)}$ et donc $e''_k = e_{\sigma\tau(k)}$;(1) ne fait que traduire $P_e^{e'} P_{e'}^{e''} = P_e^{e''}$.

• De (1) on déduit que l'application $\sigma \longmapsto A_\sigma$ de $\mathfrak{S}_n$ dans $GL_n(K)$ est un morphisme de groupes, visiblement injectif ; l'image S_n de ce morphisme est un sous groupe de $GL_n(K)$ isomorphe à $\mathfrak{S}_n$.

Remarque. On a $[1 \ldots n]A_\sigma = [\sigma(1) \ldots \sigma(n)]$, ce qui conduit à qualifier les A_σ de *matrices-permutations*.

2° Ici $\varepsilon = (\varepsilon_1,\ldots,\varepsilon_n)$ est la base canonique de K^n ; u_σ est l'endomorphisme de K^n représenté par A_σ dans cette base ; χ_σ et μ_σ sont les polynômes caractéristique et minimal communs à A_σ et u_σ.

• Etudions d'abord le cas où σ est un cycle d'ordre n.

Il existe alors une permutation $\theta\in\mathfrak{S}_n$ qui transforme $(1,2,\ldots,n)$ en $\left(1,\sigma(1),\ldots,\sigma^{n-1}(1)\right)$. Soit ε' la base $\left(\varepsilon_1,\varepsilon_{\sigma(1)},\ldots,\varepsilon_{\sigma^{n-1}(1)}\right)$ de K^n, avec $P_\varepsilon^{\varepsilon'} = A_\theta$.

En utilisant $\varepsilon_{\sigma(j)} = u_\sigma(\varepsilon_j)$, on vérifie par récurrence $\varepsilon_{\sigma^k(1)} = u_\sigma^k(\varepsilon_1)$ pour tout $k\in\mathbb{N}$. D'où $\varepsilon' = \left(\varepsilon_1, u_\sigma(\varepsilon_1),\ldots,u_\sigma^{n-1}(\varepsilon_1)\right)$ ce qui montre que u_σ est un endomorphisme cyclique.

Pour tout polynôme non nul de degré strictement inférieur à n, $P = \sum_{k=0}^{n-1} \xi_k X^k$, on a : $P(u_\sigma)(\varepsilon_1) = \sum_{k=0}^{n-1} \xi_k u_\sigma^k(\varepsilon_1) \neq 0$. D'où $P(u_\sigma)\neq 0$ et $\deg \mu_\sigma \geqslant n$.

En outre $u_\sigma^n - Id_{K^n} = 0$, et μ_σ divise X^n-1. S'agissant de polynômes normalisés, $\mu_\sigma = X^n-1$ et donc $\chi_\sigma = X^n-1$ (χ_σ est un multiple de μ_σ et $\deg \chi_\sigma = n$). □

Autre solution. On utilise : $\mathrm{mat}(u_\sigma;\varepsilon')$ qui s'écrit :

$$B = \begin{bmatrix} 0 & & & 0 & 1 \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & & 0 & 1 & 0 \end{bmatrix} .$$

En développant $\det(XI_n - B)$ suivant la dernière colonne, on obtient :

$$\chi_\sigma = \chi_B = X^n - 1 .$$

En outre, u_σ étant cyclique, on a (cf. 4.3.8, 3°) : $\mu_\sigma = \chi_\sigma$. □

• Venons-en au cas général. On décompose σ en cycles de supports $J_1, \ldots, J_m$ deux à deux distincts. Pour tout $k \in \mathbb{N}_m$, on note E_k le sous-espace de K^n engendré par les ε_i $(i \in J_k)$; les E_k, de dimensions n_k, sont stables par u_σ et E est leur somme directe ; on applique à chacun d'eux le résultat précédent ; χ_σ et μ_σ sont ainsi respectivement le produit et le PPCM des polynômes :

$$X^{n_1} - 1, \ldots, X^{n_m} - 1, \text{ où } n_k = \operatorname{card} J_k. \qquad \square$$

3° Rappelons que p est 0 ou un nombre premier.

Ici $\chi_\sigma = X^n - 1$ est scindé sur K. Soit ω l'une de ses racines ; en utilisant $B = \operatorname{mat}(u_\sigma ; \varepsilon')$ on constate que le sous-espace propre de u_σ associé à ω est de dimension 1 ; u_σ est donc diagonalisable si, et seulement si toute racine ω de $X^n - 1$ est simple. On écrit :

$$X^n - 1 = (X - \omega)Q, \text{ avec } Q = X^{n-1} + \omega X^{n-2} + \ldots + \omega^{n-1},$$

$Q(\omega) = n\omega^{n-1}$; comme $\omega \neq 0$, $Q(\omega)$ n'est nul que si $n \in p\mathbb{N}$. Il en résulte que u_σ, A_σ et B sont diagonalisables si, et seulement si $n \notin p\mathbb{N}$ (condition remplie pour tout $n \geqslant 2$ si $p = 0$).

• Supposons cette condition remplie. Nous savons diagonaliser B qui est une matrice circulante (cf. 4.2.6).

$X^n - 1$ admet n racines simples $\omega_1, \ldots, \omega_n$ (valeurs propres de B). A tout $j \in \mathbb{N}_n$, nous associons le vecteur colonne non nul $C_j = {}^t[\omega_j^{n-1} \ldots \omega_j \; 1]$ et nous constatons que $BC_j = \omega_j C_j$, ce qui signifie que le sous-espace propre de dimension 1 associé à la valeur propre ω_j est KC_j.

La (n,n) matrice P de vecteurs colonnes $C_1, \ldots, C_n$ est ainsi inversible, et :

$$B = PDP^{-1}, \text{ où } D = \operatorname{diag}(\omega_1, \ldots, \omega_n)$$

et donc : $A_\sigma = QDQ^{-1}$, où $Q = A_\theta P$ (en effet $A_\sigma = A_\theta B A_\theta^{-1}$).

4.3.13 1° Soient un corps commutatif K et un entier $n \geqslant 2$. On note H_n l'ensemble des K-matrices (n,n) inversibles, dont chaque colonne contient un, et un seul élément non nul. Montrer que H_n est un sous-groupe de $GL_n(K)$.

2° Montrer que, pour tout nombre premier p et tout $n \in \mathbb{N}^*$:

$$n!(p-1)^n \text{ divise } (p^n - 1)(p^n - p)\ldots(p^n - p^{n-1}). \qquad (1)$$

1° On convient que, dans l'élément $[\alpha_{ij}]$ de H_n, l'élément non nul de la colonne d'indice j est noté λ_j et que son indice de ligne est noté $\sigma(j)$.

A cause de $\det H_n \neq 0$, σ est une permutation de $\mathfrak{S}_n$.

H_n est ainsi l'ensemble des $[\lambda_j \delta_{i,\sigma(j)}]$, où $\sigma \in \mathfrak{S}_n$ et $(\lambda_1,\ldots,\lambda_n) \in (K^*)^n$.

- H_n est une partie de $GL_n(K)$, non vide puisqu'elle contient I_n.
- Preuve de la stabilité de H_n. Soient $X = [\lambda_j \delta_{i,\sigma(j)}]$ et $Y = [\mu_j \delta_{i,\tau(j)}]$ deux éléments de H_n. Il s'agit de vérifier $XY \in H_n$.

Le calcul est ici la méthode la plus rapide : l'élément α_{ij} de XY est la somme $\sum_{k=1}^{n} \lambda_k \delta_{i,\sigma(k)} \mu_j \delta_{k,\tau(j)}$, dont le terme général n'est nul (et alors il vaut $\lambda_{\tau(j)}\mu_j$) que si $i = \sigma(k)$ et $k = \tau(j)$, i.e. $i = \sigma\tau(j)$ et $k = \tau(j)$. D'où :

$$XY = [\lambda_{\tau(j)} \mu_j \delta_{i,\sigma\tau(j)}] \in H_n \qquad (1)$$

- De (1), on déduit que, toute $X \in H_n$ a pour inverse dans $GL_n(K)$:

$$X^{-1} = \left[\frac{1}{\lambda_{\sigma^{-1}(j)}} \delta_{i,\sigma^{-1}(j)}\right] \in H_n.$$

- En conclusion, H_n est une partie non vide de $GL_n(K)$, stable et telle que $X^{-1} \in H_n$ pour tout $X \in H_n$; c'est donc un sous-groupe de $GL_n(K)$. □

2° Le nombre premier p est fixé.

- Pour $n = 1$, il est clair que (1) est vérifiée.
- Soit $n \geqslant 2$. Utilisons 1° dans le cas où K est le corps fini $F_p = \mathbb{Z}/p\mathbb{Z}$ de cardinal p, et de caractéristique p.

Comme il existe visiblement une bijection de $\mathfrak{S}_n \times (F_p^*)^n$ sur H_n, le cardinal de H_n est $\alpha = n!(p-1)^n$. D'autre part le cardinal β de $GL_n(F_p)$, qui est un multiple de α d'après 1°, est le nombre des automorphismes du F_p-espace vectoriel $(F_p)^n$. Une base étant choisie, un automorphisme est déterminé par une base ; β est donc le nombre des bases de $(F_p)^n$. Pour obtenir l'une d'elles :

- On choisit e_1 parmi les p^n-1 vecteurs non nuls de $(F_p)^n$; la droite $\mathrm{Vect}(e_1)$ contient p vecteurs ;
- On choisit e_2 parmi les p^n-p vecteurs n'appartenant pas à $\mathrm{Vect}(e_1)$; on avait donc $(p^n-1)(p^n-p)$ possibilités pour choisir (e_1,e_2) ; le plan $\mathrm{Vect}(e_1,e_2)$ contient p^2 vecteurs ;
- On choisit e_3 parmi les p^n-p^2 vecteurs n'appartenant pas à $\mathrm{Vect}(e_1,e_2)$, et ainsi de suite, ce qui conduit à :

$$\beta = (p^n-1)(p^n-p)\ldots(p^n-p^{n-1}). \qquad \square$$

4.3.14 Soit E un K-espace vectoriel de dimension finie $n>0$. Un endomorphisme u de E est dit *simple* si, et seulement si les seuls sous-espaces de E stables par u sont E et {0}.

Montrer que u est simple si, et seulement si son polynôme caractéristique χ_u est irréductible dans $K[X]$.

La condition est suffisante. Par hypothèse, χ_u est irréductible.

Soit E' un sous-espace non nul de E, stable par u ; on note u' l'endomorphisme de E' induit par u et $\chi_{u'}$ son polynôme caractéristique ; on a $\deg \chi_{u'} = \dim E' > 0$.

On sait que $\chi_{u'}$ divise χ_u ; on a donc $\chi_{u'} = \chi_u$; d'où $\dim E' = \dim E$ et $E' = E$. □

La condition est suffisante. Par hypothèse, u est simple.

Supposons que son polynôme minimal μ_u s'écrive P_1P_2, avec P_1 et P_2 normalisés et premiers entre eux. Par le lemme des noyaux, nous avons :

$$E = \operatorname{Ker} \mu_u(u) = \operatorname{Ker} P_1(u) \oplus \operatorname{Ker} P_2(u).$$

Mais, $P_1(u)$ et $P_2(u)$ commutant avec u, leurs noyaux sont stables par u ; l'un d'eux est donc égal à $\{0\}$, l'autre à E. Supposons, pour fixer les idées que $\operatorname{Ker} P_1(u) = \{0\}$ et $\operatorname{Ker} P_2(u) = E$; on a $P_2(u) = 0$, et P_2 est un multiple de μ_u. Il en résulte $P_2 = \mu_u$ et $P_1 = 1$. En utilisant la décomposition de μ_u en polynômes irréductibles, on en déduit $\mu_u = Q^r$, où Q est irréductible et où $r \in \mathbb{N}^*$.

$\operatorname{Ker} Q(u)$, stable par u, est $\{0\}$ ou E. On n'a par $\operatorname{Ker} Q(u) = \{0\}$, sans quoi Q(u) serait injectif, il en serait de même de $(Q(u))^r = Q^r(u)$; $\operatorname{Ker} \mu_u(u)$ serait à la fois $\{0\}$ et E. On a donc $\operatorname{Ker} Q(u) = E$, et $Q(u) = 0$, ce qui exige que Q soit un multiple de μ_u et que $r = 1$; égal à Q, μ_u est ainsi irréductible dans $K[X]$.

Considérons $x \in E \setminus \{0\}$ et $F_x = \operatorname{Vect}\left(x, u(x), \ldots, u^{d-1}(x)\right)$, où d est le degré de μ_u. De $\mu_u(u)(x) = 0$, on déduit $u^d(x) \in F_x$; il en résulte que F_x est stable par u. Comme $F_x \neq \{0\}$, on a $F_x = E$ et $\dim F_x = n$. Comme $\dim F_x \leqslant d$ et $d \leqslant n$, il vient $d = n$. D'où $\mu_u = \chi_u$. □

4.3.15 Soient E un K-espace vectoriel de dimension finie $n > 0$, et u un endomorphisme de E.

1° Montrer qu'une droite D [resp. un hyperplan H] de E est stable par u si et seulement s'il existe une valeur propre λ de u telle que :

$$D \subset \left(\operatorname{Ker}(u - \lambda \mathrm{Id}_E)\right) \quad [\text{resp. } \left(\operatorname{Im}(u - \lambda \mathrm{Id}_E)\right) \subset H].$$

2° Ici E est de dimension 3, (e_1, e_2, e_3) est une base de E. Trouver tous les sous-espaces de E stables par $u \in \mathcal{L}(E)$ défini par :

$$\operatorname{mat}\left(u; (e_1, e_2, e_3)\right) = \begin{bmatrix} 3 & 1 & -1 \\ 1 & 1 & 1 \\ 2 & 0 & 2 \end{bmatrix}.$$

Remarque préliminaire. Soit F un sous-espace de E. Montrons que F est stable par u si, et seulement si le sous-espace $F^{\perp}$ de E^{*} est stable par l'endomorphisme ${}^{t}u$ de E^{*}.

- Ici F est stable par u. Considérons $x^{*} \in F^{\perp}$. Pour tout $y \in F$, nous avons $u(y) \in F$, et donc $\langle x^{*}, u(y) \rangle = 0$, i.e. $\langle {}^{t}u(x^{*}), y \rangle = 0$. Il en résulte $u(x^{*}) \in F^{\perp}$; $F^{\perp}$ est ainsi stable par ${}^{t}u$.

- La réciproque se prouve en identifiant E à son bidual E^{**} (E est de dimension finie) ; on a ainsi $F^{\perp\perp} = F$ et ${}^{tt}u = u$. □

1° Il est clair qu'une droite D de E est stable par u si, et seulement si elle est incluse dans un sous-espace propre de u.

• Compte tenu de la remarque préliminaire, un hyperplan H de E est stable par u si, et seulement si la droite $H^{\perp}$ de E^{*} est stable par ${}^{t}u$, ce qui s'écrit : il existe une valeur propre λ de ${}^{t}u$ (et donc de u car u et ${}^{t}u$ ont les mêmes valeurs propres) telle que :

$$H^{\perp} \subset \mathrm{Ker}({}^{t}u - \lambda \mathrm{Id}_{E^{*}}) \qquad (1)$$

Or on sait que : $\mathrm{Ker}({}^{t}u - \lambda \mathrm{Id}_{E^{*}}) = \left(\mathrm{Im}(u - \lambda \mathrm{Id}_{E})\right)^{\perp}$.

En utilisant : $(H^{\perp} \subset G^{\perp}) \Leftrightarrow (G \subset H)$, (1) s'écrit :

$$\left(\mathrm{Im}(u - \mathrm{Id}_{E})\right) \subset H. \qquad \square$$

2° On constate que le polynôme caractéristique de u est $(X-2)^{3}$. La seule valeur propre de u est donc $\lambda = 2$. On détermine :

$$\mathrm{Ker}(u - 2\mathrm{Id}_{E}) = \mathrm{Vect}(e_2 + e_3), \text{ de dimension 1,}$$

et : $$\mathrm{Im}(u - 2\mathrm{Id}_{E}) = \mathrm{Vect}(e_1 + e_2 + 2e_3, e_1 - e_2), \text{ de dimension 2.}$$

Ces deux sous-espaces sont, avec {0} et E, les seuls sous-espaces de E stables par u.

4.3.16 1° Soient E un $\mathbb{R}$-espace vectoriel de dimension finie $n \geqslant 2$ et u un endomorphisme de E. Montrer qu'il existe un plan de E stable par u.

2° Soient E un $\mathbb{R}$-espace vectoriel de dimension finie, impaire 2n+1, $n \in \mathbb{N}$, et u un endomorphisme de E. Montrer que, pour tout $p \in \{0, \ldots, 2n+1\}$ il existe un sous-espace de E de dimension p, stable par u.

1° Deux cas sont possibles.

1er *Cas* : le polynôme caractéristique χ de u est scindé sur $\mathbb{R}$. On dispose d'une base $(e_1, \ldots, e_n)$ de E dans laquelle u est représenté par une matrice triangulaire supérieure ; $\mathrm{Vect}(e_1, e_2)$ est un plan stable par u.

2ème *Cas* : χ n'est pas scindé sur $\mathbb{R}$. On a $\chi = \prod_{i=1}^{p} P_i^{m_i}$, $m_i \geqslant 1$, les P_i étant irréductibles, de degré 1 ou 2, normalisés et distincts, l'un deux au moins, qui sera noté Q, étant de degré 2.

On sait (cf. remarque à la fin de la solution de (4.3.8) que les endomorphismes $P_i(u)$ et en particulier $Q(u)$, sont non injectifs. Il existe donc $x \in \mathrm{Ker}\, Q(u) \setminus \{0\}$. La famille $(x, u(x))$ est libre, sans quoi il existerait $\alpha \in \mathbb{R}$ tel que $u(x) = \alpha x$ et donc $Q(\alpha) = 0$; la famille $(x, u(x), u^2(x))$ est liée à cause de $Q(u)(x) = 0$; $\mathrm{Vect}(x, u(x))$ est ainsi un plan de E stable par u. □

2° Il s'agit de prouver qu'une assertion $\mathcal{A}_n$ est vraie pour tout $n \in \mathbb{N}$.

- Il est clair que $\mathcal{A}_0$ est vraie.

- Soit $n \in \mathbb{N}$ tel que $\mathcal{A}_n$ a été vérifiée. Considérons un $\mathbb{R}$-espace vectoriel de dimension 2n+3, et $u \in \mathcal{L}(E)$. Dans E^*, nous disposons pour ${}^t u$ de l'espace stable $\{0_{E^*}\}$, d'une droite stable (le polynôme caractéristique de u, de degré impair, a au moins une racine réelle), et d'un plan stable (cf. 1°).

En utilisant la remarque préliminaire de l'exercice précédent, nous constatons que, dans E, nous disposons pour u de l'espace stable E de dimension 2n+3, d'un hyperplan stable de dimension 2n+2, et d'un sous-espace stable F de dimension 2n+1. En appliquant $\mathcal{A}_n$ à l'endomorphisme de F induit par u, nous constatons que $\mathcal{A}_{n+1}$ est vraie. □

• *Terminons par un exercice qui fait intervenir le cours d'Analyse.*

4.3.17 1° Soient I et V des $\mathbb{C}$-matrices carrées de même ordre; I est unité, V est nilpotente. Existe-t-il $\lim_{n \to +\infty} U^n$, où $U = \lambda I + V$ et $\lambda \in \mathbb{C}$?

2° Soit u un endomorphisme d'un $\mathbb{C}$-espace vectoriel E de dimension finie. On note σ le plus grand des modules des valeurs propres de u.

a) Discuter l'existence de $\lim_{n \to +\infty} u^n$.

b) Soit $\sum a_n z^n$ une série entière complexe de rayon de convergence R. Montrer que la série $\sum a_n u^n$ est absolument convergente si $\sigma < R$, divergente si $\sigma > R$.

Tous les $\mathbb{C}$-espaces vectoriels E qui interviennent sont de dimension finie. Chacun d'eux est muni de son unique structure topologique d'e.v.n.

Sur $\mathcal{L}(E)$, on adopte la norme $u \mapsto \sup_{\|x\| \leqslant 1} \|u(x)\|$.

1° On note $r \in \mathbb{N}^*$ l'indice de la matrice nilpotente V : $V^{r-1} \neq 0$ et $V^r = 0$.

a) Si r = 1, i.e. V = 0, la suite (U^n) s'écrit $(\lambda^n I)$. Elle converge vers 0 si $|\lambda| < 1$, vers I si $\lambda = 1$; elle diverge dans les autres cas.

b) Etudions maintenant le cas $r \geqslant 2$.

- Pour $\lambda = 0$, nous avons $U^n = V^n$, et donc $\lim_{n\to+\infty} U^n = 0$.

- Supposons $\lambda \neq 0$. Comme I et V commutent, nous avons :

$$\lambda^{-n} U^n = \sum_{k=0}^{r-1} C_n^k \lambda^{-k} V^k, \quad (C_n^k = 0 \text{ pour } k > n).$$

Or il existe $\lim_{n\to+\infty} (n^{-r+1} C_n^k)$; c'est 0 si $0 \leqslant k < r-1$, et $1/(r-1)!$ si $k = r-1$.

D'où : $$\lim_{n\to+\infty} \left(\frac{1}{\lambda^n n^{r-1}} U^n \right) = \frac{1}{\lambda^{r-1}(r-1)!} V^{r-1}.$$

- Si $0 < |\lambda| < 1$, alors $\lim_{n\to+\infty} (\lambda^n n^{r-1}) = 0$, et $\lim_{n\to+\infty} U^n = 0$.

- Si $|\lambda| \geqslant 1$, alors $\lim_{n\to+\infty} |\lambda^n n^{r-1}| = +\infty$. Comme $V^{r-1} \neq 0$, il existe (i,j) tel que l'élément (i,j) de V^{r-1} soit non nul. Il en résulte que l'élément (i,j) de U^n n'est pas borné. La suite (U^n) diverge.

2° a) Soient N_j, $j \in \mathbb{N}_p$, les sous-espaces caractéristiques de u associés aux valeurs propres distinctes λ_j. E est la somme directe des N_j ; ceux-ci sont stables par u ; soit u_j l'endomorphisme de N_j induit par u ; on a $u_j = \lambda_j Id_{N_j} + v_j$, où v_j est nilpotent d'indice r_j, multiplicité du zéro λ_j du polynôme minimal de u.

Soit ε une base de E obtenue en réunissant des bases ε_j des N_j qui trigonalisent les u_j. On note :

$$U_j = \mathrm{mat}(u_j ; \varepsilon_j) = \lambda_j I_j + V_j$$

où I_j est unité, et où V_j est nilpotente d'indice r_j. On en déduit :

$$\mathrm{mat}(u ; \varepsilon) = A, \text{ où } A = \mathrm{diag}(U_1, \ldots, U_p)$$

et : $$\mathrm{mat}(u^n ; \varepsilon) = A^n = \mathrm{diag}(U_1^n, \ldots, U_p^n).$$

Pour que la suite (A^n) admette une limite L, il faut et il suffit que chacune des suites (U_j^n) admette une limite L_j, et alors $L = \mathrm{diag}(L_1, \ldots, L_p)$.

- Compte tenu du 1°, on a la discussion suivante :

- Si $\sigma < 1$, alors il existe $\lim_{n\to+\infty} A^n = 0$, et donc $\lim_{n\to+\infty} u^n = 0$.

- Si u admet une valeur propre λ_j telle que $\lambda_j \neq 1$ et $|\lambda_j| \geqslant 1$, alors il n'existe pas $\lim_{n\to+\infty} U_j^n$; il n'existe donc ni $\lim_{n\to+\infty} A^n$, ni $\lim_{n\to+\infty} u^n$.

- Reste le cas où, à la notation près, on a $\lambda_1 = 1$ et $|\lambda_j| < 1$ pour $j \geqslant 2$.

Alors les suites (A^n) et (u^n) convergent si, et seulement si $V_1 = 0$, ce qui s'écrit $r_1 = 1$, et donc : 1 est zéro simple du polynôme minimal de u. Supposons cette condition remplie. Nous avons: $\lim_{n\to+\infty} A^n = \mathrm{diag}(I_1, 0, \ldots, 0)$;

$\lim_{n\to+\infty} u^n$ est donc la projection sur N_1 parallèlement à $\overset{p}{\underset{j=2}{\oplus}} N_j$. Notons que N_1 est ici $\mathrm{Ker}(u-\mathrm{Id}_E)$; quant à $\overset{p}{\underset{j=2}{\oplus}} N_j$, il est stable par $u-\mathrm{Id}_E$, qui induit un isomorphisme ce qui permet de constater qu'il s'agit de $\mathrm{Im}(u-\mathrm{Id}_E)$.

b) Supposons $\sigma<R$. Choisissons $\rho\in\mathbb{R}$ tel que $\sigma<\rho<R$; ainsi :

$$a_n u^n = a_n \rho^n (\rho^{-1}u)^n.$$

Le plus grand des modules des valeurs propres de $\rho^{-1}u$ est $\rho^{-1}\sigma<1$; d'après a), on a : $\lim_{n\to+\infty} (\rho^{-n}u^n) = 0$. Or, d'après $\rho<R$, la série numérique $\sum |a_n|\rho^n$ converge. On en déduit que $\sum \|a_n u^n\|$ converge (il existe, en effet, n_o tel que $\|u^n\| \leqslant \rho^n$ pour tout $n \geqslant n_o$).

- Supposons $\sigma>R$. Il existe une valeur propre λ de u telle que $|\lambda|>R$; soit a un vecteur propre de norme 1 associé à λ. On a : $\|u^n(a)\| = |\lambda^n|$, et donc $\|u^n\| \geqslant |\lambda^n|$ pour tout $n\in\mathbb{N}$. Or, d'après $|\lambda|>R$, la suite $(|a_n\lambda^n|)$ n'est pas bornée. On en déduit que la suite $(\|a_n u^n\|)$ n'est pas bornée, et que la série $\sum a_n u^n$ diverge. □

5. ALGEBRE BILINEAIRE

Dans ce dernier chapitre, nous ne considérons que des corps de caractéristique différente de 2.

5.1. FORMES BILINÉAIRES. FORMES QUADRATIQUES

5.1.1 Soient E un K-espace vectoriel et φ une forme bilinéaire sur E vérifiant :

$$\forall (x,y) \in E^2 \quad \big(\varphi(x,y) = 0\big) \Leftrightarrow \big(\varphi(y,x) = 0\big) \tag{1}$$

Montrer que φ est symétrique ou alternée.

Supposant que φ est non alternée, i.e. qu'il existe $x_o \in E$ tel que $\varphi(x_o,x_o) \neq 0$, nous allons montrer que φ est symétrique. La proposition en résultera.

a) Commençons par prouver que, pour tout $y \in E$, nous avons :

$$\varphi(x_o,y) = \varphi(y,x_o) \tag{2}$$

Soit $y \in E$. Il existe $\alpha \in K$ tel que $\varphi(x_o,y+\alpha x_o) = 0$ (à savoir $\alpha = -\varphi(x_o,y)/\varphi(x_o,x_o)$). Nous avons donc, d'après (1) :

$$\varphi(x_o,y+\alpha x_o) = (y+\alpha x_o,x_o)$$

En développant, nous obtenons (2).

b) Prouvons maintenant que, pour tout $(y,z) \in E^2$, nous avons :

$$\varphi(y,z) = \varphi(z,y) \tag{3}$$

ce qui signifie que φ est symétrique.

