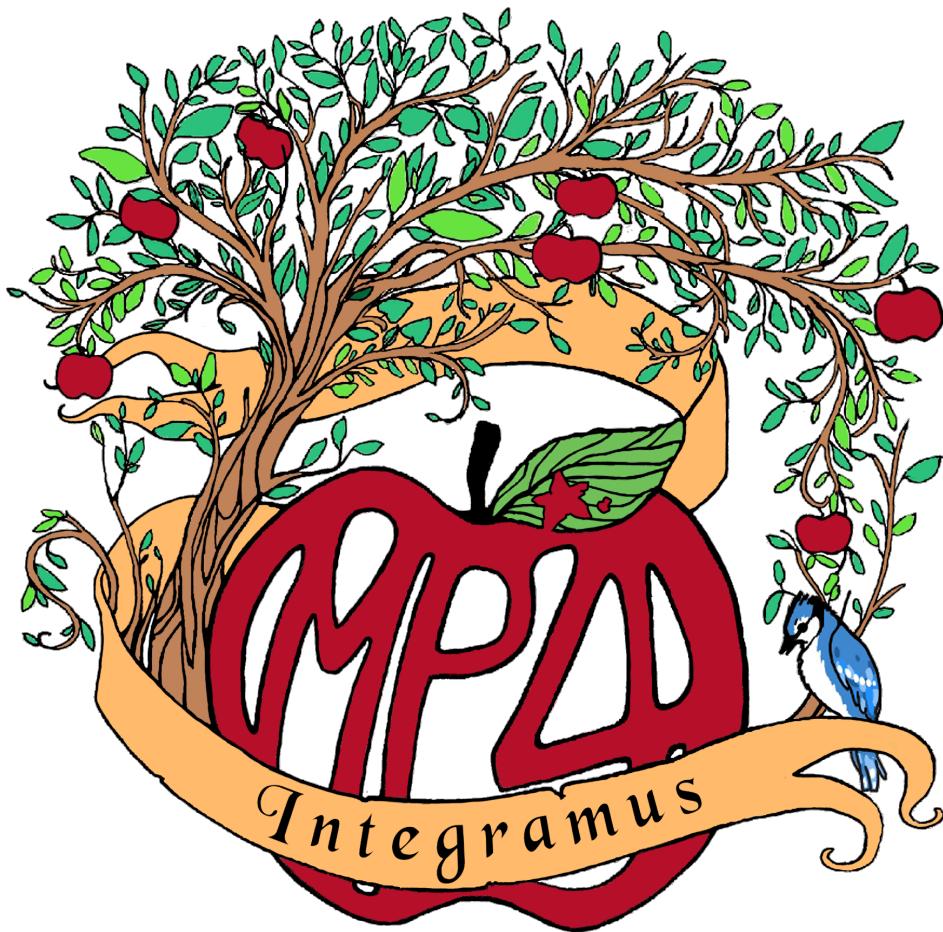


Mathématiques en MP*

Un livre inspiré par le cours de la MP*4 du lycée Louis-le-Grand

Omar Bennouna, Issam Tauil & Mehdi Chouta

Tous les cours de mathématiques indispensables pour une deuxième
année en MP*



Publié sur www.cpge-paradise.com

Préface

Ce livre contient tous les chapitres de mathématiques de deuxième année de CPGE filière MP. Les chapitres de ce cours ont été inspirés des notes de cours de la MP*4 du lycée Louis-le-Grand pendant l'année scolaire 2018/2019. Toutes les propriétés, théorèmes, et différents éléments ont été rédigés de manière assez détaillée et sont accompagnés, lorsque cela est nécessaire, de schémas et dessins qui aideront l'élève à avoir l'intuition de chaque résultat présenté. Tous les exercices du cours ont été corrigés de manière assez détaillée de manière à ce que l'élève puisse progresser si jamais il n'arrive pas à résoudre un exercice. Tous les cours contiennent un nombre considérable de notions hors programme très utile pour les concours de haut niveau (X-ENS, Centrale, Mines-Ponts). Nous espérons que le contenu de ce livre sera utile pour les élèves désirant s'approfondir dans les notions vues en deuxième année. Les chapitres actuellement présents dans cette version du livre ne représentent pas l'intégralité des chapitres du cours. Par conséquent, ce livre sera progressivement mis à jour sur le site cpge-paradise.com. Si jamais vous repérez une erreur ou alors quelque chose qui n'est pas claire lors de votre lecture, n'hésitez pas à nous contacter via l'adresse contact@cpge-paradise.com.