Soit $(y,z) \in E^2$. Il existe $(\alpha,\beta) \in K^2$ tel que $\varphi(y+\alpha x_o,\ z+\beta x_o) = 0$ [si $\varphi(y,x_o) \neq 0$, nous pouvons adopter $\alpha = 0$ et $\beta = -\varphi(y,z)/\varphi(y,x_o)$; si $\varphi(y,x_o) = 0$, nous pouvons adopter $\alpha = 1$ et $\beta = -\varphi(y+x_o,z)/\varphi(x_o,x_o)$].

Nous avons donc d'après (1) :

$$\varphi(y+\alpha x_o, z+\beta x_o) = \varphi(z+\beta x_o, y+\alpha x_o)$$

En développant, et en utilisant (2), nous obtenons (3). □

5.1.2 Soit φ une forme bilinéaire symétrique non dégénérée sur un K-espace vectoriel E de dimension finie $n>0$. On suppose qu'il existe un vecteur e_1 de E φ-isotrope et non nul.

Montrer qu'il existe une base de E formée de vecteur φ-isotropes.

• On a $E^\perp = \{0\}$ et donc $e_1 \notin E^\perp$, ce qui montre qu'il existe un vecteur a de E tel que $\varphi(e_1,a) \neq 0$.

On peut donc choisir $\alpha \in K$ tel que $e_2 = \alpha e_1 + a$ soit isotrope, i.e. tel que $2\alpha\varphi(e_1,a) + \varphi(a,a) = 0$ (on utilise ici le fait que K n'est pas de caractéristique 2). On a $\varphi(e_1,e_2) = \varphi(e_1,a) \neq 0$, et donc (e_1,e_2) est une famille libre (sans quoi on aurait $e_2 = \beta e_1$ et $\varphi(e_1,e_2) = 0$).

On note F le plan de E dont une base est (e_1,e_2).

• Montrons : $E = F \oplus F^\perp$.

Compte tenu de $\dim F + \dim F^\perp = \dim E$, il suffit de montrer $F \cap F^\perp = \{0\}$.

Soit $x = \xi e_1 + \eta e_2$ un vecteur de F appartenant à $F^\perp$. On a :

$$\varphi(x,e_1) = \varphi(x,e_2) = 0, \text{ i.e. } \eta = \xi = 0, \text{ i.e. } x = 0. \qquad \square$$

Ayant choisi une base $(\varepsilon_3,\ldots,\varepsilon_n)$ de $F^\perp$, nous disposons donc de la base $\varepsilon = (e_1,e_2,\varepsilon_3,\ldots,\varepsilon_n)$ de E.

• Pour tout $j \in \{3,\ldots,n\}$, on a $\varphi(e_1,e_2+\varepsilon_j) = \varphi(e_1,e_2) \neq 0$.

On peut donc choisir $\alpha_j \in K$ tel que $e_j = \alpha_j e_1 + e_2 + \varepsilon_j$ soit isotrope.

La famille $e = (e_1,e_2,e_3,\ldots,e_n)$ est libre et c'est une base de E ; en effet sa matrice dans la base ε est triangulaire supérieure à éléments diagonaux égaux à 1, et donc inversible.

Finalement e est une base de E formée de vecteurs isotropes. □

5.1.3 Montrer qu'il existe une unique forme quadratique non nulle sur $\mathcal{M}_2(K)$ vérifiant :

$$\forall (A,B) \in [\mathcal{M}_2(K)]^2 \quad \Phi(A.B) = \Phi(A) \cdot \Phi(B) \qquad (1)$$

Le K-espace vectoriel $\mathcal{M}_2(K)$ est rapporté à sa base canonique,

$$(e_1,e_2,e_3,e_4) = \left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right).$$

On a : $e_1+e_4 = I$ (matrice-unité) ; on note $e_2+e_3 = J$.

1° On constate que $A \longmapsto \det A$, qui est l'application :

$$\sum_{k=1}^{4} \xi_k e_k \longmapsto \xi_1\xi_4 - \xi_2\xi_3 \text{ de } \mathcal{M}_2(K) \text{ dans } K,$$

est une forme quadratique non nulle qui vérifie (1).

2° Inversement, soit Φ une forme quadratique non nulle sur $\mathcal{M}_2(K)$, vérifiant (1). Commençons par deux remarques :

a) D'après $\Phi \neq 0$, il existe $M \in \mathcal{M}_2(K)$ telle que $\Phi(M) \neq 0$. En écrivant (1) pour le couple (M,I) on obtient $\Phi(I) = 1$.

b) Si M est inversible, on écrit (1) pour (M, M^{-1}) ; d'où $\Phi(M) \neq 0$.

Si $M = 0$, on a $\Phi(M) = 0$.

Si M est de rang 1, on constate que e_2 est de rang 1, et donc équivalente à M, ce qui s'écrit $M = Q^{-1} e_2 P$, avec $(P,Q) \in \left(GL_2(K)\right)^2$.

Comme $(e_2)^2 = 0$, (1) donne $\Phi(e_2) = 0$. D'où (grâce à (1)) : $\Phi(M) = 0$.

Retenons que $M \in \mathcal{M}_2(K)$ est inversible si, et seulement si $\Phi(M) \neq 0$.

- Soit φ la forme polaire de Φ. Les e_k étant non inversibles :

$$\forall (k,\ell) \in \{1,2,3,4\}^2 \quad \varphi(e_k, e_\ell) = \frac{1}{2}\,\Phi(e_k + e_\ell)$$

et donc $\varphi(e_k, e_\ell) = 0$, sauf si $e_k + e_\ell$ est inversible, ce qui s'écrit $k+\ell = 5$. Nous avons :

$$\varphi(e_1, e_4) = \varphi(e_4, e_1) = \frac{1}{2}\,\Phi(I) = \frac{1}{2}\,.$$

Reste à calculer $\varphi(e_2, e_3) = \varphi(e_3, e_2) = \frac{1}{2}\,\Phi(J)$. On utilise :

$$2\varphi(I,J) = \Phi(I+J) - \Phi(I) - \Phi(J).$$

$\varphi(I,J) = \varphi(e_1 + e_4\,,\, e_2 + e_3) = 0$ (somme de 4 scalaires nuls) ; $\Phi(I+J) = 0$ d'après : I+J non inversible ; d'où $\Phi(J) = -\Phi(I) = -1$ et $\varphi(e_2, e_3) = \varphi(e_3, e_2) = -\frac{1}{2}$.

L'image de $\sum_{k=1}^{4} \xi_k e_k$ par Φ est donc :

$$\varphi\left(\sum_{k=1}^{4} \xi_k e_k, \sum_{k=1}^{4} \xi_k e_k\right) = 2\xi_1\xi_4\varphi(e_1, e_4) + 2\xi_2\xi_3\varphi(e_2, e_3) = \xi_1\xi_4 - \xi_2\xi_3.$$

Il en résulte que Φ n'est autre que $A \longmapsto \det A$. □

5.1.4 1° Soient un entier $n \geqslant 1$ et $E = \mathcal{M}_n(\mathbb{R})$. Montrer qu'il existe une unique forme linéaire $u \in E^*$ vérifiant les deux conditions :

i) Pour tout $(A,B) \in E^2$, $u(AB) = u(BA)$;

ii) $u(I_n) = n$, où I_n est la matrice-unité d'ordre n.

2° Montrer que $A \longmapsto u(A^2)$ est une forme quadratique sur E, dont on déterminera la signature.

1° Nous utiliserons la base canonique (E_{ij}), $(i,j) \in \mathbb{N}_n^2$, de $\mathcal{M}_n(\mathbb{R})$.

Un calcul classique fournit : $E_{ij}\, E_{k\ell} = \delta_{jk}\, E_{i\ell}$.

a) Supposons qu'il existe $u \in E^*$ vérifiant i) et ii).

Pour tout $(i,j,k,\ell) \in \mathbb{N}_n^4$ nous avons : $u(E_{ij}\, E_{k\ell}) = u(E_{k\ell}\, E_{ij})$, et :

$$\delta_{jk} u(E_{i\ell}) = \delta_{\ell i} u(E_{kj})$$

et, pour $j = k$: $u(E_{i\ell}) = \delta_{\ell i} u(E_{jj})$.

Ainsi : $u(E_{i\ell}) = 0$ si $i \neq \ell$, et $u(E_{ii}) = u(E_{jj})$ pour tout (i,j) ; notons λ la valeur commune des $u(E_{ii})$.

Soit alors $A = [\alpha_{ij}] \in E$. En écrivant $A = \sum_{i,j} \alpha_{ij}\, E_{ij}$, et en utilisant la linéarité de u, il vient, compte tenu des résultats précédents :

$$u(A) = \sum_{i,j} \alpha_{ij}\, u(E_{ij}) = \sum_{i=1}^{n} \alpha_{ii} u(E_{ii}) = \lambda \sum_{i=1}^{n} \alpha_{ii} = \lambda\, \mathrm{tr}(A).$$

La condition ii) impose en outre : $\lambda\, \mathrm{tr}(I_n) = n$, i.e. $\lambda = 1$.

La seule solution éventuelle est donc l'application $\mathrm{tr} : A \mapsto \mathrm{tr}\, A$ de E dans $\mathbb{R}$.

b) Inversement celle-ci est une forme linéaire. Elle vérifie ii), et aussi i) car :

$$\mathrm{tr}(AB) = \sum_{i,j} \alpha_{ij}\beta_{ji} = \sum_{j,i} \beta_{ji}\alpha_{ij} = \mathrm{tr}(BA).$$

2° D'après 1°, $\varphi : (A,B) \mapsto \mathrm{tr}(AB)$ est une forme bilinéaire symétrique sur E, et $\Phi : A \mapsto \mathrm{tr}(A^2)$ est la forme quadratique associée.

Rappelons que la signature de Φ est $(p,q) \in \mathbb{N}^2$, où p (resp. q) est la plus grande des dimensions des sous-espaces H de E tels que la restriction de Φ à H soit définie positive (resp. définie négative).

Soit alors F (resp. G) le sous-espace de E constitué par les matrices symétriques (resp. antisymétriques). En utilisant :

$$\forall A \in E \quad \mathrm{tr}({}^tAA) = \sum_{i,j} \alpha_{ij}^2$$

on constate que $\Phi(A) = \sum_{i,j} \alpha_{ij}^2$ pour tout $A \in F$, et $\Phi(A) = -\sum_{i,j} \alpha_{ij}^2$ pour tout $A \in G$, si bien que la restriction de Φ à F (resp. G) est définie positive (resp. définie négative). On a donc :

$$p \geqslant \dim F = n(n+1)/2 \ ; \ q \geqslant \dim G = n(n-1)/2.$$

Comme par ailleurs $p+q \leqslant n^2$, on en déduit $p+q = n^2$, et :

$$(p,q) = \big(n(n+1)/2,\ n(n-1)/2\big).$$

Notons que $p+q = n^2$ montre que Φ est non dégénérée.

Remarque. On peut retrouver (p,q) en partant de :

$$\Phi(A) = \sum_{i=1}^{n} \alpha_{ii}^2 + 2 \sum_{1\leqslant i<j\leqslant n} \alpha_{ij}\alpha_{ji}$$

qui s'écrit :

$$\Phi(A) = \sum_{i=1}^{n} \alpha_{ii}^2 + \frac{1}{2} \sum_{1\leqslant i<j\leqslant n} (\alpha_{ij}+\alpha_{ji})^2 - \frac{1}{2} \sum_{1\leqslant i<j\leqslant n} (\alpha_{ij}-\alpha_{ji})^2$$

Cette décomposition en carrés fait intervenir les n^2 formes linéaires :

$$(A \mapsto \alpha_{ii})_{1\leqslant i\leqslant n} \; ; \; (A \mapsto \alpha_{ij}+\alpha_{ji})_{1\leqslant i<j\leqslant n} \; ; \; (A \mapsto \alpha_{ij}-\alpha_{ji})_{1\leqslant i<j\leqslant n}$$

qui forment une famille libre dans l'espace vectoriel $\mathcal{L}(E^*)$, de dimension n^2.

5.1.5 Une forme quadratique Φ sur $\mathbf{R}^n$, définie positive, est donnée par :

$$\Phi(x_1,\ldots,x_n) = \sum_{i=1}^{n} \alpha_{ii}x_i^2 + 2 \sum_{1\leqslant i<j\leqslant n} \alpha_{ij}x_ix_j.$$

Trouver la signature de la forme quadratique Ψ qui à $(x_1,\ldots,x_n)$ associe :

$$\sum_{i=1}^{n} (\alpha_{nn}\alpha_{ii}-\alpha_{in}^2)x_i^2 + 2 \sum_{1\leqslant i<j\leqslant n} (\alpha_{nn}\alpha_{ij}-\alpha_{in}\alpha_{jn})x_ix_j.$$

Soient φ la forme polaire de Φ, et ε_n le vecteur $(0,\ldots,0,1)$ de $\mathbf{R}^n$. En notant $x = (x_1,\ldots,x_n)$, il vient :

$$\Psi(x) = \alpha_{nn}\Phi(x) - \left(\sum_{i=1}^{n} \alpha_{in}x_i\right)^2$$

et :
$$\Psi(x) = \Phi(\varepsilon_n)\Phi(x) - \big(\varphi(\varepsilon_n,x)\big)^2$$

ce qui montre que Ψ est une forme quadratique sur $\mathbf{R}^n$, qui est positive d'après l'inégalité de Schwarz appliquée à la forme positive Φ ; celle-ci étant en outre définie, on a $\Psi(x) = 0$ si, et seulement si ε_n et x sont colinéaires.

Le cône isotrope de Ψ, qui est aussi son noyau puisque Ψ est positive, est ainsi la droite $\mathbf{R}\varepsilon_n$. La signature de Ψ est donc (n-1,0).

5.1.6 $P \in \mathbf{R}[X]$ est dit positif quand $P(t) \geqslant 0$ pour tout $t \in \mathbf{R}$.

Soit $n \in \mathbf{N}^*$. Pour tout $(\alpha_o,\alpha_1,\ldots,\alpha_{2n}) \in \mathbf{R}^{2n+1}$, vérifier l'équivalence de :

i) La forme quadratique $\Phi : (\xi_o,\ldots,\xi_n) \mapsto \sum_{i=o}^{n} \sum_{j=o}^{n} \alpha_{i+j}\xi_i\xi_j$ est positive.

ii) Pour tout polynôme positif $P \in \mathbf{R}_{2n}[X]$, le polynôme :

$$A_P = \alpha_o P + \frac{\alpha_1}{1!} P' + \ldots + \frac{\alpha_{2n}}{(2n)!} P^{(2n)} \text{ est positif.}$$

a) Montrons d'abord que ii) équivaut à :

iii) Pour tout $Q \in \mathbf{R}_n[X]$, le polynôme A_{Q^2} est positif.

Il est clair que ii) $\Rightarrow$ iii). On prouve iii) $\Rightarrow$ ii) en utilisant : tout $P \in \mathbf{R}_{2n}[X]$ positif est la somme des carrés de deux éléments de $\mathbf{R}_n[X]$ (cf. exercice 2.1.10). □

b) Reste à prouver : i) $\Leftrightarrow$ iii).

Pour tout $Q \in \mathbf{R}_n[X]$ on a (dérivées successives d'un produit) :

$$A_{Q^2} = \sum_{k=0}^{2n} \sum_{\ell=0}^{k} \alpha_k \frac{Q^{(\ell)}}{\ell!} \frac{Q^{(k-\ell)}}{(k-\ell)!}$$

et, compte tenu de $Q^m = 0$ pour $m > n$:

$$A_{Q^2} = \sum_{i=0}^{n} \sum_{j=0}^{n} \alpha_{i+j} \frac{Q^{(i)}}{i!} \frac{Q^{(j)}}{j!}$$

Pour tous $Q \in \mathbf{R}_n[X]$ et $x \in \mathbf{R}$, on a donc :

$$A_{Q^2}(x) = \Phi\left(\frac{Q(x)}{0!}, \frac{Q'(x)}{1!}, \ldots, \frac{Q^{(n)}}{n!}\right) \qquad (1)$$

• Preuve de i) $\Rightarrow$ iii). Conséquence immédiate de (1). □

• Preuve de iii) $\Rightarrow$ i). Par hypothèse iii) est vraie. On en retient que, pour tout $(\xi_0, \ldots, \xi_n) \in \mathbf{R}^{n+1}$, le polynôme $Q = \xi_0 + \xi_1 X + \ldots + \xi_n X^n$ vérifie $A_{Q^2}(0) \geqslant 0$, ce qui, compte tenu de (1) et de $Q^{(k)}(0) = k!\xi_k$, $0 \leqslant k \leqslant n$, s'écrit $\Phi(\xi_0, \ldots, \xi_n) \geqslant 0$. □

• *Voici une application de l'exercice précédent.*

5.1.7 Soient (α_i) et (β_i), $i \in \{0, \ldots, 2n\}$, deux familles de réels. On leur associe la famille (γ_i), $i \in \{0, \ldots, 2n\}$, par :

$$\gamma_i = \sum_{k=0}^{i} C_i^k \alpha_k \beta_{i-k}$$

On note Φ_1, Φ_2 et Φ_3 les formes quadratiques sur $\mathbf{R}^{n+1}$ qui à $(x_0, \ldots, x_n)$ font correspondre respectivement :

$$\sum_{i=0}^{n} \sum_{j=0}^{n} \alpha_{i+j} \xi_i \xi_j \; ; \; \sum_{i=0}^{n} \sum_{j=0}^{n} \beta_{i+j} \xi_i \xi_j$$

et : $$\sum_{i=0}^{n} \sum_{i=0}^{n} \gamma_{i+j} \xi_i \xi_j \; .$$

Montrer que si Φ_1 et Φ_2 sont positives, alors Φ_3 est positive.

• Par hypothèse, Φ_1 et Φ_2 sont positives.

• Soit $P \in \mathbf{R}_{2n}[X]$. Pour $t \in \mathbf{R}$, $\sum_{i=0}^{2n} \frac{\gamma_i}{i!} P^{(i)}(t)$ s'écrit :

$$\sum_{i=0}^{2n} \left(\sum_{k=0}^{i} \frac{\alpha_k}{k!} \frac{\beta_{i-k}}{(i-k)!} P^{(i)}(t) \right)$$

et aussi :

$$\sum_{k=o}^{2n} \frac{\alpha_k}{k!} \left(\sum_{i=k}^{2n} \frac{\beta_{i-k}}{(i-k)!} P^{(i)}(t) \right)$$

et encore : $$\sum_{k=o}^{2n} \frac{\alpha_k}{k!} \left(\sum_{j=o}^{2n-k} \frac{\beta_j}{j!} P^{(j+k)}(t) \right)$$

et enfin : $$\sum_{k=o}^{2n} \frac{\alpha_k}{k!} Q^{(k)}(t), \text{ où } Q = \sum_{j=o}^{2n} \frac{\beta_j}{j!} P^{(j)}$$

(on a utilisé le fait que le polynôme $P^{(j+k)}$ est nul dès que j+k excède 2n, i.e. dès que j excède 2n-k).

Si P est en outre positif, alors, d'après la positivité de Φ_2, le polynôme Q, qui appartient à $\mathbf{R}_{2n}[X]$, est positif ; d'après la positivité de Φ_1, le polynôme $\sum_{k=o}^{2n} \frac{\alpha_k}{k!} Q^{(k)}$ est donc positif.

En conclusion, pour tout polynôme positif $P \in \mathbf{R}_{2n}[X]$, le polynôme $\sum_{i=o}^{2n} \frac{\gamma_i}{i!} P^{(i)}$ est positif ; la forme Φ_3 est donc positive. □

5.1.8 1° Soit $(\alpha_1,\ldots,\alpha_n) \in \mathbf{R}^n$. Trouver le rang de la (n,n) matrice :

$$\Omega_n = [\omega_{ij}], \text{ où } \omega_{ij} = \mathrm{ch}(\alpha_i - \alpha_j)$$

2° Retrouver le résultat en étudiant la forme quadratique Φ_n sur $\mathbf{R}^n$ qui est représentée par Ω_n dans la base canonique de $\mathbf{R}^n$.

1° Il est clair que si $\alpha_1 = \ldots = \alpha_n$, et en particulier si n = 1, alors tous les éléments de Ω_n sont des 1, et le rang de Ω_n est 1.

• Dorénavant nous supposons que $n \geqslant 2$ et que $\alpha_1,\ldots,\alpha_n$ ne sont pas tous égaux : il existe p et q tels que $1 \leqslant p < q \leqslant n$ et $\alpha_p \neq \alpha_q$. Nous constatons :

$$\begin{vmatrix} \mathrm{ch}(\alpha_p - \alpha_p) & \mathrm{ch}(\alpha_p - \alpha_q) \\ \mathrm{ch}(\alpha_q - \alpha_p) & \mathrm{ch}(\alpha_q - \alpha_q) \end{vmatrix} \neq 0$$

et nous avons : rang $\Omega_n \geqslant 2$, avec rang $\Omega_n = 2$ si n = 2.

Si, en outre, $n \geqslant 3$, considérons une sous-matrice carrée Ω' de Ω_n d'ordre m tel que $3 \leqslant m \leqslant n$. En utilisant $\mathrm{ch}(\alpha_i - \alpha_j) = \mathrm{ch}\,\alpha_i \,\mathrm{ch}\,\alpha_j - \mathrm{sh}\,\alpha_i \,\mathrm{sh}\,\alpha_j$, nous constatons que det Ω' est la somme de 2^m déterminants dont tous les vecteurs colonnes sont de la forme kC ou kS, où $k \in \mathbf{R}$ et où C et S sont des vecteurs colonnes fixes (qui ne dépendent que de Ω'). Chacun de ces 2^m déterminants est donc nul pour avoir deux vecteurs-colonnes proportionnels, et ainsi, det $\Omega' = 0$. D'où : rang $\Omega_n = 2$.

• En conclusion le rang de Ω_n est 1 si $\alpha_1 = \ldots = \alpha_n$, et 2 dans le cas contraire. □

2° On a :

$$\Phi_n(x) = \sum_{i,j} (\operatorname{ch}\alpha_i \operatorname{ch}\alpha_j - \operatorname{sh}\alpha_i \operatorname{sh}\alpha_j)\xi_i\xi_j$$

où $x = (\xi_1,\dots,\xi_n)$ et où (i,j) parcourt $\mathbb{N}_n^2$, i.e. $\Phi_n = F_n - G_n$ avec :

$$F_n(x) = \sum_{i,j} (\xi_i \operatorname{ch}\alpha_i)(\xi_j \operatorname{ch}\alpha_j) = \left(\sum_i \xi_i \operatorname{ch}\alpha_i\right)^2$$

et :

$$G_n(x) = \sum_{i,j} (\xi_i \operatorname{sh}\alpha_i)(\xi_j \operatorname{sh}\alpha_j) = \left(\sum_i \xi_i \operatorname{sh}\alpha_i\right)^2$$

Différence des carrés de deux formes linéaires dont la première au moins est non nulle, F_n est de rang 2 si ces deux formes sont linéairement indépendantes, de rang 1 dans le cas contraire, i.e. dans le cas où les coefficients des deux formes sont proportionnels, ce qui s'écrit :

$$\operatorname{th}\alpha_1 = \dots = \operatorname{th}\alpha_n \text{ , i.e. } \alpha_1 = \dots = \alpha_n. \qquad \square$$

5.1.9 1° Montrer que la forme quadratique sur $\mathbb{R}$ donnée par :

$$\Phi(x) = \sum_{i=1}^{n} \xi_i^2 + \sum_{1\le i<j\le n} \xi_i\xi_j \qquad (1)$$

est non dégénérée et positive.

2° Trouver une décomposition de Gauss de Φ, et retrouver 1°.

1° Conséquence immédiate de :

$$2\Phi(x) = \sum_{i=1}^{n} \xi_i^2 + \left(\sum_{i=1}^{n} \xi_i\right)^2$$

2° Pour $n=1$, $n=2$ et $n=3$, on a les décompositions de Gauss :

$$\Phi(x) = \xi_1^2 \; ; \; \Phi(x) = \left(\xi_1 + \frac{\xi_2}{2}\right)^2 + \frac{3}{4}\xi_2^2 \; ;$$

$$\Phi(x) = \left(\xi_1 + \frac{\xi_2+\xi_3}{2}\right)^2 + \frac{3}{4}\left(\xi_2 + \frac{\xi_3}{3}\right)^2 + \frac{4}{6}\xi_3^2 \; .$$

• Dans la suite, $n \in \mathbb{N}^*$ est fixé. L'étude des cas particuliers conduit à présumer que l'on a :

$$\Phi(x) = \sum_{k=1}^{n} \frac{k+1}{2k}\eta_k^2 \text{ , où } \eta_k = \xi_k + \frac{1}{k+1}(\xi_{k+1} + \dots + \xi_n) \qquad (2)$$

ce qui est une décomposition de Gauss puisque les matrices colonnes X et Y des ξ_k et des η_k sont liés par $Y = AX$, où A est une matrice triangulaire supérieure, à éléments diagonaux égaux à 1 ; (2) montre que Φ est non dégénérée positive.

• Nous allons prouver par récurrence que, pour tout $q \in \{1,\dots,n\}$, est vraie l'assertion :

$$(\mathcal{A}_q) \qquad \Phi(x) = \sum_{k=1}^{q-1} \frac{k+1}{2k}\eta_k^2 + \frac{q+1}{2q} R_q(x)$$

avec : $R_q(x) = \sum_{i=q}^{n} \xi_i^2 + \frac{2}{q+1} \sum_{q<i<j\leqslant n} \xi_i \xi_j$.

ce qui entraînera que (2) est vraie ((2) n'est autre que $\mathcal{A}_n$).

- $(\mathcal{A}_1)$ est vraie, d'après (1).
- Soit $q \in \{1,\dots,n\}$ pour lequel $(\mathcal{A}_q)$ est vraie. $R_q(x)$ s'écrit :

$$\xi_q^2 + \frac{2}{q+1} \xi_q \sum_{j=q+1}^{n} \xi_j + \sum_{i=q+1}^{n} \xi_i^2 + \frac{2}{q+1} \sum_{q+1\leqslant i<j\leqslant n} \xi_i \xi_j$$

et : $$\eta_q^2 + \left(1 - \frac{1}{(q+1)^2}\right) \sum_{i=q+1}^{n} \xi_i^2 + \frac{2}{q+1} \left(1 - \frac{1}{q+1}\right) \sum_{q+1\leqslant i<j\leqslant n} \xi_i \xi_j$$

On en déduit que $\frac{q+1}{2q} R_q(x)$ s'écrit :

$$\frac{q+1}{2q} \eta_q^2 + \frac{q+2}{2(q+1)} \sum_{i=q+1}^{n} \xi_i^2 + \frac{1}{q+1} \sum_{q+1\leqslant i<j\leqslant n} \xi_i \xi_j$$

et : $$\frac{q+1}{2q} \eta_q^2 + \frac{q+2}{2(q+1)} R_{q+1}(x).$$

Il en résulte que $(\mathcal{A}_{q+1})$ est vraie. □

5.1.10 Soient E un $\mathbb{R}$-espace vectoriel de dimension finie $n>0$, et Φ une forme quadratique sur E de signature $(n-1,1)$.

1° Soit F un sous-espace de E de dimension p, qui contient un vecteur a tel que $\Phi(a)<0$. Quelle est la signature de la restriction de Φ à F ?

2° Donner une méthode permettant de déterminer les hyperplans H de E tels que la restriction de Φ à H soit positive non dégénérée.

Application. $E=\mathbb{R}^3$, et $\Phi(x,y,z) = x^2 + 2y^2 - 2z^2 - yz - 3zx + 3xy$.

Les deux questions (qui sont indépendantes) font appel à :

Lemme. Soient E un $\mathbb{R}$-espace vectoriel de dimension finie, et Φ une forme quadratique sur E, de forme polaire φ. Si E est somme directe φ-orthogonale d'une famille $(E_i)_{1\leqslant i\leqslant m}$ de sous-espaces, alors la signature de Φ s'obtient par addition dans $\mathbb{N}^2$ des signatures des restrictions Φ_i (de formes polaires φ_i) de Φ aux E_i.

On sait en effet que chaque E_i admet une base φ_i-orthogonale e_i. On constate que la réunion e des e_i est une base φ-orthogonale de E, et on étudie les signes des éléments de la matrice diagonale qui représente Φ dans cette base.□

• Dans notre exercice, la signature de Φ est de la forme (p,q) avec $p+q=n$, ce qui montre que Φ est non dégénérée. Nous savons que, dans ces conditions, tout sous-espace non φ-isotrope G de E admet un supplémentaire φ-orthogonal.

1° D'après $\Phi(a)<0$, la droite $D=\mathbb{R}a$ est non isotrope ; elle admet donc un supplémentaire φ-orthogonal, qui est un hyperplan H de E ; d'après le lemme,

la signature de la restriction Φ_H de Φ à H est :

$$(n-1,1) - (0,1) = (n-1,0), \text{ avec } \dim H = n-1.$$

Φ_H est ainsi positive et non dégénérée (i.e. définie positive) et il en est de même pour la restriction Φ_L de Φ au sous espace $L = H \cap F$ de H.

E étant somme directe φ-orthogonale de D et de H, on en déduit, compte tenu de $D \subset F$, que F est somme directe ψ-orthogonale de D et de L (ψ est la forme polaire de la restriction Ψ de Φ à F). En particulier on a : $\dim L = p-1$, et la signature de Φ_L est $(p-1,0)$; celle de Ψ est donc :

$$(0,1) + (p-1,0) = (p-1,1). \qquad \square$$

2° D'après le début du 1°, pour tout $a \in E$ tel que $\Phi(a) < 0$, le φ-orthogonal de la droite Ra est un hyperplan qui répond à la question. Montrons que l'on a ainsi toutes les solutions.

Soit H une solution. La restriction de Φ à H étant non dégénérée, H est non φ-isotrope, et admet un supplémentaire φ-orthogonal, qui est une droite D de E ; la signature de la restriction de Φ à D est :

$$(n-1,1) - (n-1,0) = (0,1).$$

Il existe donc un $a \in D$ tel que $\Phi(a) < 0$. $\square$

Application. Cherchons d'abord la signature de Φ. Par Gauss :

$$\Phi(x,y,z) = \left(x + \frac{3}{2}y - \frac{3}{2}z\right)^2 - \frac{1}{4}(y-7z)^2 + 8z^2.$$

La signature de Φ est (2,1) ; la dimension de E est 3. L'étude s'applique. Le plan H d'équation $\alpha x + \beta y + \gamma z = 0$, avec $(\alpha,\beta,\gamma) \neq (0,0,0)$ répond à la question si et seulement s'il existe un vecteur $a = (u,v,w)$ de $\mathbf{R}^3$ tel que $\Phi(u,v,w) < 0$ et que le φ-orthogonal de Ra soit H. Cette dernière condition s'écrit :

$$\left(u + \frac{3}{2}v - \frac{3}{2}w\right)x + \left(\frac{3}{2}u + 2v - \frac{1}{2}w\right)y + \left(-\frac{3}{2}u - \frac{1}{2}v - 2w\right)z = 0$$

est une équation de H, i.e. il existe $\lambda \in \mathbf{R}^*$ tel que :

$$(2u + 3v - 3w = \lambda\alpha) \wedge (3u + 4v - w = \lambda\beta) \wedge (-3u - v - 4w = \lambda\gamma).$$

Ce système linéaire à l'inconnue (u,v,w) est sûrement cramérien et, quitte à remplacer a par un vecteur colinéaire non nul, on peut choisir λ de façon que sa solution s'écrive :

$$\left(\begin{vmatrix} \alpha & 3 & -3 \\ \beta & 4 & -1 \\ \gamma & -1 & -4 \end{vmatrix}, \begin{vmatrix} 2 & \alpha & -3 \\ 3 & \beta & -1 \\ -3 & \gamma & -4 \end{vmatrix}, \begin{vmatrix} 2 & 3 & \alpha \\ 3 & 4 & \beta \\ -3 & -1 & \gamma \end{vmatrix} \right)$$

i.e. $(-17\alpha + 15\beta + 9\gamma,\ 15\alpha - 17\beta - 7\gamma,\ 9\alpha - 7\beta - \gamma)$.

Reste à écrire que, pour ce dernier vecteur, $\Phi(u,v,w) < 0$ (ce qui assure $(\alpha,\beta,\gamma) \neq (0,0,0)$).

En conclusion, la restriction de Φ au plan H d'équations $\alpha x + \beta y + \gamma z = 0$ est positive non dégénérée si, et seulement si :

$$17\alpha^2 + 17\beta^2 + \gamma^2 - 30\alpha\beta - 18\alpha\gamma + 14\beta\gamma < 0.$$

5.2. Espaces euclidiens. Espaces hermitiens

- *Une forme sesquilinéaire φ sur un $\mathbb{C}$-espace vectoriel E est telle que :*

  $x \mapsto \varphi(x,y)$ *est semi linéaire ;* $y \mapsto \varphi(x,y)$ *est linéaire.*

  Une forme sesquilinéaire hermitienne vérifie en outre :

  $\varphi(y,x) = \overline{\varphi(x,y)}$ *pour tout* $(x,y) \in E^2$

  En dimension finie, et dans une base quelconque, une telle forme s'écrit :

  $(X,Y) \mapsto X^*AY$, *avec* $A^* = A$

- *Le produit scalaire d'un espace préhilbertien est écrit* $(x,y) \mapsto (x|y)$.

5.2.1 DETERMINANT DE GRAM. Soit $x = (x_1,\dots,x_n)$ une famille de vecteurs d'un espace E préhilbertien réel ou complexe. On appelle déterminant de Gram de x, et on note Gram(x), le déterminant de la "matrice de Gram" $[(x_i|x_j)]$, $(i,j) \in \mathbb{N}_n^2$.

Montrer que x est libre si, et seulement si Gram(x) est non nul.

• Supposons d'abord que la famille x est liée : il existe $k \in \mathbb{N}_n$ tel que x_k soit une combinaison linéaire des autres vecteurs de x. Le k-ième vecteur-colonne de la matrice de Gram de x est ainsi une combinaison linéaire des autres vecteurs-colonnes et Gram(x) = 0.

• Inversement, supposons maintenant que la famille x est libre ; x est donc une base du sous-espace F de E qu'elle engendre. Le produit scalaire de E induit sur F une structure d'espace euclidien (resp. hermitien). Soient e une base orthonormale de F et $P = P_e^x$. Le produit scalaire de F est représenté dans la base e par I_n, et dans la base x par la matrice de Gram de x ; d'après les formules de changement de bases pour une forme quadratique (resp. hermitienne), celle-ci s'écrit ${}^tPI_nP$ (P^*I_nP dans le cas hermitien). D'où : $\text{Gram}(x) = |\det P|^2 > 0$. □

Remarque. Dans tous les cas, Gram(x) est un réel positif.

5.2.2 Soient E un espace euclidien (resp. hermitien) de dimension $n > 0$, $x = (x_i)_{i\in I}$ et $y = (y_i)_{i\in I}$ des familles de vecteurs de E. Prouver l'équivalence de :

i) Il existe un automorphisme orthogonal (resp. unitaire) u de E tel que :

$\forall i \in I \quad u(x_i) = y_i$

ii) $\forall (i,j) \in I^2 \quad (x_i|x_j) = (y_i|y_j)$.

a) Preuve de i) $\Rightarrow$ ii). Si i) est vraie, on a, pour tout $(i,j) \in I^2$,

$$(x_i|x_j) = \big(u(x_i)\,|\,u(x_j)\big) = (y_i|y_j). \qquad \square$$

b) Preuve de ii) $\Rightarrow$ i). Par hypothèse, ii) est vraie.

• Remarquons d'abord que, cf. exercice 5.2.1, pour toute partie finie I' de I, on a $\mathrm{Gram}(x_i)_{i\in I'} = \mathrm{Gram}(y_i)_{i\in I'}$; On en déduit que les familles x et y ont un rang commun r. Les sous-espaces F et G de E respectivement engendrés par x et y sont de dimension r.

Il existe $J \subset I$ telle que $(x_i)_{i\in J}$ soit une base de F ; $\mathrm{Gram}(x_i)_{i\in J}$ est non nul et donc $\mathrm{Gram}(y_i)_{i\in J}$ est non nul ; $(y_i)_{i\in J}$ est une base de G.

• Etudions d'abord le cas $r = n$. Ici $F = G = E$ et il existe un unique automorphisme u de E tel que $u(x_i) = y_i$ pour tout $i \in J$.

Considérons deux éléments quelconques $z = \sum_{i\in J} \xi_i x_i$ et $z' = \sum_{i\in J} \xi'_i x_i$ de E ; nous avons ((i,j) décrivant J^2) :

$$\big(u(z)\,|\,u(z')\big) = \Big(\sum_i \xi_i y_i \,\Big|\, \sum_j \xi'_j y_j\Big) = \sum_{i,j} \bar{\xi}_i \xi'_j (y_i|y_j)$$

$$= \sum_{i,j} \bar{\xi}_i \xi'_j (x_i|x_j) = (z|z').$$

Il en résulte que u est orthogonal (resp. unitaire).

En particulier, soit $i \in I$; pour tout $j \in J$ nous avons :

$$(y_i|y_j) = (x_i|x_j) = \big(u(x_i)\,|\,u(x_j)\big) = \big(u(x_i)|y_j\big)$$

et $u(x_i) - y_i$ est orthogonal à tout y_j, $j \in J$, et donc à E.

L'automorphisme u vérifie ainsi : $u(x_i) = y_i$ pour tout $i \in I$. $\square$

• Etudions maintenant le cas $r < n$. F et G admettent des supplémentaires orthogonaux F' et G' de dimension commune n-r.

Choisissons arbitrairement des bases orthonormales de F' et G' que, pour harmoniser la notation, nous écrirons $(x_i)_{i\in L}$ et $(y_i)_{i\in L}$, bien qu'il ne s'agisse évidemment pas de sous-familles de x et y (on a $I \cap L = \phi$). Nous avons : $(x_i|x_j) = \delta_{ij} = (y_i|y_j)$ pour tout $(i,j) \in L^2$, et nous constatons aisément que :

$$\forall (i,j) \in (I \cup L)^2 \quad (x_i|x_j) = (y_i|y_j).$$

Comme $(x_i)_{i\in I\cup L}$ et $(y_i)_{i\in I\cup L}$ engendrent E, d'après ce qui précède il existe un automorphisme orthogonal (resp. unitaire) u tel que $u(x_i) = y_i$ pour tout $i \in I \cup L$, et, en particulier, pour tout $i \in I$. $\square$

Remarquons que u n'est unique que si $r = n$.

5.2.3 1° Soit E un espace préhilbertien réel. Une famille $(x_i)_{i\in I}$ de vecteurs de E est dite *obtusangle* si et seulement si :

$$\forall (i,j) \in I^2 \quad (i \neq j) \Rightarrow \big((x_i|x_j) < 0\big).$$

Pour tout $p \in \mathbb{N}^*$, montrer que si $(x_1,\ldots,x_p,x_{p+1})$ est une famille obtusangle, alors $(x_1,\ldots,x_p)$ est une famille libre.

2° Quel est le nombre maximum des vecteurs d'une famille obtusangle dans un espace euclidien de dimension $n \in \mathbb{N}^*$?

Notons qu'aucun vecteur d'une famille obtusangle d'au moins deux éléments n'est nul, et que toute sous-famille d'une famille obtusangle est elle-même obtusangle.

1° Il s'agit de montrer qu'une assertion $(\mathcal{A}_p)$ est vraie pour tout $p \in \mathbb{N}^*$.

- $(\mathcal{A}_1)$ est vraie car, si $p=1$ et si (x_1,x_2) est obtusangle, alors $x_1 \neq 0$ et (x_1) est libre.

- Soit $p \in \mathbb{N}^*$ pour lequel $(\mathcal{A}_p)$ a été vérifiée. Nous allons montrer par l'absurde que, $(x_1,\ldots,x_{p+1},x_{p+2})$ désignant une famille obtusangle, la famille $(x_1,\ldots,x_{p+1})$ est libre.

Pour cela, faisons l'hypothèse (H) : $(x_1,\ldots,x_{p+1})$ est liée.

Comme - d'après $(\mathcal{A}_p)$ appliquée à $(x_1,\ldots,x_{p+1})$ qui est obtusangle - $(x_1,\ldots,x_p)$ est libre, on a : $x_{p+1} = \sum_{i=1}^{p} \alpha_i x_i$.

Ecrivons $\|x_{p+1}\|^2 > 0$, i.e. $\sum_{i=1}^{p} \alpha_i (x_i|x_{p+1}) > 0$.

Comme $(x_i|x_{p+1}) < 0$ pour tout $i \in \mathbb{N}_p$, il existe au moins un $i \in \mathbb{N}_p$ tel que $\alpha_i < 0$ et, $x_1,\ldots,x_p$ jouant des rôles symétriques, on peut supposer $\alpha_p < 0$.

La famille $(x_1,\ldots,x_{p-1}, x_{p+1}-\alpha_p x_p, x_{p+2})$ est obtusangle. En effet :

$$\forall i \in \mathbb{N}_{p+2} \setminus \{p,p+1\} \quad (x_i|x_{p+1}-\alpha_p x_p) = (x_i|x_{p+1}) - \alpha_p (x_i|x_p) < 0.$$

La famille $x = (x_1,\ldots,x_{p-1}, x_{p+1}-\alpha_p x_p)$ est donc libre (d'après $(\mathcal{A}_p)$). Mais cette famille est liée à cause de : $x_{p+1}-\alpha_p x_p = \sum_{i=1}^{p-1} \alpha_i x_i$.

Conduisant à une contradiction, l'hypothèse (H) est absurde. □

2° Une famille obtusangle d'un espace euclidien E de dimension n ne peut avoir plus de n+1 éléments, sans quoi il existerait une famille libre de plus de n éléments de E.

Inversement, l'exercice suivant montre que, dans tout espace euclidien de dimension n, il existe une famille obtusangle de n+1 éléments. Le lecteur pourra établir directement ce résultat par récurrence sur n.

5.2.4 Soit E un espace préhilbertien réel. Une famille $(x_i)_{i\in I}$ de vecteurs unitaires de E est dite *φ-équiangulaire* si, et seulement s'il existe un réel

$\varphi \in]0,\pi]$ tel que :

$$(i,j) \in I^2 \qquad (i \neq j) \Rightarrow \big((x_i | x_j) = \cos\varphi\big)$$

1° Soit $(x_1,\ldots,x_p)$, $p \in \mathbb{N}^*$, une famille φ-équiangulaire.

a) Montrer que si $p \geqslant 2$ et $\varphi \in]\pi/2,\pi]$, alors $(x_1,\ldots,x_{p-1})$ est libre.

b) Montrer que si $\varphi \in]0,\pi/2]$, alors $(x_1,\ldots,x_p)$ est libre.

c) Montrer : $1 + (p-1)\cos\varphi \geqslant 0$.

2° Ici E est euclidien de dimension $n > 0$.

a) Montrer que pour toute famille φ-équiangulaire de n+1 vecteurs de E on a : $\cos\varphi = -1/n$.

b) Trouver toutes les familles φ-équiangulaires de n+1 vecteurs de E.

1° a) La famille $(x_1,\ldots,x_p)$ est ici obtusangle. On applique le 1° de l'exercice précédent (on a le droit de le faire grâce à $p \geqslant 2$). □

b) Ici : $0 \leqslant \cos\varphi < 1$. Soit $(\xi_i)_{1\leqslant i\leqslant p}$ une famille de réels vérifiant :

$$\sum_{i=1}^{p} \xi_i x_i = 0.$$

En multipliant scalairement par x_j, $j \in \mathbb{N}_p$, on obtient :

$$(1-\cos\varphi)\xi_j + \left(\sum_{i=1}^{p} \xi_i\right) \cos\varphi = 0$$

ce qui, compte tenu de $1 \neq \cos\varphi$, exige que les ξ_j aient une valeur commune ξ, avec :

$$\xi\big(1 + (p-1)\cos\varphi\big) = 0$$

et donc avec $\xi = 0$ puisque $\cos\varphi \geqslant 0$. □

c) Pour tous $p \in \mathbb{N}^*$ et $\varphi \in]0,\pi]$, on a :

$$\forall i \in \mathbb{N}_p \qquad (x_i \,|\, x_1 + \ldots + x_p) = 1 + (p-1)\cos\varphi$$

et donc : $\|x_1 + \ldots + x_p\|^2 = p\big(1 + (p-1)\cos\varphi\big)$, $p \in \mathbb{N}^*$. □

2° a) Il s'agit de vérifier qu'une assertion $(\mathcal{A}_n)$ est vraie pour tout $n \in \mathbb{N}^*$.

Procédons par récurrence.

- $(\mathcal{A}_1)$ est vraie car si $n = 1$ les familles φ-équiangulaires de deux vecteurs de E sont les $(x,-x)$, où x est l'un des deux vecteurs unitaires de E ; ici $\varphi = \pi$ et $\cos\varphi = -1$.

- Soit $n \geqslant 2$ tel que $(\mathcal{A}_{n-1})$ ait été vérifiée. Considérons un espace euclidien E de dimension n et une famille φ-équiangulaire $(x_1,\ldots,x_{n+1})$ de vecteurs unitaires de E. On a (cf. 1° c)) : $1 + n\cos\varphi \geqslant 0$, et donc $\sin\varphi > 0$.

Pour tout $i \in \mathbb{N}_n$, z_i désigne la projection orthogonale de x_i sur l'hyperplan $F = (\mathbb{R}x_{n+1})^{\perp}$ de E, qui est euclidien pour la structure induite par celle de E. Compte tenu de $(x_i | x_{n+1}) = \cos\varphi$, on a :

$$z_i = x_i - x_{n+1}\cos\varphi.$$

Il en résulte : $\|z_i\|^2 = 1 - \cos^2\varphi = \sin^2\varphi$, i.e. $\|z_i\| = \sin\varphi$ (car $\sin\varphi > 0$), et :

$$(z_i|z_j) = \cos\varphi(1-\cos\varphi) \text{ pour } (i,j) \in \mathbb{N}_n^2 \text{ et } i \neq j.$$

En notant $y_i = \frac{1}{\sin\varphi} z_i$, on constate que la famille $(y_1,\ldots,y_n)$ de vecteurs unitaires de F est ψ-angulaire, avec $\cos\psi = \frac{\cos\varphi}{1+\cos\varphi}$.

On peut lui appliquer $(\mathcal{H}_{n-1})$ et écrire : $\cos\psi = -1/(n-1)$, ce qui entraîne $\cos\varphi = -1/n$ (en effet : $\dim F = n-1$). □

Remarque. Soit $(x_1,\ldots,x_{n+1})$ une famille φ-équiangulaire de vecteurs unitaires de l'espace euclidien E de dimension n. La famille est obtusangle.

Elle vérifie : $x_1 + \ldots + x_{n+1} = 0$ (cf. démonstration du 1°c)).

A tout $i \in \mathbb{N}_n$ associons le vecteur unitaire y_i défini comme ci-dessus et le vecteur unitaire :

$$e_i = y_i \sin\alpha + x_{n+1}\cos\alpha, \text{ où } \alpha = \text{Arc cos } 1/\sqrt{n}.$$

Pour $i \neq j$: $(e_i|e_j) = (y_i|y_j)\sin^2\alpha + \cos^2\alpha$

$$= \frac{-1}{n-1}\left(1 - \frac{1}{n}\right) + \frac{1}{n} = 0.$$

La famille $(e_1,\ldots,e_n)$ est une base orthonormale de E ; compte-tenu de $y_1 + \ldots + y_n = 0$, on a : $x_{n+1} = (e_1 + \ldots + e_n)\cos\alpha$.

b) Le cas n = 1, déjà traité, étant mis à part, toute construction d'une famille φ-équiangulaire de n+1 vecteurs d'un espace euclidien E de dimension n, exige que l'on retrouve la situation de la remarque du a).

- Nous partons donc d'une base orthonormale $(e_1,\ldots,e_n)$ de E, arbitrairement choisie, et nous ne pouvons que lui associer les vecteurs, visiblement unitaires :

$$x_{n+1} = (e_1 + \ldots + e_n)\cos\alpha, \text{ où } \alpha = \text{Arc cos } 1/\sqrt{n},$$

$$y_i = \frac{1}{\sin\alpha}(e_i - x_{n+1}\cos\alpha), \; i \in \mathbb{N}_n,$$

$$x_i = y_i \sin\varphi + x_{n+1}\cos\varphi, \; i \in \mathbb{N}_n, \; \varphi = \text{Arc cos}(-1/n).$$

Il est clair que $(x_i|x_{n+1}) = \cos\varphi$, et que, pour $i \neq j$:

$$(x_i|x_j) = (y_i|y_j)\sin^2\varphi + \cos^2\varphi .$$

Comme $(y_i|y_j) = \frac{-\cos^2\alpha}{\sin^2\alpha} = \frac{-1}{n-1} = \frac{\cos\varphi}{1+\cos\varphi}$, on a $(x_i|x_j) = \cos\varphi$.

La famille $(x_1,\ldots,x_{n+1})$ est effectivement une solution.

- Les autres solutions devant être construites par le même procédé à partir des autres bases orthonormales de E, toutes les solutions sont les familles :

$\big(u(x_1),\ldots,u(x_{n+1})\big)$, où u est un automorphisme orthogonal de E.

(Ce dernier résultat est d'ailleurs une application de l'exercice 5.2.2).

Remarque. Au passage, nous avons démontré l'existence d'une famille obtusangle de n+1 vecteurs d'un espace euclidien de dimension n (résultat utilisé au 2° de l'exercice précédent).

5.2.5 Soient E un espace euclidien de dimension $n \geqslant 3$, k un vecteur unitaire de E, s la symétrie orthogonale par rapport à la droite $\mathbb{R}k$.

1° Montrer que $\varphi : (x,y) \mapsto (x|s(y))$ est une forme bilinéaire symétrique. Quelle est la signature de la forme quadratique Φ de forme polaire φ ?

2° On note C le cône isotrope de Φ. On donne $a \in E$ tel que $\Phi(a) > 0$.

a) Soit $H = \{x \in E \mid \varphi(x,a) = 0\}$. Montrer que, pour tout $x \in H$ on a $\Phi(x) \leqslant 0$. Déterminer $C \cap H$.

b) Ici $x \in E$ est fixé. Soit $D = \{x + \lambda a \mid \lambda \in \mathbb{R}\}$. Montrer que $C \cap D$ est constitué de deux points, sauf dans un cas que l'on précisera.

c) Quel est le noyau de la forme quadratique :

$$\Psi : x \mapsto \varphi^2(x,a) - \Phi(a)\Phi(x) \ ?$$

1° Soit $(e_1,\ldots,e_n)$ une base orthonormale de E telle que $e_n = k$.

En notant $(\xi_1,\ldots,\xi_n)$ et $(\eta_1,\ldots,\eta_n)$ les coordonnées de x et y, il vient:

$$\varphi(x,y) = -\xi_1\eta_1 - \ldots - \xi_{n-1}\eta_{n-1} + \xi_n\eta_n$$

ce qui montre que φ est une forme bilinéaire symétrique ; Φ a pour signature $(1,n-1)$, et est donc non dégénérée. □

Dorénavant nous écrirons ξ pour ξ_n et η pour η_n ; ainsi :

$$\varphi(x,y) = 2\xi\eta - (x|y) \ ; \ \Phi(x) = 2\xi^2 - \|x\|^2$$

2° L'hypothèse $\Phi(a) > 0$ s'écrit : $2\alpha^2 > \|a\|^2$.

a) Soit $x \in H$, ce qui s'écrit : $2\xi\alpha = (x|a)$; on a :

$$\Phi(x) = 2\xi^2 - \|x\|^2 = \frac{(x|a)^2}{2\alpha^2} - \|x\|^2$$

et donc : $$\Phi(x) \leqslant \frac{(x|a)^2 - \|a\|^2\|x\|^2}{2\alpha^2} \leqslant 0$$

(la seconde inégalité étant justifiée par Cauchy Schwarz). □

- Si à $x \in H$ on ajoute $x \in C$, i.e. $\Phi(x) = 0$, alors nécessairement :

$$\Phi(x) = (x|a)^2 - \|a\|^2\|x\|^2 = 0, \text{ i.e. } (\Phi(x) = 0) \wedge (x \in \mathbb{R}a)$$

ce qui, compte tenu de $\Phi(a) \neq 0$, s'écrit $x = 0$.

Inversement, il est clair que $0 \in C \cap H$. Finalement : $C \cap H = \{0\}$.

Remarque. H est l'hyperplan $(\mathbb{R}b)^\perp$, où $b = s(a)$ vérifie $\Phi(b) > 0$. En fait, nous avons montré que, pour tout $b \in E$ tel que $\Phi(b) > 0$, on a $C \cap (\mathbb{R}b)^\perp = \{0\}$.

b) D est la droite affine définie par le point x et le vecteur directeur a. L'équation "aux λ" des points d'intersection de C et D est $\Phi(x+\lambda a) = 0$, i.e. :

$$\lambda^2\Phi(a) + 2\lambda\varphi(x,a) + \Phi(x) = 0 \qquad (\&_x)$$

Comme $\Phi(a) > 0$, il est clair que si $\Phi(x) < 0$, alors $\&_x$ a deux racines distinctes.

D'après $\Phi(x) = 2\xi^2 - \|x\|^2$, il en est ainsi (en particulier) si $x \in (\mathbb{R}k)^\perp$, et $x \neq 0$. Essayons de nous ramener à ce cas. D coupe l'hyperplan $(\mathbb{R}k)^\perp$ en un unique point $y = x - \xi\alpha^{-1}a$, tel que $\Phi(y) = -\|y\|^2$.