Remerciements

Nous remercions nos professeurs de mathématiques de classes préparatoires de première et deuxième année Roger Mansuy, Alain Troesh, Yves Duval et Alain Pommellet pour la formation excellente et très agréable qu'ils nous ont offert. Nos deux années au lycée Louis-le-Grand étaient une très belle expérience grâce à eux. Nous sommes très reconnaissants à Alain Pommellet en particulier qui nous a donné son accord pour nous inspirer des notes de son cours en MP*4, Gauthier Thomas, notre professeur du cours des fonctions holomorphes à l'X pour nous avoir fourni une partie de son template LaTeX. Enfin, nous remercions également nos familles qui ont toujours été là pour nous et sans qui nous n'aurions pas pu en arriver là.

Auteurs du livre



Omar Bennouna est actuellement en troisième année du cycle d'ingénieur de l'École polytechnique au sein du département de mathématiques appliquées. Après avoir eu son bac au Maroc, il a fait deux ans de classes préparatoires en MPSI2 puis en MP*4 au lycée Louis-le-Grand. Il poursuivra à partir de septembre 2022 une thèse en mathématiques appliquées aux États-Unis.



Issam Tauil est actuellement en troisième année du cycle d'ingénieur de l'École polytechnique au sein du département de mathématiques fondamentales. Après avoir eu son bac au Maroc, il a fait deux ans de classes préparatoires en MPSI4 puis en MP*2 au lycée Louis-le-Grand. En 2021, il décroche une médaille d'or à l'IMC (International Mathematics Olympiad).



Mehdi Chouta est actuellement en troisième année du cycle d'ingénieur de l'École polytechnique où il est spécialisé en cybersécurité. Après avoir eu son bac, il a fait ses classes préparatoires en PCSI puis en PC* au lycée Henri Poincaré à Nancy.

Je dédie ce livre à Amine qui a été
et sera toujours ma plus grande
inspiration.

”Si je suis stupide, je serai la première personne stupide qui va réussir.”

Table des matières

Chapitre 1 : Ordre, inégalités	6
BORNE SUPÉRIEURE	
ENCADREMENTS	
INÉGALITÉS CLASSIQUES	
ÉTUDE DE FONCTIONS	
Chapitre 3 : Cardinaux	18
GÉNÉRALITÉS	
ENSEMBLES DÉNOMBRABLES	
EXERCICES	
Chapitre 11.1 : Espaces vectoriels normés et espaces métriques	25
ESPACES VECTORIELS NORMÉS	
GÉOMÉTRIE	
ESPACES MÉTRIQUES	
BOULES OUVERTES, FERMÉS, SPHÈRES ...	
BORNITUDE	
SUITES DANS UN ESPACE MÉTRIQUE ET DANS UN ESPACE VECTORIEL NORMÉ	
ALGÈBRES NORMÉES	
SUITES DE FONCTIONS	
Chapitre 11.2 : Ouverts et fermés	39
OUVERTS	
FERMÉS	
TOPOLOGIE INDUIITE	
INTÉRIEUR	
ADHÉRENCE	
DENSITÉ	
Chapitre 11.3 : Limites et continuité	56
LIMITES	
CONTINUITÉ	
Chapitre 11.4 : Comparaison de normes et espaces produits	74
COMPARAISON DE NORMES	
ESPACES PRODUITS	
Chapitre 11.5 : Compacité	88
VALEURS D'ADHÉRENCE	