On peut définir D par ce point y et le vecteur a. $C \cap D$ est donc constitué de deux points distincts, sauf si $y = 0$, i.e. $x \in \mathbb{R}a$, auquel cas $C \cap D = \{0\}$.

c) Somme de deux formes quadratiques, Ψ est une forme quadratique.

Pour tout $x \in E$, $\Psi(x)$ est le discriminant de l'équation $(\&_x)$, qui a deux racines si $x \notin \mathbb{R}a$, et une seule si $x \in \mathbb{R}a$. La forme Ψ est donc positive, de cône isotrope $\mathbb{R}a$; la positivité fait que le noyau de Ψ coïncide avec son cône isotrope. □

Remarque. Dans le cas $n = 3$, le lecteur pourra justifier sans calcul les résultats de 2° a) et b). E étant muni de sa structure affine canonique, il utilisera en a) le/un plan de symétrie de l'ensemble C ∪ H (plan $(0;(k,b))$, et en b) le/un plan contenant 0 et D.

5.2.6 Soit E un espace euclidien de dimension 3. On se propose de montrer que le groupe $\mathcal{R}$ des rotations de E est *simple*, i.e. que les seuls sous-groupes distingués de $\mathcal{R}$ sont $\{Id_E\}$ et $\mathcal{R}$.

$\mathcal{U}$ est l'ensemble des vecteurs unitaires de E ; pour tout $x \in \mathcal{U}$, s_x désigne la symétrie orthogonale par rapport à la droite $\mathbb{R}x$.

1° Montrer que, pour tout $(x,y) \in \mathcal{U}^2$, il existe $r \in \mathcal{R}$ tel que $rs_yr^{-1} = s_x$.

2° Soit $\mathcal{G}$ un sous-groupe distingué de $\mathcal{R}$ distinct de $\{Id_E\}$.

a) Montrer qu'il existe une rotation non identique $\rho \in \mathcal{G}$ telle que $(u|\rho(u)) \leq 0$ pour tout $u \in \mathcal{U}$ orthogonal à l'axe de ρ, et qu'il existe $v \in \mathcal{U}$ tel que $(v|\rho(v)) = 0$.

b) En déduire qu'il existe une symétrie $s_y \in \mathcal{G}$, et conclure.

1° Soit $(x,y) \in \mathcal{U}^2$. Pour toute $r \in \mathcal{R}$, $\tau = rs_yr^{-1}$ est une rotation (produit de rotations) involutive ($\tau^2 = Id_E$ est évident), distincte de Id_E (sans quoi on aurait $rs_y = r$ et $s_y = Id_E$), et elle conserve visiblement le vecteur unitaire $r(y)$; τ est donc $s_{r(y)}$. Il suffit de choisir r de façon que $r(y) = x$ (ce qui est possible d'une infinité de manières) pour avoir $\tau = s_x$. □

2° Il s'agit de montrer que $\mathcal{G} = \mathcal{R}$, i.e. que $\mathcal{G}$ contient toute $r \in \mathcal{R}$. Comme toute rotation peut être considérée comme le produit des symétries orthogonales par rapport à deux droites, il suffit de montrer : $s_x \in \mathcal{G}$ pour <u>tout</u> $x \in \mathcal{U}$.

Mieux, il suffit de montrer qu'il existe <u>un</u> $y \in \mathcal{U}$ tel que $s_y \in \mathcal{G}$. En effet, s'il en est ainsi, pour tout $x \in \mathcal{U}$ on dispose, d'après 1°, d'une $r \in \mathcal{R}$ telle que s_x coïncide avec $rs_y r^{-1}$, qui appartient au sous-groupe $\mathcal{G}$ (puisque celui-ci est distingué).

a) D'après $\mathcal{G} \neq \{Id_E\}$, il existe une rotation non identique $r \in \mathcal{G}$. Soient $\omega \in \mathcal{U}$ invariant par r, et $u \in \mathcal{U}$ orthogonal à ω ; ayant orienté E, on dispose de $p = \omega \wedge u$. On pose :

$$r(u) = u\cos\theta + p\sin\theta \ ; \ \text{d'où} : \big(u \mid r(u)\big) = \cos\theta.$$

Quitte à remplacer ω par $-\omega$, on peut supposer $0 < \theta \leqslant \pi$. Si $\pi/2 \leqslant \theta \leqslant \pi$, on adopte $\rho = r$. Sinon, il existe $k \in \mathbb{N}^*$ (pas nécessairement unique) tel que $\pi/2 \leqslant k\theta \leqslant \pi$, et on adopte $\rho = r^k$ (qui appartient à $\mathcal{G}$). □

- L'existence de ρ étant acquise, on considère un vecteur unitaire :

$$v = u\cos\varphi + \omega\sin\varphi, \text{ avec } 0 \leqslant \varphi < \pi/2.$$

On a : $\big(v \mid \rho(v)\big) = \big(u \mid \rho(u)\big)\cos^2\varphi + \sin^2\varphi$, ce qui, comme $\big(u \mid \rho(u)\big) < 0$ permet de choisir φ de façon que $\big(v \mid \rho(v)\big) = 0$. □

b) Le groupe $\mathcal{G}$ étant distingué, de $\rho \in \mathcal{G}$ on déduit :

$$s_v \rho s_v = s_v \rho s_v^{-1} \in \mathcal{G}$$

et donc : $s_v \rho s_v \rho^{-1} \in \mathcal{G}$ (puisque ρ^{-1} appartient aussi à $\mathcal{G}$).

Mais (d'après 1°) $\rho s_v \rho^{-1} = s_{\rho(v)}$, et donc $s_v s_{\rho(v)} \in \mathcal{G}$, où v et $\rho(v)$ sont des vecteurs unitaires orthogonaux, ce qui s'écrit $s_y \in \mathcal{G}$, où y est le vecteur unitaire $v \wedge \rho(v)$. □

5.2.7 Soit $A = [\alpha_{ij}]$ une (n,n) matrice orthogonale réelle ; on note σ la somme de ses éléments. Vérifier $|\sigma| \leqslant n$.

$\mathbf{R}^n$ est muni de sa structure euclidienne canonique : la base canonique $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n)$ est orthonormale. On note $e = (e_1, \ldots, e_n)$ la base orthonormale de $\mathbf{R}^n$ telle que A soit la matrice de passage de ε à e. Ainsi :

$$\forall j \in \mathbb{N}_n \quad e_j = \sum_{i=1}^{n} \alpha_{ij}\varepsilon_i$$

dont on déduit :

$$\forall (i,j) \in \mathbb{N}_n^2 \quad (\varepsilon_i \mid e_j) = \alpha_{ij}$$

et donc : $$\sigma = \Big(\sum_{i=1}^{n} \varepsilon_i \mid \sum_{j=1}^{n} e_j\Big).$$

Retenons : $\sigma^2 \leqslant \left\| \sum_{i=1}^{n} \varepsilon_i \right\|^2 \times \left\| \sum_{j=1}^{n} e_j \right\|^2$.

S'agissant de familles orthonormales :

$$\left\| \sum_{i=1}^{n} \varepsilon_i \right\|^2 = \left(\sum_{i=1}^{n} \varepsilon_i \,\middle|\, \sum_{i=1}^{n} \varepsilon_i \right) = \sum_{i=1}^{n} \|\varepsilon_i\|^2 = n$$

et, de même : $\left\| \sum_{j=1}^{n} e_j \right\|^2 = n$. □

5.2.8 1° a) Soit $A \in \mathcal{M}_n(\mathbb{R})$ antisymétrique. Montrer que :

$$(I+B)(I+A) = 2I \quad (I : \text{matrice unité } (n,n)) \tag{1}$$

définit une unique $B \in \mathcal{M}_n(\mathbb{R})$, que B est orthogonale $\left(B \in O(n)\right)$, et qu'elle n'admet pas -1 pour valeur propre.

b) Soit $B \in O(n)$, n'admettant pas -1 pour valeur propre. Montrer que (1) définit une unique $A \in \mathcal{M}_n(\mathbb{R})$, et que A est antisymétrique.

2° Montrer que les (3,3) matrices réelles orthogonales droites sont les matrices de la forme :

$$S = \begin{bmatrix} \alpha^2-\beta^2-\gamma^2+\delta^2 & 2(\alpha\beta-\gamma\delta) & 2(\gamma\alpha+\beta\delta) \\ 2(\alpha\beta+\gamma\delta) & -\alpha^2+\beta^2-\gamma^2+\delta^2 & 2(\beta\gamma-\alpha\delta) \\ 2(\gamma\alpha-\beta\delta) & 2(\beta\gamma+\alpha\delta) & -\alpha^2-\beta^2+\gamma^2+\delta^2 \end{bmatrix}$$

avec $(\alpha,\beta,\gamma,\delta) \in \mathbb{R}^4$ et $\alpha^2+\beta^2+\gamma^2+\delta^2 = 1$.

Pour toute (n,n) matrice M on a : $(I+M)(I-M) = (I-M)(I+M)$.

Si I-M est inversible, on a, en multipliant à droite et à gauche par $(I-M)^{-1}$:

$$(I-M)^{-1}(I+M) = (I+M)(I-M)^{-1} \tag{2}$$

1° a) Soit $A \in \mathcal{M}_n(\mathbb{R})$ antisymétrique.

Au titre d'élément de $\mathcal{M}_n(\mathbb{C})$, A est antihermitienne ; iA est hermitienne, et donc à valeurs propres réelles ; les valeurs propres de A sont imaginaires pures. On en déduit que $A \in \mathcal{M}_n(\mathbb{R})$ n'admet pas de valeur propre sauf, éventuellement, 0 ; I+A et I-A sont donc inversibles et (1) définit, sans ambiguité :

$$B = -I + 2(I+A)^{-1}.$$

En utilisant : $I = (I+A)(I+A)^{-1}$, on obtient : $B = (I-A)(I+A)^{-1}$.

D'où : $B^{-1} = (I+A)(I-A)^{-1}$

et aussi, compte tenu de ${}^tA = -A$, ${}^tI = I$ et ${}^t(M^{-1}) = ({}^tM)^{-1}$:

$${}^tB = (I-A)^{-1}(I+A).$$

En utilisant (2), on en déduit $B^{-1} = {}^tB$; B est donc orthogonale.

- D'après (1), I+B est inversible ; -1 n'est pas valeur propre de B. □

Remarque. Pour toute $M \in O(n)$, le polynôme caractéristique χ_M s'écrit :

$$(X-1)^p(X+1)^q \prod_{k=1}^{m}(X^2-2X\cos\theta_k+1), \quad \theta_k \in]0,\pi[. \tag{3}$$

On a : $\det M = (-1)^q$; M est donc droite $\left(M \in SO(n)\right)$ si, et seulement si q est pair, condition remplie si -1 n'est pas valeur propre de M.

Ici $\det B = 1$ se retrouve en utilisant :

$$\det B = \frac{\det(I-A)}{\det(I+A)} \text{ et } (I-A) = {}^t(I+A).$$

b) Soit $B \in O(n)$, n'admettant pas -1 pour valeur propre $\left(\text{on a : } B \in SO(n)\right)$. De : I+B est inversible, on déduit que (1) définit, sans ambiguité :

$$A = -I + 2(I+B)^{-1} .$$

En utilisant : $I = (I+B)(I+B)^{-1}$, on obtient : $A = (I-B)(I+B)^{-1}$.

D'où, compte tenu de ${}^tB = B^{-1}$:

$${}^tA = (I+B^{-1})^{-1}(I-B^{-1}) = (B+I)^{-1}(B-I).$$

En utilisant (2), on en déduit : ${}^tA = -A$; A est donc antisymétrique.

2° a) D'après le 1°, $B \in \mathcal{M}_3(\mathbb{R})$ est orthogonale droite, n'admettant pas -1 pour valeur propre, si, et seulement s'il existe $(a,b,c) \in \mathbb{R}^3$ tel que :

$$B = -I+2(I+A)^{-1}, \text{ où } A = \begin{bmatrix} 0 & c & -b \\ -c & 0 & a \\ b & -a & 0 \end{bmatrix}$$

On calcule successivement I+A, $\det(I+A)$, $(I+A)^{-1}$; on trouve :

$$B = \frac{1}{a^2+b^2+c^2+1}\begin{bmatrix} a^2-b^2-c^2+1 & 2(ab-c) & 2(ca+b) \\ 2(ab+c) & -a^2+b^2-c^2+1 & 2(bc-a) \\ 2(ca-b) & 2(bc+a) & -a^2-b^2+c^2+1 \end{bmatrix}$$

Pour obtenir une expression homogène, on pose :

$$a = \alpha\delta^{-1} \quad , \; b = \beta\delta^{-1} \quad , \; c = \gamma\delta^{-1}$$

où δ est choisi de façon que : $\delta^2(a^2+b^2+c^2+1) = 1$, ce qui entraîne :

$$\alpha^2+\beta^2+\gamma^2+\delta^2 = 1.$$

On aboutit ainsi à la forme : $B = S$.

b) Etudions maintenant $B \in SO(3)$ admettant -1 pour valeur propre.

D'après (3), -1 est racine double de χ_B, et 1 en est racine simple. On en déduit aisément que, $\mathbb{R}^3$ étant muni de sa structure euclidienne canonique, B représente dans la base canonique (e_1,e_2,e_3), qui est orthonormale, une symétrie orthogonale par rapport à une droite. Un calcul classique montre que, cette droite étant notée $\mathbb{R}k$, avec $k = \alpha e_1+\beta e_2+\gamma e_3$ et $\alpha^2+\beta^2+\gamma^2 = 1$, la matrice B s'écrit :

$$\begin{bmatrix} 2\alpha^2-1 & 2\alpha\beta & 2\gamma\alpha \\ 2\alpha\beta & 2\beta^2-1 & 2\beta\gamma \\ 2\gamma\alpha & 2\beta\gamma & 2\gamma^2-1 \end{bmatrix}$$

On reconnaît la matrice S dans laquelle $\delta = 0$. □

5.2.9 Soient E un espace hermitien et u une application de E dans E vérifiant :

$$\forall (x,y) \in E^2 \quad \big(u(x)\,|\,u(y)\big) = (y|x) \tag{1}$$

Montrer que u est semi-linéaire.

E, qui est hermitien, admet une base orthonormale $(e_1,\ldots,e_n)$. On a :

$$\forall (i,j) \in \mathbb{N}_n^2 \quad \big(u(e_i)\,|\,u(e_j)\big) = (e_j|e_i) = \delta_{ij}.$$

Ainsi $\big(u(e_1),\ldots,u(e_n)\big)$ est une base orthonormale de E.

Pour tout $x \in E$, on a :

$$x = \sum_{i=1}^{n} \xi_i e_i \ , \quad \text{avec } \xi_i = (e_i|x),$$

et :
$$u(x) = \sum_{i=1}^{n} \xi'_i u(e_i), \quad \text{avec } \xi'_i = \big(u(e_i)\,|\,u(x)\big).$$

En utilisant (1) : $\xi'_i = (x|e_i) = \overline{\xi}_i$. D'où :

$$u(x) = \sum_{i=1}^{n} \overline{\xi}_i\, u(e_i).$$

Il est alors clair que u est semi-linéaire. □

5.2.10 $\mathbb{C}^3$ étant muni de sa structure hermitienne canonique, soit $u \in \mathcal{L}(\mathbb{C}^3)$ représenté dans la base canonique $(\varepsilon_1,\varepsilon_2,\varepsilon_3)$ par la matrice :

$$A = \begin{bmatrix} 0 & -2 & -1 \\ 2 & 0 & 2 \\ 1 & -2 & 0 \end{bmatrix}$$

Trouver les bases orthonormales de $\mathbb{C}^3$ qui diagonalisent u.

• La base canonique étant orthonormale, et A étant anti-hermitienne l'endomorphisme u est anti-hermitien. Comme iu est hermitien, il existe des bases orthonormales de $\mathbb{C}^3$ qui diagonalisent iu. Or une base diagonalise u si, et seulement si elle diagonalise iu.

• Le polynôme caractéristique de u est $X(X^2+9)$; les valeurs propres sont :

$$\lambda_1 = 0 \ ; \quad \lambda_2 = 3i \ ; \quad \lambda_3 = -3i.$$

On constate que les sous-espaces propres associés sont $\mathbb{C}e_1$, $\mathbb{C}e_2$, $\mathbb{C}e_3$, avec $e_1 = (2,1,-2)$, $e_2 = (4+3i,2-6i,5)$, $e_3 = (4-3i,2+6i,5)$.

Deux vecteurs propres associés à des valeurs propres distinctes étant orthogonaux, aussi bien pour u que pour iu, (e_1,e_2,e_3) est une base orthogonale de $\mathbb{C}^3$ (ce qu'il est aisé de vérifier directement). Nous allons la normer en utilisant : $\|e_1\|^2 = 9$, et :

$$\|e_2\|^2 = \|e_3\|^2 = |4+3i|^2 + |2-6i|^2 + 25 = 90.$$

Nous disposons ainsi de la base orthonormale de $\mathbb{C}$, (c_1,c_2,c_3), où :

$$c_1 = \frac{e_1}{3}\ ,\ c_2 = \frac{e_2}{3\sqrt{10}}\ ,\ c_3 = \frac{e_3}{3\sqrt{10}}\ .$$

Dans cette base, u est représenté par diag(0,3i,-3i). Comme on peut remplacer c_1,c_2,c_3 par les vecteurs opposés, on a 8 solutions.

5.2.11 Soient E un espace hermitien et a un vecteur unitaire de E.

A tout $k\in\mathbb{C}$ on associe $u\in\mathcal{L}(E)$ défini par :

$$x \mapsto x + k(a|x)a.$$

A quelle condition u est-il :

1° bijectif ? (on explicitera u^{-1}) ;

2° hermitien ? ; 3° unitaire ?

La linéarité de u tient à celle de $p : x \mapsto (a|x)a$, qui est le projecteur orthogonal sur la droite $\mathbb{C}a$. On a :

$$u = Id_E + kp = (k+1)p + q$$

où $q = Id_E - p$ est le projecteur orthogonal sur l'hyperplan $(\mathbb{C}a)^\perp$.

Soit $e = (e_1,\ldots,e_n)$ une base orthonormale de E telle que $e_1 = a$ et que $(e_2,\ldots,e_n)$ soit une base orthonormale de $(\mathbb{C}a)^\perp$. On a :

$$Mat(u;e) = D \quad \text{où} \quad D = diag(k+1,1,\ldots,1).$$

1° Pour que u soit bijectif, il faut et il suffit que D soit inversible, i.e. que $k+1 \neq 0$. Lorsque cette condition est remplie on a :

$$D^{-1} = diag\left(\frac{1}{k+1},1,\ldots,1\right) \quad \text{et} \quad u^{-1} = Id_E - \frac{k}{k+1}\,p.$$

2° Pour que u soit hermitien, il faut et il suffit que D soit hermitienne, i.e. que $k\in\mathbb{R}$.

3° Pour que u soit unitaire, il faut et il suffit que D le soit, i.e. que $DD^* = I_n$, ce qui s'écrit $|k+1| = 1$. □

5.2.12 Soient E et F des K-espaces vectoriels et $u\in\mathcal{L}(E,F)$. On cherche toutes les $u'\in\mathcal{L}(F,E)$ vérifiant : $uu'u = u$ et $u'uu' = u'$. (1)

a) Montrer que si u' est une solution, alors :

$$\operatorname{Ker} u \oplus \operatorname{Im} u' = E \quad \text{et} \quad \operatorname{Ker} u' \oplus \operatorname{Im} u = F.$$

b) Inversement, montrer que, pour tout couple (E',F') où E' est un supplémentaire de Ker u dans E et F' un supplémentaire de Im u dans F, il existe une unique $u' \in \mathcal{L}(F,E)$ vérifiant :

$$uu'u = u \quad \text{et} \quad u'uu' = u' \quad \text{et} \quad \operatorname{Ker} u' = F' \quad \text{et} \quad \operatorname{Im} u' = E'. \qquad (2)$$

c) Conclure.

a) De (1) on déduit u'uu'u = u'u ; p = u'u est donc un projecteur de E.

De p = u'u et u = up on déduit Ker p = Ker u.

De p = u'u et u' = pu' on déduit Im p = Im u'.

Commer Ker p ⊕ Im p = E, il vient Ker u ⊕ Im u' = E.

- On montre de même que q = uu' est le projecteur de F de noyau Ker u' et d'image Im u, ce qui entraîne Ker u' ⊕ Im u = F. □

b) Soit un couple (E',F') (dont on admet l'existence si E et F sont de dimension infinie). Nous savons que u induit un isomorphisme $\bar{u}$ de E' (supplémentaire de son noyau) sur son image Im u.

• Supposons qu'il existe $u' \in \mathcal{L}(F,E)$ vérifiant (2). D'après a), uu' est le projecteur q de F de noyau F' et d'image Im u. Pour tout $y \in F$ nous avons :

$$\big(u'(y) \in E'\big) \wedge \big(uu'(y) = q(y)\big) \quad \text{i.e.} \quad u'(y) = (\bar{u})^{-1}\big(q(y)\big).$$

• Si (2) admet une solution, celle-ci est donc $v : y \mapsto (\bar{u})^{-1}\big(q(y)\big)$.

• Inversement cette application v est linéaire, de noyau F' et d'image E' ; elle vérifie uv = q, et donc uvu = qu = u et vuv = vq = v. C'est l'unique solution de (2).

c) Il est clair que, quand (E',F') décrit l'ensemble des couples formés d'un supplémentaire de Ker u dans E et d'un supplémentaire de Im u dans F, la solution v de (2) liée à (E',F') décrit l'ensemble des solutions de (1).

Remarque. Si u est un isomorphisme, le seul choix possible de (E',F') est $(E,\{0_F\})$; (1) admet u^{-1} pour solution unique, ce que l'on peut d'ailleurs constater directement.

5.2.13 Soient E et F des espaces euclidiens (resp. hermitiens) et $u \in \mathcal{L}(E,F)$. On note u^+ l'unique élément de $\mathcal{L}(F,E)$ qui vérifie (cf. exercice précédent) :

$$uu^+u = u \ ; \ u^+uu^+ = u^+ \ ; \ \operatorname{Ker} u^+ = (\operatorname{Im} u)^\perp \ , \ \operatorname{Im} u^+ = (\operatorname{Ker} u)^\perp.$$

1° Montrer que, pour tout $y_o \in F$, $x_o = u^+(y_o)$ est la <u>meilleure solution approchée en norme</u> de l'équation $u(x) = y_o$, ce qui signifie que :

i) Pour tout $x \in E$, on a $\|u(x)-y_o\| \geqslant \|u(x_o)-y_o\|$;

et ii) Pour tout $x \in E \setminus \{x_o\}$ tel que $\|u(x)-y_o\| = \|u(x_o)-y_o\|$, on a $\|x\| > \|x_o\|$.

2° a) Montrer qu'il existe un unique $u^* \in \mathcal{L}(F,E)$ vérifiant :

$$\forall (x,y) \in E \times F \quad (u(x)|y)_F = (x|u^*(y))_E . \qquad (1)$$

Déterminer le noyau et l'image de u^*.

b) Montrer que si u est injectif, alors : $u^+ = (u^*u)^{-1}u^*$, et que, si u est surjectif, alors : $u^+ = u^*(uu^*)^{-1}$.

Ici $(u^+)^+ = u$; u et u^+ jouent des rôles symétriques ; on dit que u^+ est l'application *pseudo-inverse* de u.

1° On a $u(x) \in \operatorname{Im} u$ pour tout $x \in E$; d'autre part (cf. exercice précédent) $u(x_o) = uu^+(y_o)$ est la projection orthogonale $q(y_o)$ de y_o sur Im u ; d'où i).

• Pour tout $x \in E$ tel que $\|u(x)-y_o\| = \|u(x_o)-y_o\| = \|q(y_o)-y_o\|$, on a $u(x) = q(y_o) = u(x_o)$, i.e. $x-x_o \in \operatorname{Ker} u$; en outre $x_o \in (\operatorname{Ker} u)^\perp$; d'où ii). □

Remarque. On constate que x_o est l'unique solution de norme minimale de l'équation $u(x) = q(y_o)$, et n'est solution de $u(x) = y_o$ que si $y_o \in \operatorname{Im} u$ (ce qui est toujours le cas si u est surjectif). D'autre part, si u est injectif, alors x_o est la solution unique de $u(x) = q(y_o)$. Ceci explique que le calcul de u^+ à partir de u se simplifie lorsque u est injectif ou surjectif.

2° a) On rapporte E et F de dimensions m et n à des bases orthonormales e et f, et on pose : $A = \operatorname{mat}(u;e,f)$. On constate que $u^* \in \mathcal{L}(F,E)$ vérifie (1), si, et seulement si $B = \operatorname{mat}(u^*;f,e)$ vérifie (dans le cas hermitien) :

$$\forall (X,Y) \in \mathcal{M}_{m,1}(\mathbb{C}) \times \mathcal{M}_{n,1}(\mathbb{C}) \quad X^*A^*Y = X^*BY$$

ce qui s'écrit $B = A^*$. □

• En utilisant (1) on obtient :

$$\operatorname{Ker} u^* = \{y \in F \mid \forall x \in E \quad (u(x)|y) = 0\} = (\operatorname{Im} u)^\perp .$$

Comme (1) entraîne $(u^*)^* = u$, on en déduit :

$$\operatorname{Ker} u = (\operatorname{Im} u^*)^\perp, \text{ et donc : } \operatorname{Im} u^* = (\operatorname{Ker} u)^\perp .$$

• Notons que nous avons généralisé la notion d'adjoint d'un endomorphisme.

b) Ici u est injectif. Nous avons par (1) :

$$\forall x \in E \quad (x|u^*u(x)) = \|u(x)\|^2$$

dont nous déduisons : $\operatorname{Ker}(u^*u) = \operatorname{Ker} u = \{0_E\}$, et $u^*u \in GL(E)$.

Nous disposons ainsi de $u' = (u^*u)^{-1}u^* \in \mathcal{L}(F,E)$, avec $u'u = \mathrm{Id}_E$.

D'où, d'une part : $uu'u = u$ et $u'uu' = u'$, d'autre part : $\operatorname{Ker} u' = \operatorname{Ker} u^* = (\operatorname{Im} u)^\perp$, et enfin, tout $x \in E$ étant l'image de $u(x)$ par u', $\operatorname{Im} u' = E = (\operatorname{Ker} u)^\perp$.

D'après l'unicité de u^+, il en résulte : $(u^*u)^{-1}u^* = u^+$. □

• Nous laissons au lecteur le soin de vérifier : $u^*(uu^*)^{-1} = u^+$ dans le cas où u est surjectif.

5.2.14 Soient E un espace hermitien, et u un endomorphisme de E. Montrer que u commute avec u^* (i.e. est normal) si et seulement s'il existe un polynôme $P \in \mathbb{C}[X]$ tel que $u^* = P(u)$.

La condition est suffisante. Il est clair que $u^* = P(u)$ entraîne $u^*u = uu^*$. □

La condition est nécessaire. Par hypothèse $u^*u = uu^*$.

Comme u est normal, il existe une base orthonormale $e = (e_1, \ldots, e_n)$ de E telle que :

$$\mathrm{mat}(u;e) = \mathrm{diag}(\alpha_1, \ldots, \alpha_n).$$

On en déduit :

$$\mathrm{mat}(u^*;e) = \mathrm{diag}(\overline{\alpha}_1, \ldots, \overline{\alpha}_n).$$

Désignons par $\lambda_1, \ldots, \lambda_p$ les éléments distincts de l'ensemble $\{\alpha_1, \ldots, \alpha_n\}$. D'après l'étude du polynôme d'interpolation de Lagrange, il existe $P \in \mathbb{C}[X]$ tel que:

$$\forall k \in \mathbb{N}_p \quad P(\lambda_k) = \overline{\lambda}_k.$$

Il en résulte :

$$\forall i \in \mathbb{N}_n \quad P(\alpha_i) = \overline{\alpha}_i.$$

et : $\mathrm{mat}\big(P(u);e\big) = \mathrm{diag}\,\big(P(\alpha_1), \ldots, P(\alpha_1)\big) = \mathrm{mat}(u^*;e)$

et donc : $P(u) = u^*$. □

5.2.15 Soient E un espace euclidien, et $(u_i)_{i \in I}$ une famille d'endomorphismes symétriques de E. Prouver l'équivalence des assertions :

i) Les u_i commutent deux à deux.

ii) Il existe une base orthonormale de E qui diagonalise chacun des u_i.

• Il s'agit d'une extension de l'exercice 4.2.4. On s'appuie ici sur la propriété suivante, dont la démonstration est immédiate : *Pour tout endomorphisme symétrique* u *d'un espace euclidien* E, *et pour tout sous espace non nul* F *de* E *stable par* u, *l'endomorphisme* v *de* F *induit par* u *est symétrique.*

• Reste à reprendre les démonstrations du 4.2.4, en remplaçant *base* par *base orthonormale* et *diagonalisable* par *symétrique*, et en remarquant que (dans la vérification de i) ⇒ ii)) la somme directe $E = E_1 \oplus E_1'$ est ici orthogonale.

5.2.16 Soient E un espace préhilbertien réel, et u un endomorphisme de E qui admet un adjoint u^* tel que : $u^*u - uu^* = \mathrm{Id}_E$. (1)

1° Montrer que $\dim E = +\infty$, et que u est injectif.

2° On note $h = u^*u$.

a) On suppose que h admet une valeur propre λ ; soit x_o un vecteur propre associé ; on note $u^n(x_o) = x_n$ et $(u^*)^n(x_o) = y_n$, $n \in \mathbb{N}$. Vérifier :

$$h(x_n) = (\lambda+n)x_n \ ; \ h(y_n) = (\lambda-n)y_n . \qquad (2)$$

En déduire : $\lambda \in \mathbb{N}^*$.

b) Montrer que si u^* est non injectif, alors h admet des valeurs propres qui sont les entiers strictement positifs. Vérifier que, pour tout $p \in \mathbb{N}^*$, le sous-espace propre associé à la valeur propre p est $u^{p-1}(\operatorname{Ker} u^*)$.

3° Montrer que l'on obtient un exemple de la situation qui vient d'être étudiée en adoptant $E = \mathbb{R}[X]$, muni de la structure préhilbertienne :

$$\left(\sum a_n X^n \,|\, \sum b_n X^n\right) = \sum n! a_n b_n$$

et $u : P \longmapsto XP$.

1° a) Si E était de dimension finie, on aurait $\operatorname{tr}(u^*u - uu^*) = \dim E$ à cause de (1), et $\operatorname{tr}(u^*u - uu^*) = 0$ à cause de $\operatorname{tr} AB = \operatorname{tr} BA$. □

b) Pour tout $x \in \operatorname{Ker} u$, on a :

$$\|u^*(x)\|^2 = \left(u^*(x) \,|\, u^*(x)\right) = \left(x \,|\, uu^*(x)\right)$$
$$= \left(x \,|\, u^*u(x)\right) - \|x\|^2 = -\|x\|^2$$

et donc $\|x\|^2 \leqslant 0$, ce qui exige $x = 0$. □

2° On a : $h^* = (u^*u)^* = h$; h est donc symétrique.

De plus : $\left(x \,|\, u^*u(x)\right) = \|u(x)\|^2 > 0$ pour $x \neq 0$ (u est injectif).

Enfin, si $h(x_o) = \lambda x_o$ et $x_o \neq 0$, alors $\left(x_o \,|\, h(x_o)\right) = \lambda \|x_o\|^2$; toute valeur propre éventuelle de h est donc strictement positive.

a) Par hypothèse : $h(x_o) = \lambda x_o$ et $x_o \neq 0$. De $u^*u(x_o) = \lambda x_o$ on déduit, en prenant les images par u, et en utilisant $u(x_o) = x_1$:

$$uu^*(x_1) = \lambda x_1, \text{ i.e. } h(x_1) = (\lambda+1)x_1 .$$

Comme u est injectif, $x_o \neq 0$ entraîne $x_1 \neq 0$; $(\lambda+1)$ est valeur propre de h, un vecteur propre associé étant $x_1 = u(x_o)$.

Par récurrence : pour tout $n \in \mathbb{N}$, $\lambda+n$ est valeur propre de h, un vecteur propre associé étant $x_n = u^n(x_o)$.

• De $u^*u(x_o) = \lambda x_o$, i.e. $uu^*(x_o) = (\lambda-1)x_o$, on déduit, en prenant les images par u^* et en utilisant $u^*(x_o) = y_1$:

$$h(y_1) = (\lambda-1)y_1 .$$

Par récurrence : $h(y_n) = (\lambda-n)y_n$ pour tout $n \in \mathbb{N}$.

En outre : $\|y_1\|^2 = \left(u^*(x_o) \,|\, u^*(x_o)\right) = \left(x_o \,|\, uu^*(x_o)\right)$ ce qui entraîne : $\|y_1\|^2 = (\lambda-1)\|x_o\|^2$ et, par récurrence :

$$\|y_n\|^2 = (\lambda-n)(\lambda-n+1)..(\lambda-1)\|x_o\|^2 \text{ pour tout } n \in \mathbb{N}^* .$$

- Si $\lambda \in \mathbf{R}_+^*$ n'était pas entier strictement positif, on trouverait $m \in \mathbf{N}^*$ tel que $\|y_m\|^2 < 0$; d'où, nécessairement : $\lambda \in \mathbf{N}^*$.

On constate alors : $y_n = 0$ pour $n \geqslant \lambda$, $y_n \neq 0$ pour $n \in \{1,\dots,\lambda-1\}$. Ainsi : pour tout $n \in \{1,\dots,\lambda-1\}$, $\lambda - n$ est valeur propre de h, un vecteur propre associé étant $y_n = (u^*)^n(x_o)$.

•• En conclusion : si h admet une valeur propre, alors h admet une infinité de valeurs propres, qui sont les entiers strictement positifs.

b) Pour le moment, on ne fait aucune hypothèse sur l'injectivité de u^*.

A tout $p \in \mathbf{N}^*$, on associe les sous-espaces de E :

$$E_p = \{x \in E \mid h(x) = px\} \; ; \; F_p = u^{p-1}(\operatorname{Ker} u^*).$$

On va montrer par récurrence : $E_p = F_p$ pour tout $p \in \mathbf{N}^*$.

- Il est clair que $E_1 = F_1$. En effet $x \in E_1$ s'écrit $uu^*(x) = 0$, et aussi (u étant injectif) $u^*(x) = 0$, i.e. $x \in F_1$.

- Reste à montrer que, $E_p = F_p$ étant acquis ($p \geqslant 1$), on a $E_{p+1} = F_{p+1}$.

Soit $x \in E_{p+1} \setminus \{0\}$; x est vecteur propre de h, associé à la valeur propre p+1 ; d'après a), $u^*(x)$ est vecteur propre de h associé à la valeur propre p ; on a $u^*(x) \in F_p$, et donc $uu^*(x) \in F_{p+1}$. Or $uu^*(x) = h(x) - x = px$; d'où $x \in F_{p+1}$; ainsi : $E_{p+1} \subset F_{p+1}$.

Inversement soit $x \in F_{p+1}$; il existe $y \in F_p$ tel que $x = u(y)$, et donc $px = u(py)$; puisque $y \in E_p$, ceci s'écrit $px = uh(y) = uu^*u(y)$, et encore $px = uu^*(x)$, dont on déduit $h(x) = (p+1)x$ et $x \in E_{p+1}$; ainsi $F_{p+1} \subset E_{p+1}$. □

• Ajoutons maintenant l'hypothèse $\operatorname{Ker} u^* \neq \{0\}$. L'injectivité de u, et donc des u^{p-1}, fait que aucun des $E_p = F_p$ n'est réduit à $\{0\}$. Tout $p \in \mathbf{N}^*$ est valeur propre de h, le sous-espace propre associé étant F_p.

3° On constate aisément que u admet pour adjoint $u^* : P \longmapsto P'$, et que (1) est vérifié ; u^* est non injectif, $\operatorname{Ker} u^*$ étant l'ensemble des constantes ; h est $P \longmapsto XP' + P$; l'étude qui précède en fournit les valeurs propres et les sous-espaces propres, qu'il est - bien sûr - aisé d'obtenir directement.

5.3. Endomorphismes positifs, Matrices positives

Applications

• *Les notions introduites dans les deux exercices qui suivent sont utiles dans de nombreux exercices.*

5.3.1 ENDOMORPHISMES HERMITIENS POSITIFS. Soient E un espace hermitien, et h un endomorphisme hermitien de E. Prouver l'équivalence des assertions :

i) La forme hermitienne Φ sur E, associée à h par $\Phi(x) = (x|h(x))$ est positive (resp. positive, non dégénérée) ;

ii) Les valeurs propres de h sont positives (resp. strictement positives).

Lorsque ces assertions sont vraies, on dit que h est positif (resp. strictement positif).

On sait que le polynôme caractéristique de l'endomorphisme hermitien h est scindé sur $\mathbb{R}$, et que $(\alpha_1,\ldots,\alpha_n)$ désignant un système de ses racines, il existe une base orthonormale $(e_1,\ldots,e_n)$ de E telle que $h(e_i) = \alpha_i e_i$ pour tout $i \in \mathbb{N}_n$. On a :

$$\Phi\left(\sum_{i=1}^{n} \xi_i e_i\right) = \sum_{i=1}^{n} \alpha_i |\xi_i|^2 \text{ pour tout } (\xi_1,\ldots,\xi_n) \in \mathbb{C}^n \qquad (1)$$

et donc : $\Phi(e_i) = \alpha_i$ pour tout $i \in \mathbb{N}_n$. (2)

i) $\Rightarrow$ ii). Résulte de (2).

ii) $\Rightarrow$ i) . Résulte de (1). □

5.3.2 MATRICES HERMITIENNES POSITIVES. Soit H une matrice hermitienne.

Prouver l'équivalence des assertions :

i) La forme hermitienne Φ sur $\mathbb{C}^n$ associée à H par $\Phi(X) = X^* HX$ est positive (resp. positive, non dégénérée) ;

ii) Les valeurs propres de H sont positives (resp. strictement positives).

Lorsque ces assertions sont vraies, on dit que H est positive (resp. strictement positive, et aussi positive, non dégénérée).

Ici (i) équivaut en effet à : l'endomorphisme hermitien de $\mathbb{C}^n$ muni de sa structure hermitienne canonique qui est représenté par H dans la base canonique (orthonormale) est positif (resp. strictement positif). □

Une matrice hermitienne positive est ainsi représentative :

- d'un endomorphisme hermitien positif d'un espace hermitien dans une base orthonormale ;

- d'une forme hermitienne positive d'un $\mathbb{C}$-espace vectoriel (base quelconque).

Remarque. Il va de soi que le lecteur pourra se limiter à définir les endomorphismes symétriques positifs d'un espace euclidien, et les matrices réelles, symétriques positives.

5.3.3 Soient E un $\mathbb{R}$-espace vectoriel de dimension finie $n>0$, Φ une forme quadratique sur E, et $A = [\alpha_{ij}]$ la matrice qui représente Φ dans une base donnée $\varepsilon = (\varepsilon_1,\ldots,\varepsilon_n)$ de E. A tout $k \in \mathbb{N}_n$, on associe :

$$\Delta_k = \det A_k, \text{ où } A_k = [\alpha_{ij}],\ (i,j) \in \mathbb{N}_k^2.$$

1° On suppose ici : $\Delta_k \neq 0$ pour tout $k \in \mathbb{N}_n$. On pose $\Delta_o = 1$. Montrer que la signature de Φ est $(n-q,q)$, où q est le nombre des changements de signe entre deux éléments consécutifs de la famille $(\Delta_o, \Delta_1, \ldots, \Delta_n)$.

2° Montrer que Φ est positive non dégénérée (i.e. que A est strictement positive) si, et seulement si $\Delta_k > 0$ pour tout $k \in \mathbb{N}_n$.

• Les matrices A, et donc A_k sont symétriques.

• Pour tout $k \in \mathbb{N}_n$, la restriction Φ_k de Φ au sous-espace E_k de E dont une base est $(\varepsilon_1, \ldots, \varepsilon_k)$ admet A_k pour matrice dans cette base ; Φ_k est donc non dégénérée si, et seulement si $\Delta_k \neq 0$. On note φ_k la forme polaire de Φ_k.

1° Ici les Φ_k sont non dégénérées. Pour tout $k \in \mathbb{N}_n$, la signature de Φ_k s'écrit donc $\sigma_k = (p_k, q_k)$, avec $p_k + q_k = k$, et on a (en utilisant une base φ_k-orthogonale de E_k) : $\operatorname{sgn} \Delta_k = (-1)^{q_k}$.

• Soit $k \in \mathbb{N}_{n-1}$. En utilisant deux fois la définition d'une signature, on constate qu'il existe un sous-espace F_k de E_k, de dimension p_k, tel que la restriction de Φ_k à F_k soit définie positive, et que, F_k étant un sous-espace de E_{k+1}, on a : $p_{k+1} \geqslant \dim F_k$.

Ainsi $p_{k+1} \geqslant p_k$ et, symétriquement, $q_{k+1} \geqslant q_k$.

Compte tenu de $p_{k+1} + q_{k+1} = p_k + q_k + 1$, deux cas sont possibles : ou bien $\sigma_{k+1} = (p_k + 1, q_k)$, ou bien $\sigma_{k+1} = (p_k, q_k + 1)$.

Il est clair qu'ils correspondent respectivement à $\Delta_k \Delta_{k+1} > 0$ et à $\Delta_k \Delta_{k+1} < 0$.

• En utilisant $q_1 = 1$ si $\Delta_1 < 0$ et $q_1 = 0$ si $\Delta_1 > 0$, la proposition s'en déduit par une récurrence immédiate. □

2° On rappelle qu'une forme quadratique positive est non dégénérée si, et seulement si elle est définie.

• La condition est nécessaire. Par hypothèse, Φ est définie, positive. Pour tout $k \in \mathbb{N}_n$, Φ_k est donc définie positive, ce qui exige $\Delta_k > 0$.

• La condition est suffisante. Par hypothèse, $\Delta_k > 0$ pour tout $k \in \mathbb{N}_n$. L'étude du 1° s'applique, avec ici $q_k = q_1 = 0$ pour tout $k \in \mathbb{N}_n$, ce qui entraîne que Φ est positive, non dégénérée. □

5.3.4 Soit $A = [\alpha_{ij}] \in \mathcal{M}_n(\mathbb{R})$, où $\alpha_{ij} = 1/(i+j)$.
Montrer que la matrice A est strictement positive.

Première solution. On utilise l'exercice précédent. Ici (cf. 3.3.10)

$$\forall p \in \mathbb{N}_n \quad \Delta_p = \prod_{1 \leqslant i < j \leqslant p} (j-i)^2 / \prod_{i,j} (i+j) > 0. \qquad \square$$

Seconde solution. On utilise 5.3.5, 2° avec $a_i = i$ et $b_i = 1$.

5.3.5 1° Soit $f = (f_1, \ldots, f_n)$ une famille d'applications continues d'un intervalle réel $[u,v]$, $u<v$, dans $\mathbf{R}$. A tout $(i,j) \in \mathbb{N}_n^2$, on associe :

$$\alpha_{ij} = \int_u^v f_i(t) f_j(t) dt.$$

La matrice $A = [\alpha_{ij}]$ est-elle positive ? strictement positive ?

2° Etudier la matrice $A = [\alpha_{ij}]$, avec $\alpha_{ij} = (a_i b_j + a_j b_i)^{-1}$, où les a_i et les b_j sont des réels strictement positifs.

1°) La matrice $A \in \mathcal{M}_n(\mathbf{R})$ est visiblement symétrique.

Pour toute matrice ${}^tX = [\xi_1 \ldots \xi_n] \in \mathcal{M}_{1,n}(\mathbf{R})$, on a :

$${}^tXAX = \int_u^v \left(\sum_{i=1}^n \xi_i f_i(t) \right)^2 dt$$

et donc :

i) ${}^tXAX \geqslant 0$, ce qui montre que A est positive ;

ii) ${}^tXAX = 0$ si, et seulement si $\sum_{i=0}^n \xi_i f_i$ est l'élément nul du $\mathbf{R}$-espace vectoriel E des applications continues de $[u,v]$ dans $\mathbf{R}$.

De ii) on déduit que A est strictement positive si, et seulement si la famille f d'éléments de E est libre.

Remarque. Le résultat s'étend au cas où, les f_i n'étant définies et continues que sur $]u,v]$, les intégrales α_{ij} convergent.

2° Ici $u = 0$, $v = 1$, et $f_i(t) = 1/b_i . t^{-1/2+a_i/b_i}$. Le 1° s'applique (compte tenu de la remarque s'il existe $i \in \mathbb{N}_n$ tel que $a_i/b_i < 1/2$), avec $\alpha_{ij} = (a_i b_j + a_j b_i)^{-1}$. La stricte positivité de A correspond au cas où les a_i/b_i sont deux à deux distincts (ainsi que l'on s'en assure en étudiant la fonction $\sum_{i=0}^n \xi_i f_i(t)$ au voisinage de 0).

5.3.6 Soit g une application continue, positive et non nulle d'un intervalle réel $[u,v]$, $u<v$, dans $\mathbf{R}$. A tout $(i,j) \in \{0,1,\ldots,n\}$ on associe :

$$\alpha_{ij} = \int_u^v t^{i+j} g(t) dt.$$

Montrer que la matrice $A = [\alpha_{ij}]$, $(i,j) \in \{0,\ldots,n\}^2$, est inversible.

Cet exercice est voisin de celui qui précède. Nous allons prouver le résultat plus fort : la matrice symétrique A est strictement positive.

• Pour toute ${}^tX = [\xi_0 \ldots \xi_n] \in \mathcal{M}_{1,n+1}(\mathbb{R})$, on a :

$$ {}^tXAX = \int_u^v \left(\sum_{i=0}^{n} \xi_i t^i \right)^2 g(t)dt \geqslant 0. $$

• Supposons maintenant que la matrice-colonne X est non nulle. On lui associe la fonction $P_X : t \longmapsto \xi_0 + \xi_1 t + \ldots + \xi_n t^n$ qui admet un nombre fini de racines.

Par ailleurs, d'après le choix de g, il existe un sous-intervalle [u',v'] de [u,v], non réduit à un point, sur lequel g ne prend que des valeurs strictement positives. La restriction à [u',v'] de la fonction positive $t \longmapsto \big(P_X(t)\big)^2 g(t)$ est donc non nulle, et son intégrale sur [u',v'] est strictement positive. D'où, a fortiori, ${}^tXAX > 0$. □

5.3.7 Soient E un espace euclidien (resp. hermitien), u et v des endomorphismes symétriques positifs (resp. hermitiens positifs) de E. Vérifier :

$$ 0 \leqslant \mathrm{tr}(uv) \leqslant \mathrm{tr}\ u.\mathrm{tr}\ v\ . $$

On sait qu'il existe une base orthonormale $(e_1,\ldots,e_n)$ de E qui diagonalise v; dans cette base, u et v sont représentés par des matrices de la forme :

$$ A = [\alpha_{ij}] \quad \text{et} \quad D = \mathrm{diag}(\lambda_1 \ldots \lambda_n). $$

On a : $$ \mathrm{tr}(uv) = \mathrm{tr}(AD) = \sum_{j=1}^{n} \alpha_{jj}\lambda_j. $$

Or, d'après la positivité de u et de v :

$$ \alpha_{jj} = \big(e_j \big| u(e_j)\big) \in \mathbb{R}_+ \quad \text{et} \quad \lambda_j = \big(e_j \big| v(e_j)\big) \in \mathbb{R}_+. $$

D'où : $$ 0 \leqslant \mathrm{tr}(uv) \leqslant \left(\sum_{j=1}^{n} \alpha_{jj} \right) \left(\sum_{j=1}^{n} \lambda_j \right) = \mathrm{tr}\ u.\mathrm{tr}\ v. $$ □

Traduction matricielle. Pour tout couple (A,B) de (n,n) matrices réelles symétriques et positives (resp. hermitiennes positives), on a :

$$ 0 \leqslant \mathrm{tr}(AB) \leqslant \mathrm{tr}\ A.\mathrm{tr}\ B. $$

5.3.8 On note $\mathcal{T}_n$ l'ensemble des (n,n) matrices réelles (resp. complexes) triangulaires supérieures à éléments diagonaux dans $\mathbb{R}_+^*$.

1° Soit E un espace euclidien (resp. hermitien) de dimension n. Montrer qu'à toute base ε de E on peut associer une unique base orthonormale b de E telle que $P_\varepsilon^b \in \mathcal{T}_n$.

2° Soit M une (n,n) matrice réelle (resp. complexe) inversible. Montrer qu'il existe une unique $T \in \mathcal{T}_n$ telle que MT soit orthogonale (resp. unitaire).

3° Soit A une (n,n) matrice réelle symétrique (resp. hermitienne) strictement positive. Montrer qu'il existe une unique $B \in \mathcal{T}_n$ telle que $A = B^* B$ (B^* est mis pour ${}^t B$ dans le cas réel).

On note $A = [\alpha_{ij}]$. Montrer $0 < \det A \leqslant \prod_{j=1}^{n} \alpha_{jj}$. Cas d'égalité ?

D'après 3.2.10 toute matrice de $\mathcal{T}_n$ est inversible, à inverse dans $\mathcal{T}_n$.

1° Il s'agit de justifier le procédé d'orthonormalisation de Schmidt, ce qui consiste à montrer qu'à toute base ε de E on peut associer une unique base orthonormale b de E telle que :

$$\forall j \in \mathbb{N}_n \quad [\mathrm{Vect}(b_1,\ldots,b_j) = \mathrm{Vect}(\varepsilon_1,\ldots,\varepsilon_j)] \wedge [(b_j|\varepsilon_j) \in \mathbb{R}_+^*]. \quad (1)$$

• Soit ε une base quelconque de E. Supposons qu'il existe une base orthonormale b telle que $P_\varepsilon^b \in \mathcal{T}_n$, ce qui s'écrit $P_b^\varepsilon \in \mathcal{T}_n$, et donc (1).

On a : $$\forall j \in \mathbb{N}_n \quad \left[\varepsilon_j = \sum_{i=1}^{j} (b_i|\varepsilon_j) b_i\right] \wedge [(b_j|\varepsilon_j) \in \mathbb{R}_+^*].$$

D'où :

$$b_j = \frac{1}{(b_j|\varepsilon_j)}\, e_j, \text{ où } e_j = \varepsilon_j - \sum_{i=1}^{j-1} (b_i|\varepsilon_j) b_i \quad (2)$$

ce qui fournit : $\|e_j\| = (b_j|\varepsilon_j)$.

Nécessairement, pour tout $j \in \mathbb{N}_n$, on a : $b_j = e_j / \|e_j\|$ avec :

$$e_j = \varepsilon_j - \sum_{i=1}^{j-1} \frac{(e_i|\varepsilon_j)}{\|e_i\|^2}\, e_i. \quad (3)$$

- Inversement, on constate qu'à partir de $e_1 = \varepsilon_1$, (3) fournit (par récurrence sur j) une unique famille $e = (e_1,\ldots,e_n)$, que celle-ci est orthogonale, formée de vecteurs non nuls et telle que :

$$\forall j \in \mathbb{N}_n \quad [\mathrm{Vect}(e_1,\ldots,e_j) = \mathrm{Vect}(\varepsilon_1,\ldots,\varepsilon_j)] \wedge [(e_j|\varepsilon_j) = \|e_j\|^2].$$

En posant $b_j = e_j / \|e_j\|$, on a $(b_j|\varepsilon_j) = \|e_j\| \in \mathbb{R}_+^*$, et on constate que la famille $(b_1,\ldots,b_n)$ est une base orthonormale de E qui vérifie (1). □

Remarques. a) P_ε^e et donc P_e^ε sont triangulaires supérieures à élément diagonaux égaux à 1.

b) Dans le calcul pratique des b_j, on utilise (2) plutôt que (3).

2° Ici E est $\mathbb{R}^n$ (resp. $\mathbb{C}^n$) muni de sa structure euclidienne (resp. hermitienne) canonique. On note c la base canonique, qui est orthonormale, et ε la base quelconque définie par $P_c^\varepsilon = M$. D'après 1°, il existe une unique base b orthonormale (i.e. telle que $A = P_c^b$ soit orthogonale ou unitaire) pour laquelle $T = P_\varepsilon^b$ appartient à $\mathcal{T}_n$. On a $A = P_c^\varepsilon P_\varepsilon^b = MT$. □

Remarque. Cette décomposition fournit un calcul pratique de $M^{-1} = TA^{-1}$, avec $A^{-1} = {}^t A$ (resp. $A^{-1} = A^*$).

En fait, pour des raisons de "propagation des erreurs d'arrondis", on n'utilise pas la méthode de Schmidt, mais une récurrence (méthode de Householder) conduisant à la décomposition de M sous la forme M = AR, A orthogonale ou unitaire, R triangulaire.

3° Ici E est $\mathbf{R}^n$ (resp. $\mathbb{C}^n$). La forme quadratique (resp. hermitienne) sur E, Φ de forme polaire φ, représentée par A dans la base canonique est positive, non dégénérée. On dispose donc de l'espace euclidien (resp. hermitien) (E,φ). La base canonique de E, qui est ici notée ε, n'est en général pas φ-orthonormale.

Pour toute $B \in \mathcal{T}_n$, on a $A = B^* B = B^* I_n B$ si, et seulement si Φ est représentée par I_n dans la base b définie par $P_b^{\varepsilon} = B$, i.e. si et seulement si cette base b est φ-orthonormale. Or (cf. 1°), il existe une unique base φ-orthonormale b telle que $P_b^{\varepsilon} \in \mathcal{T}_n$. □

Remarque. La décomposition $A = B^* B$ permet de ramener la résolution d'un système linéaire à celle de deux systèmes à matrices triangulaires. La détermination de la matrice B se fait assez facilement par coefficients indéterminés.

En pratique, lorsqu'elle s'applique, cette méthode est préférable à la méthode de Gauss.

• Soit $[\beta_{ij}]$ la matrice $B \in \mathcal{T}_n$ telle que $A = [\alpha_{ij}] = B^* B$.

Pour tout $j \in \mathbf{N}_n$, on a : $\alpha_{jj} = \sum_{i=1}^{j} |\beta_{ij}|^2 \geqslant (\beta_{jj})^2$, $(\beta_{jj} \in \mathbf{R}_+^*)$.

Comme $\det A = \det B^* \det B = \left(\prod_{j=1}^{n} \beta_{jj} \right)^2$, il vient :

$$0 < \det A \leqslant \prod_{j=1}^{n} \alpha_{jj}$$

avec égalité si et seulement si $\beta_{ij} = 0$ pour tout (i,j) tel que $i < j$, ce qui s'écrit : B est diagonale, et encore : A est diagonale. □

Remarque. Si A est positive, sans l'être strictement, on a $\det A = 0$; d'autre part Φ est ici positive dégénérée, et les $\alpha_{ii} = \Phi(\varepsilon_i)$ sont des réels positifs. On a :

$$0 = \det A \leqslant \prod_{j=1}^{n} \alpha_{jj}.$$

5.3.9 Soit $M = [\mu_{ij}]$ une (n,n) matrice réelle (resp. complexe). Vérifier :

$$|\det M|^2 \leqslant \prod_{j=1}^{n} \left(\sum_{i=1}^{n} |\mu_{ij}|^2 \right) \quad \text{(inégalité d'Hadamard).}$$

$A = M^* M = [\alpha_{ij}]$ est symétrique (resp. hermitienne) positive (d'après : pour tout $X \in \mathcal{M}_{n,1}(\mathbb{C})$, on a $X^* A X = (MX)^* (MX) \geqslant 0$), et (cf. exercice précédent) on a :

$$|\det M|^2 = \det A \leqslant \prod_{j=1}^{n} \alpha_{jj}, \text{ avec } \alpha_{jj} = \sum_{i=1}^{n} |\mu_{ij}|^2. \qquad \square$$

Si $\mathbf{R}^n$ (resp. $\mathbb{C}^n$) est muni de sa structure euclidienne (resp. hermitienne) canonique, $|\det M|$ est majoré par le produit des normes des vecteurs-colonnes de M.

5.3.10 1° Soit $A \in \mathcal{M}_n(\mathbb{R})$ antisymétrique. Montrer : $\det(I_n+A) \geqslant 1$.

2° Soient $S \in \mathcal{M}_n(\mathbb{R})$ symétrique positive, et $T \in \mathcal{M}_n(\mathbb{R})$ antisymétrique.

Montrer : $\det(S+T) \geqslant \det S$ (1)

(On pourra commencer par le cas où S est strictement positive).

1° Considérons A comme un élément de $\mathcal{M}_n(\mathbb{C})$; A est antihermitienne, iA est hermitienne et donc les racines de son polynôme caractéristique sont réelles; les racines sur $\mathbb{C}$ du polynôme caractéristique χ_A de A, dont les coefficients sont réels, sont imaginaires pures, et s'écrivent donc ; $i\alpha_1, -i\alpha_1, \ldots, i\alpha_p, -i\alpha_p, 0, \ldots, 0$ avec $2p \leqslant n$ et $\alpha_k > 0$ pour tout $k \in \mathbb{N}_p$. D'où l'expression, valable aussi bien dans $\mathbb{R}[X]$ que dans $\mathbb{C}[X]$:

$$\det(XI_n - A) = X^{n-2p} \prod_{k=1}^{p} (X^2+\alpha_k^2) .$$

On en déduit :

$$\det(I_n + A) = (-1)^n \det(-I_n - A) = \prod_{k=1}^{p} (1+\alpha_k^2) \geqslant 1. \qquad \square$$

2° Soit $S \in \mathcal{M}_n(\mathbb{R})$ symétrique, strictement positive. Dans $\mathbb{R}^n$ la forme quadratique Φ, de forme polaire φ, déterminée dans la base canonique ε par $X \mapsto {}^tXSX$ est positive, non dégénérée. On dispose de l'espace euclidien $(\mathbb{R}^n, \varphi)$; le procédé de Gram-Schmidt permet d'en construire une base φ-orthonormale e, dans laquelle Φ est représentée par I_n ; notant $P = P_\varepsilon^e$, nous avons ${}^tPSP = I_n$.

Soit $T \in \mathcal{M}_n(\mathbb{R})$ antisymétrique ; $A = {}^tPTP$ est antisymétrique, et, en utilisant 1° :

$$1 \leqslant \det(I_n+A) = \det\left({}^tP(S+T)P\right) = (\det P)^2 \det(S+T) .$$

Compte tenu de $(\det P)^2 \det S = 1$, on obtient (1).

• Ici $S \in \mathcal{M}_n(\mathbb{R})$ n'est que symétrique positive. On dispose de $\Omega \in \mathcal{M}_n(\mathbb{R})$ orthogonale telle que ${}^t\Omega S\Omega = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, $\lambda_k \in \mathbb{R}_+$.

Pour tout $m \in \mathbb{N}^*$, la matrice S_m définie par :

$${}^t\Omega S_m \Omega = \operatorname{diag}(\lambda_1 + \frac{1}{m}, \ldots, \lambda_n + \frac{1}{m})$$

est symétrique, strictement positive.

Soit $T \in \mathcal{M}_n(\mathbb{R})$ antisymétrique. Pour tout $m \in \mathbb{N}$, on a :

$$\det(S_m+T) \geqslant \det S_m \qquad \square$$

$\mathcal{M}_n(\mathbb{R})$ est muni de son unique structure topologique d'e.v.n.

On a : $\lim_{m \to +\infty} S_m = S$, on en déduit (1).

5.3.11 POLYNOMES DE LEGENDRE. 1° a) Montrer que l'on dispose de l'espace préhilbertien réel $(\mathbb{R}[X], (\,|\,))$, où $(\,|\,) : (\mathbb{R}[X])^2 \to \mathbb{R}$ est définie par :

$$(P|Q) = \int_{-1}^{+1} P(t)Q(t)dt.$$

b) Montrer qu'il existe une unique famille orthonormale $(P_n)_{n\in\mathbb{N}}$ telle que $\deg P_n = n$ et que $(P_n|X^n) \in \mathbb{R}_+^*$ pour tout $n\in\mathbb{N}$. Montrer qu'il s'agit d'une base de $\mathbb{R}[X]$. Expliciter les polynômes P_o, P_1 et P_2.

2° A tout $n\in\mathbb{N}$, on associe le polynôme $Q_n = \frac{1}{2^n n!}\frac{d^n}{dX^n}(X^2-1)^n$.

a) Montrer que Q_n est de degré n, qu'il a n racines simples appartenant à $]-1,1[$ et qu'il est orthogonal à tout polynôme P tel que $\deg P < n$.

b) Calculer $\|Q_n\|$, $Q_n(1)$ et $Q_n(-1)$.

c) Montrer $P_n = \lambda_n Q_n$ et calculer λ_n.

3° Etablir : $\forall n\in\mathbb{N}^* \quad Q_{n+1} = \alpha_n XQ_n + \beta_n Q_{n-1}$ où α_n et β_n sont des réels que l'on précisera.

4° Etablir : $\forall n\in\mathbb{N} \quad (X^2-1)Q_n'' + 2XQ_n' - n(n+1)Q_n = 0.$

1° a) Pour tout $(P,Q)\in(\mathbb{R}[X])^2$, l'intégrale $\int_{-1}^{+1} P(t)Q(t)dt$ existe ; pour $P = Q$ elle est positive, strictement si $P = Q$ et $P \neq 0$; $(|)$, qui est visiblement une forme bilinéaire sur $\mathbb{R}[X]$, est définie positive ; c'est un produit scalaire. □

b) La condition : $(\deg P_n = n) \wedge \left((P_n|X^n) \in \mathbb{R}_+^*\right)$ pour tout $n\in\mathbb{N}$ s'écrit :

$$\forall n\in\mathbb{N} \quad [\mathrm{Vect}(P_o,\ldots,P_n) = \mathrm{Vect}(X^o,\ldots,X^n)] \wedge [(P_n|X^n) \in \mathbb{R}_+^*].$$

Le procédé d'orthonormalisation de Schmidt (cf. 5.3.8) assure l'existence et l'unicité d'une famille orthonormale répondant à la question, donnée par :

$$\forall n\in\mathbb{N} \quad P_n = E_n/\|E_n\| \quad \text{où} \quad E_n = X^n - \sum_{i=o}^{n-1}(P_i|X^n)P_i. \qquad (1)$$

On vérifie par récurrence que chaque monôme de P_n est de degré pair ou impair, selon que n est pair ou impair.

• Il est clair que la famille (P_n), indexée par $\mathbb{N}$ et formée de polynômes échelonnés en degrés, est une base de $\mathbb{R}[X]$.

• On calcule, de proche en proche :

$$E_o = 1 \; ; \; P_o = 1/\sqrt{2} \; ; \; E_1 = X \; ; \; P_1 = \sqrt{3/2}\,X \; ; \; E_2 = X^2 - 1/3 \; ; \; P_2 = 3\sqrt{10}/4.(X^2-1/3).$$

2° $U_n = (X^2-1)^n$ est un polynôme de degré 2n : $U_n^{(n)}$ et Q_n sont donc des polynômes de degré n.

a) U_n admet pour racines -1 et 1, chacune avec la multiplicité n.

Appliquons le théorème de Rolle.

U_n', de degré 2n-1, admet pour racines -1 et 1, chacune avec la multiplicité n-1, et un $\gamma_{11} \in]-1,1[$; en tout 2n-1 racines réelles.

U_n'', de degré 2n-2, admet pour racines -1 et 1, chacune avec la multiplicité n-2, un $\gamma_{21} \in]-1,\gamma_{11}[$ et un $\gamma_{22} \in]\gamma_{11},1[$; en tout 2n-2 racines réelles. Par récurrence on aboutit à : $U_n^{(n)}$, et donc Q_n, de degré n ont n racines réelles distinctes appartenant à $]-1,1[$.

• En intégrant par parties autant de fois que nécessaire, on constate que, pour tout polynôme P, $\int_{-1}^{+1} U_n^{(n)}(t)P(t)dt$ s'écrit :

$$\left[U_n^{(n-1)}P - U_n^{(n-2)}P' + \ldots + (-1)^{n-1}U_n P^{(n-1)}\right]_{-1}^{1} + (-1)^n \int_{-1}^{1} U_n(t)P^{(n)}(t)dt.$$

Compte tenu de ce que 1 et -1 sont racines de $U_n, \ldots, U_n^{(n-1)}$, on a :

$$\int_{-1}^{1} Q_n(t)P(t)dt = (-1)^n \frac{1}{2^n n!} \int_{-1}^{1} U_n(t)P^{(n)}(t)dt \qquad (2)$$

Si deg P<n, alors $P^{(n)} = 0$; l'intégrale est nulle et Q_n est orthogonal à P.

b) Pour $P = Q_n$ on a $P^{(n)}(t) = \frac{1}{2^n n!} U_n^{(2n)}(t) = \frac{(2n)!}{2^n n!}$. D'où, par (2) :

$$\|Q_n\|^2 = (-1)^n \frac{(2n)!}{(2^n n!)^2} \int_{-1}^{1} U_n(t)dt.$$

En écrivant $U_n(t) = (t+1)^n(t-1)^n$ on obtient (par un calcul classique que l'on trouvera au 4.2.1 du tome I de nos exercices d'Analyse) :

$$\int_{-1}^{1} U_n(t)dt = (-1)^n \frac{(n!)^2}{(2n+1)!} 2^{2n+1}.$$

D'où : $\|Q_n\|^2 = \frac{2}{2n+1}$.

• Par la formule de Leibniz, avec $V_n = (X+1)^n$ et $W_n = (X-1)^n$:

$$U_n^{(n)} = V_n^{(n)}W_n + \ldots + C_n^p V_n^{(n-p)} W_n^{(p)} + \ldots + C_n^n V_n W_n^{(n)}.$$

D'où : $U_n^{(n)}(1) = 2^n n!$ et $U_n^{(n)}(-1) = (-1)^n 2^n n!$

et donc : $Q_n(1) = 1$ et $Q_n(-1) = (-1)^n$.

c) Pour $n \in \mathbb{N}^*$, on considère l'espace vectoriel $\mathbb{R}_n[X]$, de dimension n+1, et on constate que les sous-espaces $\mathbb{R}P_n$ et $\mathbb{R}Q_n$, de dimension 1, qui admettent le même sous-espace orthogonal $\mathbb{R}_{n-1}[X]$, sont confondus. D'où $P_n = \lambda_n Q_n$ avec $\lambda_n \in \mathbb{R}^*$.

Compte tenu de $\|P_n\| = 1$ et $\|Q_n\| = \sqrt{\frac{2}{2n+1}}$, on a $|\lambda_n| = \sqrt{\frac{2n+1}{2}}$.

On a en outre : $(P_n|X^n) = \lambda_n(Q_n|X^n) \in \mathbb{R}_+^*$, et, d'après (2) :

$$(Q_n|X^n) = (-1)^n \frac{1}{2^n n!} \int_{-1}^{1} U_n(t)n!dt \in \mathbb{R}_+^*$$

Finalement : $\lambda_n = \sqrt{\frac{2n+1}{2}}$.

3° Le polynôme XQ_n appartient à $\mathbb{R}_{n+1}[X]$ dont une base est $(Q_0, \ldots, Q_{n+1})$. Il s'écrit donc :

$$XQ_n = \sum_{i=0}^{n+1} \mu_i Q_i, \text{ avec } \mu_{n+1} \neq 0 \text{ (puisque deg } Q_n = n).$$

Pour tout $j \in \{0,\dots,n-2\}$, on a $\deg(XQ_j) < \deg Q_n$. D'où :

$$(Q_n | XQ_j) = (XQ_n | Q_j) = 0 = \sum_{i=0}^{n+1} \mu_i (Q_i | Q_j) = \mu_j \| Q_j \|^2$$

et : $$XQ_n = \mu_{n+1} Q_{n+1} + \mu_n Q_n + \mu_{n-1} Q_{n-1}.$$

Mais XQ_n, Q_{n+1} et Q_{n-1} ont la même parité, différente de celle de Q_n : on a donc $\mu_n = 0$, ce qui justifie l'écriture $Q_{n+1} = \alpha_n XQ_n + \beta_n Q_{n-1}$.

En prenant les valeurs au point $t = 1$, on obtient : $\alpha_n + \beta_n = 1$.

En écrivant que les coefficients dominants sont les mêmes :

$$\alpha_n \frac{1}{2^n n!} \frac{(2n)!}{n!} = \frac{1}{2^{n+1}(n+1)!} \frac{(2n+2)!}{(n+1)!}$$

d'où : $$\alpha_n = \frac{2n+1}{n+1} \quad \text{et} \quad \beta_n = \frac{-n}{n+1}.$$

Finalement : $(n+1)Q_{n+1} = (2n+1)XQ_n - nQ_{n-1}$, ce qui permet de calculer les Q_n de proche en proche, à partir de $Q_0 = 1$ et $Q_1 = X$.

4° Reprenons $U_n = (X^2-1)^n$. Nous avons $U_n' = 2nX(X^2-1)^{n-1}$ et :

$$(X^2-1)U_n' = 2n\, XU_n.$$

En dérivant les deux membres n+1 fois par Leibniz :

$$(X^2-1)U_n^{(n+2)} + (n+1)2XU_n^{(n+1)} + n(n+1)U_n^{(n)} = 2nXU_n^{(n+1)} + 2n(n+1)U_n^{(n)}.$$

i.e. $$(X^2-1)U_n^{(n+2)} + 2XU_n^{(n+1)} - n(n+1)U_n^{(n)} = 0.$$ □

Remarque. L'étude s'étend à l'espace préhilbertien complexe $(\mathbb{C}[X], (\,|\,))$ où

$$(P|Q) = \int_{-1}^{1} \overline{P(t)}\, Q(t)dt.$$

5.3.12 PROJECTEURS ORTHOGONAUX. Soient E un espace euclidien (resp. hermitien), p un projecteur de E, F l'image de p et G son noyau.

1° Montrer que l'endomorphisme p de E est symétrique (resp. hermitien) si et seulement si $G = F^\perp$. Lorsqu'il en est ainsi, on dit que p est le projecteur orthogonal sur F.

2° Montrer que le projecteur p est orthogonal si, et seulement s'il vérifie :

$$\forall x \in E \quad \| p(x) \| \leqslant \| x \| \qquad (1)$$

1° Question classique. Rappelons la démonstration.

- Si p admet un adjoint égal à p ; $\operatorname{Ker} p^* = (\operatorname{Im} p)^\perp$ s'écrit $G = F^\perp$.
- Supposons $G = F^\perp$. Pour tout $(x,y) \in E^2$, nous pouvons écrire :

$$x = p(x) + x',\ y = p(y) + y',\ \text{avec } (x',y') \in (F^\perp)^2$$

et en déduire que $(x|p(y))$ et $(p(x)|y)$ sont l'un et l'autre égaux à $(p(x)|p(y))$. L'endomorphisme p est ainsi symétrique (resp. hermitien).

2° Le lecteur s'aidera d'une figure, faite dans le cas euclidien.

- Si p est orthogonal, (1) est une conséquence de Pythagore.
- Supposons que p n'est pas orthogonal, i.e. que $G \neq F^{\perp}$. C'est qu'il existe $(a,b) \in F \times G$ tel que $(b|a) \neq 0$, ce qui implique $a \neq 0$ et $b \neq 0$.

Dans l'ensemble $a + \mathbb{C}b$, il existe un unique élément c tel que $(b|c) = 0$; il est donné par $c = a+\lambda b$ avec $(b|a+\lambda b) = 0$; on a $c \neq a$.

Comme c et a-c, de somme a, sont orthogonaux, on a (Pythagore) :

$$\|a\|^2 = \|c\|^2 + \|a-c\|^2, \text{ avec } a = p(c) \text{ et } a-c \neq 0.$$

Il en résulte $\|p(c)\| > \|c\|$. Ici (1) n'est pas vérifié. □

Remarque. Une autre façon de prouver que, si le projecteur p vérifie (1), alors il est orthogonal, est d'utiliser l'exercice suivant (mais c'est moins naturel).

5.3.13 Soient E un espace euclidien (resp. hermitien) et $u \in \mathcal{L}(E)$ tel que :

$$\forall x \in E \quad \|u(x)\| \leqslant \|x\| \tag{1}$$

On note p le projecteur orthogonal de E d'image Ker(I-u), où $I = Id_E$.

1° Trouver le noyau de p. En déduire que les sous-espaces Ker(I-u) et Im(I-u) de E sont supplémentaires orthogonaux.

2° A tout $n \in \mathbb{N}^*$, on associe $u_n = \frac{1}{n}(I+u+\ldots+u^{n-1})$. Montrer que $(\mathcal{L}(E)$ étant muni de son unique structure topologique d'e.v.n.) on a :

$$\lim_{n \to +\infty} u_n = p.$$

1° Ker p et Im p = Ker(I-u) sont supplémentaires orthogonaux.

Nous allons montrer : $\mathrm{Ker}(I-u) = \mathrm{Ker}(I-u)^*$. (2)

Il en résultera : $(\mathrm{Ker}(I-u))^{\perp} = (\mathrm{Ker}(I-u)^*)^{\perp}$

i.e. $\mathrm{Ker}\, p = \mathrm{Im}(I-u)$.

D'où la proposition.

- Vérifions d'abord : $\forall x \in E \quad \|u^*(x)\| \leqslant \|x\|$. (3)

En effet, pour tout $x \in E$, on a : $\|u^*(x)\|^2 = (x|u(u^*(x)))$, et :

$$\|u^*(x)\|^2 \leqslant \|x\| \, \|u(u^*(x))\| \leqslant \|x\| \, \|u^*(x)\|. \qquad \square$$

- Soit $x \in \mathrm{Ker}(I-u)$, i.e. x tel que $u(x) = x$; $\|u^*(x) - x\|^2$ s'écrit :

$$\|u^*(x)\|^2 + \|x\|^2 - (u^*(x)|x) - (x|u^*(x))$$

et :
$$\|u^*(x)\|^2 + \|x\|^2 - (x|u(x)) - (u(x)|x)$$

et :
$$\|u^*(x)\|^2 - \|x\|^2.$$

D'où, par (3) : $\|u^*(x)-x\|^2 \leqslant 0$, et donc $u^*(x) = x$.

Ainsi : $\quad \mathrm{Ker}(I-u) \subset \mathrm{Ker}(I-u^*)$.

Symétriquement (grâce à (3)) : $\mathrm{Ker}(I-u^*) \subset \mathrm{Ker}(I-u)$.

Reste à utiliser $(I-u)^* = I-u^*$ pour obtenir (2). □

Remarque. Si u est, en outre, un projecteur, alors (I-u) est un projecteur, orthogonal d'après ce qui précède, et donc le projecteur u est orthogonal.

2° Soit $x \in E$. Ecrivons $x = p(x) + q(x)$, $p(x) \in \mathrm{Im}\ p$ et $q(x) \in \mathrm{Ker}\ p$.

- Nous avons $u\big(p(x)\big) = p(x)$. D'où : $u_n\big(p(x)\big) = p(x)$ pour tout $n \in \mathbb{N}^*$.
- D'autre part, d'après $q(x) \in \mathrm{Im}(I-u)$, il existe $y \in E$ tel que :

$$q(x) = (I-u)(y).$$

Or : $\quad u_n(I-u) = \frac{1}{n}(I-u^n)$, et $u_n\big(q(x)\big) = \frac{1}{n}\big(y-u^n(y)\big)$.

Comme $\|u^n(y)\| \leqslant \|y\|$ (récurrence), il vient : $\|u_n\big(q(x)\big)\| \leqslant \frac{2}{n}\|y\|$.

Il en résulte : $\lim\limits_{n\to+\infty} \|u_n\big(q(x)\big)\| = 0$.

- Retenons : $\lim\limits_{n\to+\infty} \|(u_n-p)(x)\| = 0$ pour tout $x \in E$. (4)
- $\mathcal{L}(E)$ étant de dimension finie, toutes les normes sur $\mathcal{L}(E)$ sont équivalentes, et nous pouvons utiliser la norme :

$$N(f) = \sum_{i=1}^{p} \|f(e_i)\|, \text{ où } (e_1,\ldots,e_p) \text{ est une base de } E.$$

Nous avons (par (4)) : $\lim\limits_{n\to+\infty} \|(u_n-p)(e_i)\| = 0$ pour tout $i \in \mathbb{N}_p$.

D'où : $\quad \lim\limits_{n\to+\infty} N(u_n-p) = 0$. □

5.3.14 Soient E un espace hilbertien réel (resp. complexe), muni de la distance associée à la norme euclidienne (resp. hermitienne), et u un endomorphisme continu de E. On note :

$$\mu = \sup_{\|x\|\leqslant 1,\|y\|\leqslant 1} \big|\big(x|u(y)\big)\big| \ ; \ \lambda = \sup_{\|x\|\leqslant 1} \big|\big(x|u(x)\big)\big|.$$

1° Vérifier : $\mu = \|u\|$, où $\|u\| = \sup\limits_{\|x\|\leqslant 1} \|u(x)\| = \sup\limits_{x\neq 0} \big(\|u(x)\| / \|x\|\big)$.

2° A-t-on toujours $\lambda = \mu$? Etudier le cas où u est symétrique (resp. hermitien).

L'existence de la norme $\|u\|$ de l'application linéaire continue u, et l'inégalité :

$$\big|\big(x|u(y)\big)\big| \leqslant \|x\|\,\|u(y)\| \leqslant \|u\|\,\|x\|\,\|y\|$$

entraînent l'existence de λ et de μ, ainsi que : $\lambda \leqslant \mu \leqslant \|u\|$.

1° Nous allons prouver : $\|u\| \leqslant \mu$. Il en résultera : $\mu = \|u\|$.

Soit $x \in E$ tel que $\|x\| \leqslant 1$. Nous avons :

$$\|u(x)\|^2 = \big(y|u(x)\big), \text{ où } y = u(x),$$

et donc : $\|u(x)\|^2 \leqslant \mu \|y\| = \mu \|u(x)\|$.

Que $u(x)$ soit nul ou non nul, on en déduit : $\|u(x)\| \leqslant \mu$. □

2° On n'a pas toujours $\lambda = \mu$. C'est ainsi que si E est réel et si u est anti-symétrique non nul, on a, pour tout $x \in E$:

$$\big(x|u(x)\big) = -\big(u(x)|x\big) = -\big(x|u(x)\big).$$

L'application $x \longmapsto \big|\big(x|u(x)\big)\big|$ est nulle et $\lambda = 0$, alors que $\mu = \|u\| \neq 0$.

• Dans la suite u est symétrique (resp. hermitien). Nous allons prouver $\mu \leqslant \lambda$; il en résultera : $\lambda = \mu = \|u\|$.

Le calcul vaut que E soit réel ou complexe.

Soit $(x,y) \in E^2$ tel que $\|x\| \leqslant 1$ et $\|y\| \leqslant 1$. Notons θ un argument de $\big(x|u(y)\big)$ et posons $k = e^{-i\theta}$, avec $k \in \{1,-1\}$ dans le cas réel. Il vient :

$$\big|\big(x|u(y)\big)\big| = k\big(x|u(y)\big) = \big(x|u(ky)\big).$$

Il en résulte que $\big(x|u(ky)\big)$ est réel, et donc égal à son conjugué $\big(u(ky)|x\big)$; compte tenu de l'existence de u^* et de $u^{**} = u$, celui-ci s'écrit $\big(ky|u(x)\big)$. D'où :

$$\begin{aligned} 4\big|\big(x|u(y)\big)\big| &= 2\big(x|u(ky)\big) + 2\big(ky|u(x)\big) \\ &= \big(x+ky|u(x+ky)\big) - \big(x-ky|u(x-ky)\big), \end{aligned}$$

et :
$$\begin{aligned} 4\big|\big(x|u(y)\big)\big| &\leqslant \lambda\big(\|x+ky\|^2 + \|x-ky\|^2\big) \\ &\leqslant 2\lambda\big(\|x\|^2 + \|ky\|^2\big) \leqslant 4\lambda. \end{aligned}$$

□

5.3.15 Soient E un espace euclidien (resp. hermitien) et $u \in \mathcal{L}(E)$.

1° a) Vérifier $\|u^*\| = \|u\|$, où $\|f\| = \sup_{\|x\| \leqslant 1} \|f(x)\|$.

b) Vérifier que u^*u est symétrique (resp. hermitien) positif.

Comparer les rangs de u et u^*u. Montrer : $\|u^*u\| = \|u\|^2$.

2° Donner une expression de $\|u\|$ en fonction des valeurs propres de u^*u.

Etudier le cas particulier où u est symétrique (resp. hermitien).

3° Ici u et v sont deux endomorphismes de E. Donner un encadrement des modules des valeurs propres de vu faisant intervenir celles de u^*u et v^*v.

1° a) E étant de dimension finie, u^* existe, u et u^* sont continus.

D'après l'exercice précédent :

$$\|u\| = \sup_{\|x\| \leqslant 1,\ \|y\| \leqslant 1} \big|\big(x|u(y)\big)\big| \ ; \|u^*\| = \sup_{\|x\| \leqslant 1,\ \|y\| \leqslant 1} \big|\big(y|u^*(x)\big)\big|.$$

Or, pour tout $(x,y) \in E^2$:

$$|(y|u^*(x))| = |(u(y)|x)| = |(x|u(y))|. \qquad \square$$

b) D'après $(u^*u)^* = u^*u$, u^*u est symétrique (resp. hermitien).

La forme Φ associée à u^*u, et définie par :

$$\Phi(x) = (x|u^*u(x)) = (u(x)|u(x)) = \|u(x)\|^2 \qquad (1)$$

est positive, et (par définition) u^*u est positif.

- D'après (1), le noyau de u est le cône isotrope de Φ, et donc le noyau de Φ (qui est positive) ; u et Φ ont ainsi le même rang ; or le rang de Φ est égal à celui de u^*u ; en conclusion, u et u^*u ont le même rang.

- D'après (1), pour tout $x \in E$ tel que $\|x\| \leqslant 1$ on a :

$$\|u(x)\|^2 \leqslant \|x\| \, \|u^*u\| \, \|x\| \leqslant \|u^*u\|.$$

D'où $\|u\|^2 \leqslant \|u^*u\|$. Or $\|u^*u\| \leqslant \|u^*\| \, \|u\| = \|u\|^2$ (cf a) .

Finalement : $\|u^*u\| = \|u\|^2$. $\square$

Comme $u^{**} = u$, on déduit de ce qui précède que uu^* est symétrique (resp. hermitien) positif, de même rang que u^* (et donc que u) et que $\|uu^*\| = \|u\|^2$.

2° On note $(\lambda_1,\ldots,\lambda_n)$ la famille croissante des racines (réelles et positives) du polynôme caractéristique de u^*u. On sait qu'il existe une base orthonormale $(e_i)_{1\leqslant i\leqslant n}$ de E telle que $u^*u(e_i) = \lambda_i e_i$ pour tout $i \in \mathbf{N}_n$.

Pour tout $x \in E$ on écrit :

$$x = \sum_{i=1}^{n} \xi_i e_i \quad \text{et} \quad u^*u(x) = \sum_{i=1}^{n} \xi_i \lambda_i e_i,$$

et, par (1) :

$$\|u(x)\|^2 = \left(\sum_{i=1}^{n} \xi_i e_i \mid \sum_{i=1}^{n} \xi_i \lambda_i e_i \right) = \sum_{i=1}^{n} |\xi_i|^2 \lambda_i.$$

D'où : $$\lambda_1 \|x\|^2 \leqslant \|u(x)\|^2 \leqslant \lambda_n \|x\|^2 \qquad (2)$$

En outre : $\|u(e_n)\|^2 = \lambda_n$, et donc $\|u\| = \sqrt{\lambda_n}$.

Remarque. La plus grande des valeurs propres de u^*u est $\|u\|^2 = \|u^*u\|$.

• Si u est symétrique (resp. hermitien), les λ_i sont les carrés des racines α_i (réelles, mais pas nécessairement positives) du polynôme caractéristique de u, ainsi qu'on le constate en utilisant une base orthonormale de E qui diagonalise u ; λ_n est le plus grand des α_i^2. D'où :

$$\|u\| = \max_{1\leqslant i\leqslant n} |\alpha_i|.$$

3° En remplaçant x par v(x) dans (2), on a, pour tout $x \in E$:

$$\lambda_1 \|v(x)\|^2 \leqslant \|uv(x)\|^2 \leqslant \lambda_n \|v(x)\|^2. \qquad (3)$$

En notant $\mu_1,\ldots,\mu_n$, avec $0\leqslant\mu_1\leqslant\ldots\leqslant\mu_n$, les racines du polynôme caractéristique de v^*v, on a, pour tout $x\in E$:

$$\mu_1\|x\|^2\leqslant\|v(x)\|^2\leqslant\mu_n\|x\|^2$$

et, compte tenu de (3) :

$$\lambda_1\mu_1\|x\|^2\leqslant\|uv(x)\|^2\leqslant\lambda_n\mu_n\|x\|^2\,. \tag{4}$$

Pour toute valeur propre ν de uv, on applique (4) à un vecteur propre x associé à ν, et compte tenu de $x\neq0$, on obtient :

$$\lambda_1\mu_1\leqslant|\nu|^2\leqslant\lambda_n\mu_n\,,$$

avec $|\nu|^2=\nu^2$ dans le cas réel.

5.3.16 1° Soient E un espace euclidien (resp. hermitien) et $u\in\mathcal{L}(E)$. Montrer que :

$$M=\{x\in E\mid\|u(x)\|=\|u\|\,\|x\|\},\ \text{où}\ \|u\|=\sup_{\|x\|\leqslant1}\|u(x)\|$$

est un sous-espace de E non réduit à $\{0\}$.

2° A quelle condition a-t-on $M=E$?

1° Puisque $\|u(x)\|^2=\left(x\middle|u^*u(x)\right)$ pour tout $x\in E$, l'exercice fait intervenir $v=u^*u$, qui a été étudié dans l'exercice précédent ; on a vu que v est symétrique (resp. hermitien) positif, et que $\|v\|=\|u\|^2=\|u^*\|^2$. D'où :

$$M=\left\{x\in E\mid\left(x\middle|v(x)\right)=\|v\|\,\|x\|^2\right\}. \tag{1}$$

• Soit $x\in M\setminus\{0\}$. Compte tenu de Cauchy-Schwarz, qui donne :

$$0\leqslant\left(x\middle|v(x)\right)\leqslant\|x\|\,\|v(x)\|\leqslant\|v\|\,\|x\|^2$$

on a : $\left(x\middle|v(x)\right)=\|x\|\,\|v(x)\|$

et donc x et v(x) sont colinéaires. Puisque $x\neq0$, il existe un scalaire λ tel que $v(x)=\lambda x$, et, compte tenu de (1), on a $\lambda=\|v\|$.

• Le cas $x=0$ ne posant pas de problème, on a :

$$\forall x\in M\quad v(x)=\|v\|x\,.$$

Mais (exercice précédent), $\|v\|$ est la plus grande des valeurs propres (toutes dans $\mathbf{R}_+$) de l'endomorphisme positif v. Il en résulte $M\subset F$, où F est le sous-espace propre de v associé à $\|v\|$.

• Inversement, pour tout $x\in F$ on a $v(x)=\|v\|x$, et (par (1)) : $x\in M$.

• En conclusion $M=F$. □

2° On a $M=E$ si, et seulement si : $\|u(x)\|=\|u\|\,\|x\|$ pour tout $x\in E$, i.e. si et seulement si u est soit l'endomorphisme nul, soit une similitude de E.

5.3.17 Soit (u,v) un couple d'endomorphismes d'un espace euclidien (resp. hermitien) de dimension n. Prouver l'équivalence des assertions :

i) Les polynômes caractéristiques de u^*u et v^*v sont égaux ;

ii) Il existe deux automorphismes orthogonaux (resp. unitaires) w et w' de E tels que $v = w'uw$.

Preuve de ii) ⇒ i). Par hypothèse $v = w'uw$, avec $w^* = w^{-1}$ et $(w')^* = (w')^{-1}$. On calcule $v^*v = w^{-1}u^*uw$, ce qui montre que u^*u et v^*v ont le même polynôme caractéristique.

Preuve de i) ⇒ ii). Par hypothèse, u^*u et v^*v qui - ainsi que nous l'avons déjà vu - sont symétriques (resp. hermitiens) positifs, ont un même polynôme caractéristique. Celui-ci a n racines réelles et positives, que nous pouvons noter $\alpha_1,\ldots,\alpha_n$ avec $0 \leqslant \alpha_n \leqslant \ldots \leqslant \alpha_1$.

• Nous savons qu'il existe une base orthonormale $(e_1,\ldots,e_n)$ de E telle que :

$$\forall i \in \mathbb{N}_n \quad u^*u(e_i) = \alpha_i e_i .$$

Pour tout $(i,j) \in \mathbb{N}_n^2$, nous avons (compte tenu de $\overline{\alpha_i} = \alpha_i$) :

$$\big(u(e_i)\,|\,u(e_j)\big) = \big(u^*u(e_i)\,|\,e_j\big) = \alpha_i(e_i\,|\,e_j) = \alpha_i\delta_{ij}, \qquad (1)$$

et, en particulier : $\|u(e_i)\| = \sqrt{\alpha_i}$. (2)

Il existe un entier k tel que $\alpha_i > 0$ si, et seulement si $i \leqslant k$. Pour $i \leqslant k$, on définit $e'_i \in E$ pour : $u(e_i) = \sqrt{\alpha_i}\, e'_i$. D'après (1) et (2), $(e'_1,\ldots,e'_k)$ est une famille orthonormale, que l'on complète en une base orthonormale $(e'_1,\ldots,e'_n)$ de E. On constate (en utilisant $\alpha_i = 0$ pour $i > k$) :

$$\forall i \in \mathbb{N}_n \quad u(e_i) = \sqrt{\alpha_i}\, e'_i .$$

• En procédant de même pour v, on met en évidence deux autres bases orthonormales $(f_1,\ldots,f_n)$ et $(f'_1,\ldots,f'_n)$ de E telles que :

$$\forall i \in \mathbb{N}_n \quad v(f_i) = \sqrt{\alpha_i}\, f'_i .$$

• Soit w (resp. w') l'endomorphisme de E défini par :

$$\forall i \in \mathbb{N}_n \quad w(f_i) = e_i \quad [\text{resp. } w'(e'_i) = f'_i] .$$

Les bases étant orthonormales, w et w' sont des automorphismes orthogonaux (resp. unitaires). Pour tout $i \in \mathbb{N}_n$, de $w(f_i) = e_i$ on déduit :

$$uw(f_i) = u(e_i) = \sqrt{\alpha_i}\, e'_i .$$

et : $$w'uw(f_i) = \sqrt{\alpha_i}\, w'(e'_i) = \sqrt{\alpha_i}\, f'_i = v(f_i).$$

Il en résulte : $v = w'uw$. □

5.3.18 Soit A une $\mathbb{C}$-matrice carrée. Montrer qu'il existe une matrice unitaire U telle que $U^{-1}AU$ soit triangulaire supérieure.

- Il s'agit d'une variante de la trigonalisation d'une $\mathbb{C}$-matrice carrée.
- Il suffit de montrer qu'est vraie pour tout $n \in \mathbb{N}^*$ l'assertion :

$(\mathcal{T}_n)$ Pour tout espace hermitien E de dimension n et tout $u \in \mathcal{L}(E)$, il existe une base orthonormale de E dans laquelle u est représenté par une matrice triangulaire supérieure.

- $(\mathcal{T}_1)$ est vraie : pour $n = 1$, toute base orthonormale de E répond à la question.

- Soit $n \geqslant 2$ tel que $(\mathcal{T}_{n-1})$ soit vraie. Considérons E hermitien de dimension n et $u \in \mathcal{L}(E)$. Au titre d'endomorphisme d'un $\mathbb{C}$-espace vectoriel, u admet une valeur propre α_{11} ; soit e_1 un vecteur propre unitaire associé :

$$u(e_1) = \alpha_{11} e_1 . \tag{1}$$

On munit $E' = (\mathbb{R}e_1)^{\perp}$ de la restriction du produit scalaire de E ; E' est ainsi hermitien, de dimension n-1. On dispose de $v \in \mathcal{L}(E')$ induit par $p \circ u$, où $p \in \mathcal{L}(E)$ est le projecteur orthogonal sur E' ; on a :

$$\forall x \in E' \quad v(x) = p\big(u(x)\big).$$

D'après l'hypothèse de récurrence, il existe une base orthonormale $(e_2, \ldots, e_n)$ de E' telle que :

$$v(e_2) = \alpha_{22} e_2 \ ; \ldots \ ; v(e_n) = \alpha_{2n} e_2 + \ldots + \alpha_{nn} e_n \ . \tag{2}$$

Mais, pour tout $x \in E'$, les vecteurs u(x) et v(x) ne diffèrent que par un élément de $\mathbb{R}e_1$; en particulier :

$$u(e_2) = \alpha_{12} e_1 + v(e_2) \ ; \ldots ; \ u(e_n) = \alpha_{1n} e_1 + v(e_n). \tag{3}$$

Il est clair que $(e_1, e_2, \ldots, e_n)$ est une base orthonormale de E ; de (1), (2) et (3) on déduit que la matrice $[\alpha_{ij}]$ qui représente u dans cette base est triangulaire supérieure.

Remarque : On peut aussi prouver ce résultat en utilisant le procédé d'orthogonalisation de Schmidt (cf. exercice 5.3.8).

5.3.19 1° a) Montrer que $A = [\alpha_{ij}] \longmapsto \|A\| = \left(\sum_{i,j} |\alpha_{ij}|^2 \right)^{1/2}$ est une norme sur l'espace vectoriel $\mathcal{M}_n(\mathbb{C})$.

b) Vérifier : $|\operatorname{tr} A| \leqslant \sqrt{n}\, \|A\|$ pour toute $A \in \mathcal{M}_n(\mathbb{C})$.

c) Vérifier : $\|AB\| \leqslant \|A\| \|B\|$ pour tout $(A,B) \in \big(\mathcal{M}_n(\mathbb{C})\big)^2$.

2° Soient $A \in \mathcal{M}_n(C)$ et $(\lambda_1, \ldots, \lambda_n)$ un système de racines de son polynôme caractéristique. Vérifier : $\|A\|^2 \geqslant \sum_{k=1}^{n} |\lambda_k|^2$.

Que se passe-t-il si A est hermitienne ?

1° a) On munit $\mathcal{M}_n(\mathbb{C})$ de sa structure hermitienne canonique en convenant que la base canonique est orthonormale. Le produit scalaire est ainsi :

$$\varphi : ([\alpha_{ij}], [\beta_{ij}]) \mapsto \sum_{i,j} \overline{\alpha}_{ij}\beta_{ij}.$$

La forme hermitienne associée est $\Phi : [\alpha_{ij}] \mapsto \sum_{i,j} |\alpha_{ij}|^2$.

Il en résulte que $\|\cdot\| = \sqrt{\Phi}$ est la norme euclidienne. □

b) On remarque :

$$\varphi(A,B) = \mathrm{tr}(A^* B) \; ; \; \Phi(A) = \mathrm{tr}(A^* A) \; ; \; \|A\| = \sqrt{\mathrm{tr}(A^* A)}.$$

(on sait que $A^* A$ est hermitienne positive).

Pour toute $A \in \mathcal{M}_n(\mathbb{C})$, l'inégalité de Schwarz fournit :

$$|\varphi(I_n, A)| \leqslant \sqrt{\Phi(I_n)}\sqrt{\Phi(A)}$$

qui n'est autre que : $|\mathrm{tr}\, A| \leqslant \sqrt{n}\, \|A\|$, avec d'ailleurs égalité si et seulement si la matrice A est scalaire. □

c) On a : $\|AB\|^2 = \sum_{i,j} |\sum_k \alpha_{ik}\beta_{kj}|^2$.

Pour (i,j) donné, $|\sum_k \alpha_{ik}\beta_{kj}|^2$ est majoré par $\left(\sum_k |\alpha_{ik}\beta_{kj}|\right)^2$ et (Schwarz) par $\left(\sum_k |\alpha_{ik}|^2\right)\cdot\left(\sum_k |\beta_{kj}|^2\right)$. D'où :

$$\|AB\|^2 \leqslant \sum_{i,j} \left(\sum_k |\alpha_{ik}|^2\right)\cdot\left(\sum_k |\beta_{kj}|^2\right)$$

et : $\|AB\|^2 \leqslant \left(\sum_{i,j} |\alpha_{ij}|^2\right)\cdot\left(\sum_{i,j} |\beta_{ij}|^2\right) = \|A\|^2 \|B\|^2$. □

Autre solution : On utilise la remarque du 1°b. On a :

$$\|AB\|^2 = \mathrm{tr}((AB)^* AB) = \mathrm{tr}(B^* A^* AB) = \mathrm{tr}(A^* ABB^*).$$

Comme $A^* A$ et BB^* sont hermitiennes positives, il vient (cf. exercice 5.3.7):

$$\|AB\|^2 \leqslant \mathrm{tr}(A^* A).\mathrm{tr}(BB^*) = \|A\|^2 \|B^*\|^2 = \|A\|^2 \|B\|^2. \quad \square$$

2° D'après l'exercice précédent, on peut associer à A une matrice unitaire U telle que $T = U^{-1}AU$ soit triangulaire. Notons $T = [\tau_{ij}]$; les τ_{kk} sont les racines λ_k du polynôme caractéristique commun à A et T ; nous avons :

$$T^* T = U^* A^* (U^{-1})^* U^{-1} AU = U^{-1} A^* AU.$$

$A^* A$ et $T^* T$ sont ainsi semblables, et donc de même trace. D'où :

$$\|A\|^2 = \|T\|^2 = \sum_{i,j} |\tau_{ij}|^2 \geqslant \sum_{k=1}^{n} |\tau_{kk}|^2 = \sum_{k=1}^{n} |\lambda_k|^2 \quad \square$$

Si A est hermitienne, on sait, sans qu'il soit nécessaire d'utiliser l'exercice précédent, qu'il existe une matrice unitaire U telle que :

$$U^{-1}AU = \mathrm{diag}(\lambda_1,\ldots,\lambda_n)\,.$$

Ici : $$\|A\|^2 = \|\mathrm{diag}(\lambda_1,\ldots,\lambda_n)\|^2 = \sum_{k=1}^{n} |\lambda_k|^2.$$

Remarque : Plus généralement, on vérifie : $\|A\|^2 = \sum_{k=1}^{n} |\lambda_k|^2$ si et seulement si $A^*A = AA^*$.

5.3.20 Soient E un espace euclidien (resp. hermitien), Φ et Ψ des formes quadratiques (resp. hermitiennes) sur E, u et v les endomorphismes symétriques (resp. hermitiens) associés par $\Phi(x) = (x|u(x))$ et $\Psi(x) = (x|v(x))$.

On note $(\lambda_1,\ldots,\lambda_n)$ et $(\mu_1,\ldots,\mu_n)$ les familles croissantes des racines des polynômes caractéristiques de u et v (qui sont réelles).

1° Soit $k \in \mathbf{N}_n$. Montrer que, $\mathcal{U}(k)$ désignant l'ensemble des sous-espaces de E de dimension au moins égale à k, on a :

$$\lambda_k = \min_{W\in\mathcal{U}(k)} \left(\max_{x\in S(W)} \Phi(x) \right), \text{ où } S(W) \text{ est la sphère unité de } W. \quad (1)$$

Peut-on échanger min et max dans (1) ?

2° $\mathcal{L}(E)$ étant muni de la norme $\|f\| = \sup_{x\in S(E)} \|f(x)\|$, montrer :

$$\forall k \in \mathbf{N}_n \quad |\mu_k - \lambda_k| \leqslant \|v-u\|\,.$$

3° On suppose ici que la forme $\Psi - \Phi$ est positive. Montrer que :

$$\forall k \in \mathbf{N}_{n-r} \quad \lambda_k \leqslant \mu_k \leqslant \lambda_{k+r}\,, \quad \text{où } r = \mathrm{rg}(\Psi-\Phi),$$

et que si, en outre Φ est positive, alors : $0 \leqslant \det u \leqslant \det v$.

1° L'application Φ de E dans $\mathbf{R}$ est continue. Pour tout sous-espace W de E, sa restriction à S(W), qui est un compact non vide de E, admet des bornes qu'elle atteint.

- On sait qu'il existe une base orthonormale $(e_1,\ldots,e_n)$ de E telle que :

$$\forall i \in \mathbf{N}_n \quad u(e_i) = \lambda_i e_i\,.$$

On note $F_i = \mathrm{Vect}(e_1,\ldots,e_i)$ et $G_i = \mathrm{Vect}(e_i,\ldots,e_n)$.

- Soit $k \in \mathbf{N}_n$. Pour tout élément $\sum_{i=1}^{k} \xi_i e_i$ de F_k, on a :

$$\|x\|^2 = \sum_{i=1}^{k} |\xi_i|^2 \quad \text{et} \quad \Phi(x) = \sum_{i=1}^{k} \lambda_i |\xi_i|^2 \leqslant \lambda_k \|x\|^2.$$

En particulier : $e_k \in S(F_k)$ et $\Phi(e_k) = \lambda_k$. D'où :

$$\lambda_k = \max_{x\in S(F_k)} \Phi(x)\,. \quad (2)$$

De même : $$\lambda_k = \min_{x\in S(G_k)} \Phi(x)\,. \quad (3)$$

- Soit alors $W \in \mathcal{U}(k)$. On a $\dim W \geqslant k$. De $\dim W + \dim G_k \geqslant n+1$, on déduit l'existence d'un vecteur unitaire $y \in W \cap G_k$.

Comme $y \in S(G_k)$, (3) donne $\lambda_k \leqslant \Phi(y)$. D'où, comme $y \in S(W)$:

$$\lambda_k \leqslant \max_{x \in S(W)} \Phi(x) . \qquad (4)$$

Compte tenu de $F_k \in \mathcal{U}(k)$ et de (2), (4), vraie pour tout $W \in \mathcal{U}(k)$, donne (1). □

• Nous laissons au lecteur le soin de vérifier :

$$\lambda_k = \max_{W \in \mathcal{U}(n+1-k)} \left(\min_{x \in S(W)} \Phi(x) \right) . \qquad (1')$$

Remarques. a) En faisant $k = 1$ dans (3), puis $k = n$ dans (2), on obtient :

$$\lambda_1 = \min_{x \in S(E)} \Phi(x) \quad \text{et} \quad \lambda_n = \max_{x \in S(E)} \Phi(x)$$

b) En remarquant que, pour tout $x \in E \setminus \{0\}$, le "quotient de Rayleigh" $R_u(x) = \big(x \,|\, u(x)\big) / \|x\|^2$ est $\Phi(x) / \|x\|^2$), on a, dans (1) :

$$\max_{x \in S(W)} \Phi(x) = \max_{x \in W \setminus \{0\}} R_u(x).$$

2° Soit $k \in \mathbf{N}_n$. F_k ayant la même signification qu'au 1°, de (1), dans lequel on a remplacé Φ par Ψ et λ_k par μ_k, on déduit :

$$\mu_k \leqslant \max_{x \in S(F_k)} \big(\Phi(x) + Q(x)\big), \text{ où } Q = \Psi - \Phi.$$

Compte tenu de (2), il vient :

$$\mu_k - \lambda_k \leqslant \max_{x \in S(F_k)} Q(x).$$

Pour tout $x \in S(F_k)$, on a : $Q(x) = \big(x \,|\, (v-u)x\big) \leqslant \|v-u\|$.

D'où : $\mu_k - \lambda_k \leqslant \|v-u\|$, et, symétriquement : $\lambda_k - \mu_k \leqslant \|u-v\|$. □

Remarque. Les endomorphismes symétriques (resp. hermitiens) de E constituent un sous-espace $\mathcal{H}(E)$ de $\mathcal{L}(E)$ que l'on munit de la distance $(f,g) \mapsto \|f-g\|$. En associant à tout $u \in \mathcal{L}(E)$ le k-ième élément (k donné) de la famille croissante des racines du polynôme caractéristique de u, on obtient une application uniformément continue de $\mathcal{H}(E)$ dans $\mathbf{R}$.

3° Ici $Q = \Psi - \Phi$ est positive, de rang r ; N désigne son noyau.

On utilise une base orthonormale $(e'_1, \ldots, e'_n)$ de E telle que :

$$\forall i \in \mathbf{N}_n \quad v(e'_i) = \mu_i e'_i.$$

On note $G'_i = \mathrm{Vect}(e'_i, \ldots, e'_n)$.

• Soit $k \in \mathbf{N}_{n-r}$. On a : $\dim N + \dim G'_k = (n-r) + (n+1-k)$.

Comme : $\dim(N \cap G'_k) = \dim N + \dim G'_k - \dim(N+G'_k)$

il vient : $\dim(N \cap G'_k) \geqslant n + 1 - (k+r)$.

D'où, par (1') et (3), et compte tenu de $\Phi(x) = \Psi(x)$ pour $x \in N$:

$$\lambda_{k+r} \geqslant \min_{x \in S(N \cap G'_k)} \Phi(x) = \min_{x \in S(N \cap G'_k)} \Psi(x) \geqslant \min_{x \in S(G'_k)} \Psi(x) = \mu_k.$$

• Enfin $\lambda_k \leqslant \mu_k$ est une conséquence immédiate de $\Phi \leqslant \Psi$ et de (1). □

• Si $0 \leqslant \Phi \leqslant \Psi$, alors $0 \leqslant \lambda_k \leqslant \mu_k$ et, par multiplication : $0 \leqslant \det u \leqslant \det v$.

5.3.21 Les entiers $n \geqslant 2$ et $i \in \mathbb{N}_n$ sont donnés.

1° Soient $A \in \mathcal{M}_n(\mathbb{R})$ symétrique et $A_i \in \mathcal{M}_{n-1}(\mathbb{R})$ déduite de A en supprimant la i-ème ligne et la i-ième colonne. On note $(\lambda_1,\dots,\lambda_n)$ et $(\alpha_1,\dots,\alpha_{n-1})$ les familles croissantes des racines des polynômes caractéristiques de A et A_i. Montrer :

$$\forall k \in \mathbb{N}_{n-1} \quad \lambda_k \leqslant \alpha_k \leqslant \lambda_{k+1} . \tag{1}$$

2° Soient $A \in \mathcal{M}_{n,1}(\mathbb{R})$ et $B \in \mathcal{M}_n(\mathbb{R})$ symétriques et strictement positives ; A_i et B_i s'en déduisent en supprimant la i-ième ligne et la i-ième colonne. Montrer :

$$\frac{\det(A+B)}{\det(A_i+B_i)} \geqslant \frac{\det A}{\det A_i} + \frac{\det B}{\det B_i} . \tag{2}$$

1° Il est clair que A_i est symétrique. Les polynômes caractéristiques de A et A_i sont donc scindés sur $\mathbb{R}$, ce qui justifie la notation.

$E = \mathbb{R}^n$ est muni de sa structure euclidienne canonique : sa base canonique ε est orthonormale. Soit ε' la famille déduite de ε par suppression du i-ième vecteur ; elle est base orthonormale du sous-espace E' de E qu'elle engendre (muni de la structure euclidienne induite).

On note u et Φ [resp. v et Ψ] l'endomorphisme symétrique de E [resp. E'] et la forme quadratique sur E [resp. E'] représentés par A [resp. A_i] dans la base ε [resp. ε'] ; Ψ est visiblement la restriction de Φ à E'.

On dispose de bases orthonormales e de E et e' de E', telles que :

$$\forall j \in \mathbb{N}_n \quad u(e_j) = \lambda_j e_j \ ; \ \forall j \in \mathbb{N}_{n-1} \quad v(e'_j) = \alpha_j e'_j .$$

• Soit $k \in \mathbb{N}_{n-1}$. Le sous-espace $G' = \mathrm{Vect}(e'_k,\dots,e'_{n-1})$ de E' (et aussi de E) a pour dimension n-k, et, S(G') désignant sa sphère unité, on a (exercice précédent) :

$$\alpha_k = \min_{x \in S(G')} \Psi(x) = \min_{x \in S(G')} \Phi(x) \leqslant \lambda_{k+1} .$$

Les sous-espaces $G = \mathrm{Vect}(e_k,\dots,e_n)$ de E et $F' = \mathrm{Vect}(e'_1,\dots,e'_k)$ de E' ayant les dimensions $n+1-k$ et k, de somme n+1, il existe un vecteur unitaire $y \in G \cap F'$ et :

$$\lambda_k = \min_{x \in S(G)} \Phi(x) \leqslant \Phi(y) = \Psi(y) \leqslant \alpha_k . \qquad \square$$

2° Ici les valeurs propres λ_k de A, et donc (d'après (1)), celles de A_i sont strictement positives ; on a $\det A > 0$ et $\det A_i > 0$.

Puisque $u \in GL(E)$, l'équation linéaire $u(x) = \varepsilon_i$, qui s'écrit :

$$AX = {}^t[0\ldots010\ldots0], \text{ (1 en i-ème position)}$$

admet la solution unique $u^{-1}(\varepsilon_i)$ dont la i-ème composante dans la base canonique ε de E est, d'après les formules de Cramer :

$$\big(\varepsilon_i \big| u^{-1}(\varepsilon_i)\big) = \frac{\det A_i}{\det A} > 0 .$$

• Considérant maintenant $\mathcal{C} = \{x \in \mathbb{R}^n \mid (\varepsilon_i|x) \neq 0\}$, nous allons montrer :

$$\min_{x \in \mathcal{C}} \frac{\big(x \big| u(x)\big)}{(\varepsilon_i|x)^2} = \frac{\det A}{\det A_i} . \tag{3}$$

L'endomorphisme u^{-1} de E est symétrique, de valeurs propres $(\lambda_k)^{-1}$ et donc strictement positif. La forme quadratique associée, dont la forme polaire est $(y,z) \mapsto \big(y \big| u^{-1}(z)\big)$, est positive, non dégénérée, et, en utilisant l'inégalité de Schwarz, on a, pour tout $x \in E$:

$$(\varepsilon_i|x)^2 = \big(\varepsilon_i \big| u^{-1}(u(x))\big)^2 \leqslant \big(\varepsilon_i \big| u^{-1}(\varepsilon_i)\big)\big(u(x) \big| x\big) .$$

S'agissant de réels strictement positifs, retenons :

$$\forall x \in \mathcal{C} \quad \frac{\big(u(x) \big| x\big)}{(\varepsilon_i|x)^2} \geqslant \frac{1}{\big(\varepsilon_i \big| u^{-1}(\varepsilon_i)\big)} = \frac{\det A}{\det A_i} . \tag{4}$$

Pour $x = u^{-1}(\varepsilon_i)$, on a $x \in \mathcal{C}$, et égalité dans (4). D'où (3).

• Les matrices A et B étant symétriques strictement positives, il en est de même pour A+B.

En écrivant (avec $B = \mathrm{mat}(w;\varepsilon)$) :

$$\min_{x \in \mathcal{C}} \frac{\big(x \big| (u+w)(x)\big)}{(\varepsilon_i|x)^2} \geqslant \min_{x \in \mathcal{C}} \frac{\big(x \big| u(x)\big)}{(\varepsilon_i|x)^2} + \min_{x \in \mathcal{C}} \frac{\big(x \big| w(x)\big)}{(\varepsilon_i|x)^2}$$

et en utilisant (3), ainsi que deux égalités analogues, on obtient (2).

5.3.22 Soient Φ et Ψ des formes quadratiques sur $\mathbb{R}^n$ (resp. hermitiennes sur $\mathbb{C}^n$), Φ étant positive, non dégénérée. L'application $f : x \mapsto \Psi(x)/\Phi(x)$ de $\mathbb{R}^n \setminus \{0\}$ (resp. $\mathbb{C}^n \setminus \{0\}$) dans $\mathbb{R}$ est-elle bornée ?

La forme polaire φ de Φ est un produit scalaire, et on dispose de l'espace euclidien $(\mathbb{R}^n, \varphi)$ [resp. de l'espace hermitien $(\mathbb{C}^n, \varphi)$].

Dans celui-ci, $\Phi(x)$ est le carré de la norme du vecteur x, et $\Psi(x)$ s'écrit $\big(x \big| u(x)\big)$, où u est l'endomorphisme φ-symétrique (resp. φ-hermitien) associé à la forme quadratique Ψ.

Soient $(\lambda_1, \ldots, \lambda_n)$ la famille croissante des valeurs propres de u, et e une base φ-orthonormale telle que $u(e_i) = \lambda_i e_i$ pour tout $i \in \mathbb{N}_n$. En utilisant cette base, on constate, pour tout $x \in E$:

$$\lambda_1 \Phi(x) \leqslant \Psi(x) \leqslant \lambda_n \Phi(x) \ ; \ \Psi(e_1) = \lambda_1 \ ; \ \Psi(e_n) = \lambda_n .$$

On en déduit que f admet les bornes λ_1 et λ_n, et qu'elle atteint ces bornes. □

Interprétation matricielle. Soient A et B des (n,n) matrices symétriques (resp. hermitiennes), A étant strictement positive. L'application $X \mapsto \frac{X^* BX}{X^* AX}$ de $\mathbf{R}^n \setminus \{0\}$ (resp. $\mathbb{C}^n \setminus \{0\}$) dans $\mathbf{R}$ est bornée et atteint ses bornes, qui sont la plus petite et la plus grande valeur propre de $A^{-1}B$.

Ici Φ et Ψ sont les formes représentées par A et B dans la base canonique ε.

L'endomorphisme u est représenté dans la base ε par C telle que :

$$\forall X,Y \quad X^* A(CY) = X^* BY,$$

i.e. telle que $AC = B$; A étant inversible, $C = A^{-1}B$. □

Notons que ε n'est en général pas φ-orthonormale, et que C n'est en général pas symétrique (resp. hermitienne), ce qui n'empêche pas son polynôme caractéristique d'être scindé sur $\mathbf{R}$.

5.3.23 On donne $\alpha \in \mathbf{R}_+^*$ et $H \in \mathcal{M}_n(\mathbf{R})$ symétrique et strictement positive ; E_α est l'ensemble des $A \in \mathcal{M}_n(\mathbf{R})$ symétriques, positives et telles que $\det A \geqslant \alpha$. Montrer :

$$\min_{A \in E_\alpha} \left(\operatorname{tr}(AH)\right) = n(\alpha \det H)^{1/n}.$$

• H étant symétrique, il existe U orthogonale et H_1 diagonale telles que :

$$H = UH_1U^{-1}.$$

Les éléments diagonaux $\lambda_1, \ldots, \lambda_n$ de H_1 sont les valeurs propres de H, et, celle-ci étant strictement positive, ce sont des réels strictements positifs.

On a : $$\det H = \det H_1 = \prod_{i=1}^{n} \lambda_i, \quad \lambda_i \in \mathbf{R}_+^*$$

• Soit $A \in E_\alpha$. En utilisant $\operatorname{tr}(VU^{-1}) = \operatorname{tr}(U^{-1}V)$, on obtient :

$$\operatorname{tr}(AH) = \operatorname{tr}(A_1H_1), \text{ où } A_1 = U^{-1}AU.$$

On a : ${}^tA_1 = {}^tU{}^tA{}^t(U^{-1}) = U^{-1}AU = A_1$; A_1 est symétrique.

Semblable à A, A_1 est symétrique positive ; son déterminant est det A, on a donc $A_1 \in E_\alpha$.

Notant $A_1 = [\alpha_{ij}]$, on obtient :

$$\operatorname{tr}(AH) = \operatorname{tr}(A_1H_1) = \sum_{i=1}^{n} \alpha_{ii}\lambda_i, \quad \lambda_i \in \mathbf{R}_+^*.$$

La stricte positivité de A_1 (dûe à $\det A_1 \neq 0$) fait (cf. 5.3.8, 3°) que $\alpha_{ii} \in \mathbf{R}_+^*$ et que $\alpha \leqslant \det A_1 \leqslant \prod_{i=1}^{n} \alpha_{ii}$.

En utilisant l'inégalité classique entre moyennes arithmétique et géométrique, on a donc :

$$\frac{1}{n}\,\mathrm{tr}(AH) \geqslant \left(\prod_{i=1}^{n}\alpha_{ii}\lambda_i\right)^{1/n} = \left(\prod_{i=1}^{n}\alpha_{ii}\right)^{1/n}\left(\prod_{i=1}^{n}\lambda_i\right)^{1/n}$$

et : $$\mathrm{tr}\,(AH) \geqslant n(\alpha \det H)^{1/n}. \qquad (1)$$

En particulier la matrice $A_o = (\alpha \det H)^{1/n} H^{-1}$ est symétrique positive, et telle que : $\det A_o = (\alpha \det H).\det H^{-1} = \alpha$. On a :

$$A_o \in E_\alpha \quad \text{et} \quad \mathrm{tr}(A_o H) = n(\alpha \det H)^{1/n}$$

ce qui achève la démonstration. □

Remarque. Le résultat reste vrai si l'on remplace $\mathcal{M}_n(\mathbb{R})$ par $\mathcal{M}_n(\mathbb{C})$ et symétrique par hermitienne (U est alors unitaire).

5.3.24 On donne $H \in \mathcal{M}_n(\mathbb{R})$ symétrique et positive. $O(n)$ désignant le groupe orthogonal de degré n sur $\mathbb{R}$, montrer :

$$\max_{A\in O(n)} \left(\mathrm{tr}(AH)\right) = \mathrm{tr}\ H.$$

• H étant symétrique, il existe U orthogonale et H_1 diagonale telles que :

$$H = UH_1U^{-1}.$$

Les éléments diagonaux $\lambda_1,\ldots,\lambda_n$ de H_1 sont les valeurs propres de la matrice symétrique H, et, celle-ci étant positive, ce sont des réels positifs.

On a : $$\mathrm{tr}\ H = \mathrm{tr}\ H_1 = \sum_{i=1}^{n}\lambda_i, \quad \lambda_i \in \mathbb{R}_+.$$

• Soit $A \in O(n)$. En utilisant $\mathrm{tr}(VU^{-1}) = \mathrm{tr}(U^{-1}V)$, on obtient :

$$\mathrm{tr}(AH) = \mathrm{tr}(AUH_1U^{-1}) = \mathrm{tr}(U^{-1}AUH_1)$$

et : $$\mathrm{tr}(AH) = \mathrm{tr}(A_1H_1), \text{ où } A_1 = U^{-1}AU \text{ appartient à } O(n).$$

Notant $A_1 = [\alpha_{ij}]$, on obtient :

$$\mathrm{tr}(AH) = \mathrm{tr}(A_1H_1) = \sum_{i=1}^{n}\alpha_{ii}\lambda_i, \quad \lambda_i \in \mathbb{R}_+.$$

Or, A_1 étant orthogonale : $\sum_{j=1}^{n}\alpha_{ij}^2 = 1$, et $\alpha_{ii}^2 \leqslant 1$, et $\alpha_{ii} \leqslant 1$.

D'où : $$\mathrm{tr}(AH) \leqslant \sum_{i=1}^{n}\lambda_i, \text{ i.e. } \mathrm{tr}(AH) \leqslant \mathrm{tr}\ H. \qquad (1)$$

On achève la démonstration en utilisant $I_n \in O(n)$ et $\mathrm{tr}(I_nH) = \mathrm{tr}\ H$.

Remarques. a) Si H est inversible, on n'a égalité dans (1) que pour $A = I_n$. En effet, ici $\lambda_i \in \mathbb{R}_+^*$, et compte-tenu de $\alpha_{ii} \leqslant 1$, on n'a $\sum_{i=1}^{n}\alpha_{ii}\lambda_i = \sum_{i=1}^{n}\lambda_i$ que si les α_{ii} sont tous égaux à 1, ce qui exige $\alpha_{ij} = 0$ pour $i \neq j$; d'où $A_1 = I_n$ et $A = I_n$.

b) Le résultat reste vrai si l'on part de H hermitienne et positive, et si A décrit le groupe unitaire de degré n.

5.3.25 Soient une (n,n) matrice A réelle, symétrique positive, et un entier $k \geqslant 1$. Montrer qu'il existe une unique (n,n) matrice B réelle, symétrique positive, telle que $B^k = A$.

Nous allons démontrer la proposition équivalente : *Soient un espace euclidien* E, *un endomorphisme* u *symétrique positif de* E, *et un entier* $k \geqslant 1$; *alors il existe un unique endomorphisme* v *symétrique positif de* E *tel que* $v^k = u$.

Le polynôme caractéristique de u est scindé sur $\mathbb{R}$; soient $\lambda_1,\ldots,\lambda_p$ ses racines distinctes, qui sont des réels positifs ; pour tout $i \in \mathbb{N}_p$, notons E_i le sous-espace propre de u associé à la valeur propre λ_i ; E est somme directe orthogonale des E_i ; u induit sur E_i l'endomorphisme $\lambda_i I_i$, où I_i est l'identité de E_i.

Nous allons raisonner par conditions nécessaires et suffisantes.

a) Supposons qu'il existe une solution v.

- Puisque $v^k = u$, nous avons $uv = vu$ $(= v^{k+1})$, et donc chaque E_i est stable par v ; notons v_i l'endomorphisme de E_i induit par v.

- Utilisant à nouveau $v^k = u$, nous avons : $v_i^k = \lambda_i I_i$.

- D'autre part, v étant symétrique il est clair que v_i l'est (pour la structure euclidienne induite) ; v étant positif, v_i l'est (les valeurs propres de v_i sont des valeurs propres de v). Il existe donc une base e_i de E_i qui diagonalise v_i ; nous avons :

$$\mathrm{mat}(v_i;e_i) = \mathrm{diag}(\alpha_{i,1},\ldots,\alpha_{i,m_i}),\ m_i = \dim E_i,$$

et, d'après ce qui précède :

$$\forall j \in \mathbb{N}_{m_i} \quad (\alpha_{i,j} \geqslant 0) \wedge \left((\alpha_{i,j})^k = \lambda_i\right), \text{ et donc } \alpha_{i,j} = \lambda_i^{1/k}.$$

Retenons : $v_i = \lambda_i^{1/k} I_i$.

• A ce stade, nous pouvons affirmer que le problème a au maximum une solution, l'endomorphisme w de E défini par :

$$\forall i \in \mathbb{N}_p \quad \forall x \in E_i \quad w(x) = \lambda_i^{1/k} x. \tag{1}$$

b) Reste à s'assurer que cet endomorphisme est une solution. Or de (1) on déduit que $w^k = u$, que w est symétrique, et que la forme quadratique $x \mapsto (x|w(x))$ est positive. □

Remarques. a) Il résulte de cet exercice que deux (n,n) matrices réelles, symétriques positives sont égales si et seulement s'il existe $k \in \mathbb{N}^*$ tel que $A^k = B^k$.

b) On se place souvent dans le cas $k = 2$ (cf. exercice suivant).

c) Le résultat subsiste si on remplace réelle symétrique par hermitienne.

5.3.26 Soit $A \in GL_n(\mathbb{R})$. Montrer qu'il existe un unique couple (S,M), où $S \in O(n)$ et où $M \in \mathcal{M}_n(\mathbb{R})$ est symétrique et positive, vérifiant :

$$A = SM.$$

Raisonnons par condition nécessaire et suffisante.

• Supposons qu'il existe un couple (S,M) répondant à la question.

Nous avons : ${}^tA = {}^tM{}^tS = MS^{-1}$, et donc ${}^tAA = M^2$.

Nous savons que ${}^tAA$ est symétrique et positive. L'exercice précédent nous apprend qu'il existe une unique matrice symétrique et positive H telle que ${}^tAA = H^2$. Nous avons donc nécessairement M = H.

Comme A est inversible, nous avons $(\det H)^2 = (\det A)^2 \neq 0$; H est inversible et A = SH exige $S = AH^{-1}$.

• Le problème admet donc au maximum une solution, le couple (AH^{-1},H), où H est l'unique matrice symétrique et positive telle que $H^2 = {}^tAA$.

• Pour s'assurer que ce couple convient, il suffit de s'assurer que AH^{-1} est orthogonale. Or :

$${}^t(AH^{-1}) = {}^t(H^{-1}){}^tA = ({}^tH)^{-1}{}^tA = H^{-1}{}^tA$$

et : $${}^t(AH^{-1})(AH^{-1}) = H^{-1}{}^tAAH^{-1} = H^{-1}H^2H^{-1} = I_n.$$ □

Remarque. a) On peut voir que, si l'on suppose seulement $A \in \mathcal{M}_n(\mathbb{R})$, on dispose encore d'un couple (S,M) répondant à la question, mais ce couple n'est pas nécessairement unique.

b) On peut remplacer la condition A = SM par A = MS.

c) Pour $A \in GL_n(\mathbb{C})$ on a, de façon unique, A = SM, où $S \in U(n)$ et où M est hermitienne positive.

5.3.27 $\mathbf{R}^n$ est muni de sa structure euclidienne canonique ; la base canonique ε est orthonormale ; Φ est la forme quadratique sur $\mathbf{R}^n$ déterminée par :

$$\sum_{k=1}^{n} \xi_k \varepsilon_k \mapsto \sum_{k=1}^{n} (\xi_1 + \ldots + \xi_k)^2$$

Expliciter une base orthonormale de $\mathbf{R}^n$ dans laquelle Φ est représentée par une matrice diagonale.

La forme quadratique Φ (qui est positive et non dégénérée) est représentée dans la base orthonormale ε par la matrice symétrique $\Omega = [\omega_{ij}]$, où $\omega_{ij} = n+1 - \max(i,j)$. Il s'agit de trouver les valeurs propres de Ω (qui sont strictement positives) et d'expliciter une base orthonormale de $\mathbf{R}^n$ formée de vecteurs propres de Ω (le cours nous garantit l'existence d'une telle base).

• Le réel $\lambda \in \mathbf{R}_+^*$, est une valeur propre de Ω si, et seulement si le système des n équations linéaires $f_p = 0$, $1 \leqslant p \leqslant n$, dans lequel :

$$f_p(x_1,\dots,x_n) = (n+1-p)\sum_{j=1}^{p} x_j + \sum_{j=p+1}^{n}(n+1-j)x_j - \lambda x_p$$

admet une solution non nulle. Ce système s'écrit successivement :

$$-f_p + f_{p+1} = 0,\ 1 \leqslant p \leqslant n-1\ ;\ -f_n = 0$$

$$-f_1 + f_2 = 0\ ;\ f_{p-1} - 2f_p + f_{p+1} = 0,\ 2 \leqslant p \leqslant n-1\ ;\ f_{n-1} - 2f_n = 0.$$

On adjoint les inconnues x_o et x_{n+1}, les équations $x_o = x_1$ et $x_{n+1} = 0$, ce qui ramène à écrire que le système des n+2 équations linéaires :

$$(S_\lambda)\ \begin{cases} x_{p-1} + \left(\frac{1}{\lambda} - 2\right)x_p + x_{p+1} = 0,\ 1 \leqslant p \leqslant n \\ x_o = x_1\ ;\ x_{n+1} = 0 \end{cases}$$

admet une solution non nulle, i.e. telle que $x_o \neq 0$.

On voit apparaître une suite récurrente, ce qui conduit à considérer les zéros sur $\mathbb{C}$, r et 1/r, de $X^2 + \left(\frac{1}{\lambda} - 2\right)X + 1$; notons que $r \neq 1$.

- Si $\lambda = 1/4$, on a $r = 1/r = -1$, et (S_λ) s'écrit :

$$\begin{cases} x_p = (a+bp)(-1)^p,\ 0 \leqslant p \leqslant n+1 \\ a = -(a+b)\ \ ;\ \ a + b(n+1) = 0 \end{cases}$$

et n'admet que la solution nulle ; 1/4 n'est pas valeur propre de Ω.

- Soit $\lambda \in \mathbf{R}_+^* \setminus \{1/4\}$. On a $r \neq -1$, et (S_λ) s'écrit :

$$\begin{cases} x_p = ar^p + br^{-p}\ ;\ 0 \leqslant p \leqslant n+1 \\ a + b = ar + br^{-1}\ ;\ ar^{n+1} + br^{-n-1} = 0 \end{cases}$$

et donc (compte tenu de $r \neq 1$) :

$$\begin{cases} b = ar\ ;\ r^{2n+1} = -1 \\ x_p = a(r^p + r^{1-p}),\ \ 0 \leqslant p \leqslant n+1. \end{cases}$$

Pour que $\lambda \in \mathbf{R}_+^* \setminus \{1/4\}$ soit valeur propre de Ω, il faut et il suffit que $r^{2n+1} = -1$ avec $r \neq -1$, i.e. que r soit l'un des $r_k = \exp(i\theta_k)$ avec $\theta_k = \frac{2k-1}{2n+1}\pi$ et $k \in \mathbf{N}_n$, ou l'un des inverses de ces r_k, i.e. que $1/\lambda = 2 - r - 1/r$ soit l'un des $2 - 2\cos\theta_k = 4\sin^2\theta/2$, i.e. que λ soit l'un des $\lambda_k = 1/(4\sin^2(\theta_k/2))$.

En conclusion, la (n,n) matrice symétrique Ω admet les n valeurs propres λ_k strictement positives et deux à deux distinctes. On sait en outre que des vecteurs propres associés à des valeurs propres distinctes sont orthogonaux.

• Pour $k \in \mathbf{N}_n$ le sous-espace propre associé à λ_k s'écrit donc $\mathbf{R}c_k$, où c_k a pour composantes dans la base canonique les $a(r_k^p + r_k^{1-p})$, $p \in \mathbf{N}_n$, ou des nombres proportionnels, par exemple les :

$$\frac{1}{2}\left(r_k^{p-1/2} + r_k^{-p+1/2}\right) = \cos\left((p-1/2)\theta_k\right),\ \ \theta_k = \frac{2k-1}{2n+1}\pi.$$

De $c_k = \sum_{p=1}^{n} \cos\left((p-1/2)\theta_k\right)\varepsilon_p$, on déduit :

$$2\|c_k\|^2 = n + \sum_{p=1}^{n} \cos\big((2p-1)\theta_k\big).$$

Or : $$-1 + 2\sum_{p=1}^{n} \cos\big((2p-1)\theta_k\big) = \sum_{p=-n}^{n} \cos\big((2p-1)\theta_k\big) = 0.$$

D'où : $$2\|c_k\|^2 = n+1/2 \quad \text{et} \quad \|c_k\| = \sqrt{2n+1}\ /2\ .$$

• Finalement $(e_1,\ldots,e_n)$, où $e_k = \dfrac{2}{\sqrt{2n+1}}\, c_k$, est une base orthonormale de $\mathbf{R}^n$ dans laquelle la forme quadratique Φ s'écrit :

$$\sum_{k=1}^{n} \eta_k e_k \longmapsto \sum_{k=1}^{n} \frac{1}{4\sin^2\theta_k/2}\, \eta_k^2.$$

5.3.28 Soit $n \in \mathbf{N}^*$. A toute (n,n) matrice réelle orthogonale $A = [a_{ij}]$, $(i,j) \in \mathbf{N}_n^2$, on associe le réel $f(A) = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij}$.

1° Montrer que l'application f de O(n) dans R ainsi définie admet une borne supérieure, qui sera notée μ.

2° Montrer qu'il existe une matrice triangulaire T telle que, pour toute matrice A de O(n), $f(A) = \mathrm{tr}(AT)$; en déduire qu'il existe une matrice symétrique et positive H telle que $\mu = \mathrm{tr}\ H$ et une unique matrice orthogonale A telle que $f(A) = \mu$.

3° Vérifier : $$\mu = \mathrm{tr}\ H = \frac{1}{2} \sum_{k=1}^{\mu} 1/\cos\frac{k\pi}{2n+1}\ . \qquad (1)$$

1° Les éléments a_{ij} d'une matrice orthogonale vérifiant $a_{ij}^2 \leqslant 1$, et donc $a_{ij} \leqslant 1$, on a $f(A) \leqslant n(n+1)/2$ pour toute $A \in O(n)$.

L'application f est ainsi majorée ; elle admet donc une borne supérieure. □

2° On constate que $f(A) = \mathrm{tr}(AT)$, où T est la (n,n) matrice réelle dont l'élément (i,j) est 1 si $i \geqslant j$, et 0 si $i < j$.

T est inversible ($\det T = 1$) et - d'après l'exercice n° 5.3.26 - elle s'écrit de manière unique $T = SH$, où $S \in O(n)$ et où H est l'unique matrice réelle, symétrique et positive telle que $H^2 = {}^tTT$.

Pour toute $A \in O(n)$, on a ainsi $f(A) = \mathrm{tr}(ASH)$, avec $AS \in O(n)$; d'après l'exercice 5.3.24, on en déduit :

$$f(A) \leqslant \mathrm{tr}\ H,$$

et, H étant inversible, on n'a l'égalité que si $AS = I_n$, ce qui s'écrit : $A = S^{-1} = HT^{-1}$. En conclusion : $\mu = \mathrm{tr}\ H$. □

3° La matrice $\Omega = {}^tTT$ est symétrique, positive et inversible ; son polynôme caractéristique admet une famille de racines de la forme $(\lambda_1,\ldots,\lambda_n)$

avec $\lambda_k \in \mathbb{R}_+^*$. On sait que $(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_n})$ est une famille de racines du polynôme caractéristique de H, et on a

$$\mu = \operatorname{tr} H = \sum_{k=1}^{n} \sqrt{\lambda_k}.$$

On calcule : $\Omega = [\omega_{ij}]$ avec $\omega_{ij} = n+1 - \max(i,j)$.

Les valeurs propres de Ω ont été calculées (exercice précédent). Nous avons obtenu les $\lambda_k = \dfrac{1}{4\sin^2 \theta_k/2}$; $\theta_k = \dfrac{2k-1}{2n+1}\pi$, $k \in \mathbb{N}_n$.

Nous avons $0 < \theta_k < \pi$ et donc $\sin \theta_k/2 > 0$. D'où, en utilisant :

$$\frac{\theta_k}{2} = \frac{\pi}{2} - \frac{(n+1-k)\pi}{2n+1}$$

$$\mu = \frac{1}{2} \sum_{k=1}^{n} 1/\cos \frac{(n+1-k)\pi}{2n+1} \; . \qquad \square$$

MASSON, Editeur
120, boulevard Saint-Germain
75280 Paris Cedex 06
Dépôt légal : juin 1992

Imprimé en France

IMPRIMERIE LOUIS-JEAN
av. d'Embrun, 05002-GAP
Dépôt légal : 373 mai 1992

ISBN : 2-225-81314-0