DÉFINITIONS ET PROPRIÉTÉS STRUCTURELLES

PRODUIT D'ESPACES COMPACTS

SUITES DANS UN COMPACT

UNIFORME CONTINUITÉ

OPTIMISATION SUR UN COMPACT

COMPLÉMENTS

Chapitre 11.6 : Applications linéaires continues

105

QUELQUES PROPRIÉTÉS

EXERCICES

Chapitre 11.7 : Espaces vectoriels normés de dimension finie

113

ÉQUIVALENCE DES NORMES

SUITES ET COMPOSANTES

COMPACITÉ ET COMPLÉTUDE

FONCTIONS POLYNÔMES SUR \mathbb{K}^n

EXERCICES

Chapitre 11.8 : Connexité

124

GÉNÉRALITÉS

PARTIES CONNEXES PAR ARC

APPLICATION AUX FONCTIONS À VARIABLES RÉELLES

Chapitre 11.9 : Convexité

134

ENVELOPPE CONVEXE

PROJECTION ET SÉPARATION

Chapitre 19 : Groupes

142

LE GROUPE $(\mathbb{Z}/n\mathbb{Z}, +)$

ORDRE D'UN ÉLÉMENT

ACTIONS DE MORPHISMES

GROUPES CYCLIQUES

GROUPE ENGENDRÉ PAR UNE PARTIE

COMPLÉMENTS

Chapitre 23 : Polynômes

170

PRÉAMBULE

POLYNÔMES COMPLEXES

POLYNÔMES RÉELS

POLYNÔMES À COEFFICIENTS RATIONNELS

IRRÉDUCTIBILITÉ DE $\mathbb{Z}[X]$

CPGE

paradise

Chapitre 26 : Systèmes linéaires	183
GÉNÉRALITÉS	
SYSTÈME DE CRAMER	
VALEURS PROPRES ET SYSTÈMES HOMOGÈNES	
MATRICES DE PERMUTATION	
COMMENT DÉTERMINER $\text{Ker } A$ EN PRATIQUE ?	
COMMENT RÉSOUTRE $AX = B$ EN PRATIQUE ?	
Chapitre 28 : Réduction d'endomorphisme	194
STABILITÉ	
ÉLÉMENTS PROPRES	
ENDOMORPHISMES ET MATRICES DIAGONALISABLES	
ACTION DES POLYNÔMES	
POLYNOME CARACTÉRIQUE	
TRIGONALISATION	
ENDOMORPHISMES CYCLIQUES	
RÉDUCTION ET TOPOLOGIE	
Chapitre 30.1 : Probabilités	247
TRIBUS	
ESPACES PROBABILISÉS	
ÉVÉNEMENT PRESQUE SÛR, ÉVÉNEMENT NÉGLIGEABLE	
EXEMPLES D'ESPACES PROBABILISÉS	
Chapitre 30.2 : Indépendance, conditionnement	253
ÉVÉNEMENTS INDÉPENDANTS	
CONDITIONNEMENT	
TRIBUS INDÉPENDANTES	
BOREL-CANTELLI	
Chapitre 30.3 : Variables aléatoires	258
GÉNÉRALITÉS	
VARIABLES DISCRÈTES	
VARIABLES ALÉATOIRES DISCRÈTES INDÉPENDANTES	
LOIS USUELLES	
COMPLÉMENTS	
Chapitre 30.4 : Couples de variables aléatoires	268
LOI CONJOINTE, LOI MARGINALE	

Chapitre 34 : Espaces préhilbertiens réels	271
GÉOMÉTRIE D'UN ESPACE PRÉHILBERTIEN	
ORTHOGONALITÉ	
Compléments : Espaces préhilbertiens réels, compléments	284
DÉCOMPOSITION DE CARTAN (IWASAWA)	
MATRICES DE GRAM	
Chapitre 36 : Espaces préhilbertiens complexes	292
ESPACES HERMITIENS	
OPÉRATIONS UNITAIRES	
Chapitre 42 : Endomorphismes d'un espace hermitien	297
ADJONCTION MATRICIELLE	
ADJONCTION DANS $\mathcal{L}(E)$	



CHAPITRE 1

Ordre, inégalités

I Borne supérieure

Rappel I.1.

Toute partie de \mathbb{R} non vide et majorée possède une borne supérieure.

Contre-exemple dans \mathbb{Q} : L'ensemble $A = \{r \in \mathbb{Q} \mid r^2 < 2\}$ ne possède pas de borne supérieure rationnelle. En effet, supposons qu'il en ait une et posons $C = \sup A \in \mathbb{Q}$. Alors $0 \leq C \leq \sqrt{2}$ car $\sqrt{2}$ est un majorant de A , et $0 \in A$. Mieux, $C < \sqrt{2}$ car $\sqrt{2}$ est irrationnel. Par densité de \mathbb{Q} dans \mathbb{R} , il existe $r \in \mathbb{Q}$ tel que $0 \leq C < r < \sqrt{2}$. Donc $r^2 < 2$, donc C n'est pas le supremum de A .

Proposition I.2.

Soit $c \in \mathbb{R}$. Si A est une partie de \mathbb{R} non vide et majorée, alors on a l'équivalence :

$$c = \sup A \iff \forall x \in A, x \leq c \text{ et } \forall \varepsilon > 0, \exists x \in A, c - \varepsilon < x \leq c$$

Applications

1. Le théorème de la limite monotone pour les suites réelles bornées en est une.
2. Considérons une fonction $f : \mathbb{R}^+ \mapsto \mathbb{R}$ croissante et majorée. Alors f possède une limite finie en $+\infty$. En effet, posons $\ell = \sup f$, et fixons $\varepsilon > 0$. Il existe alors $x_\varepsilon \in \mathbb{R}^+$ tel que $\ell - \varepsilon < f(x_\varepsilon) \leq \ell$. La croissance de f assure de plus que pour tout $x \geq x_\varepsilon$, $\ell - \varepsilon < f(x) \leq \ell$. Donc, $f(x) \xrightarrow{x \rightarrow +\infty} \ell$.

Proposition I.3.

Soit A une partie de \mathbb{R} non vide et majorée.

- Si $\lambda > 0$, alors $\sup(\lambda A) = \lambda \sup(A)$.
- Si $a \in \mathbb{R}$, $\sup(a + A) = a + \sup(A)$.

De même, considérons des fonctions f et g d'un ensemble non vide I et à valeurs dans \mathbb{R} .

- Si $\lambda > 0$, alors $\sup(\lambda f) = \lambda \sup(f)$.
- Si $a \in \mathbb{R}$, $\sup(a + f) = a + \sup(f)$.
- $\sup(f + g) \leq \sup(f) + \sup(g)$.



Preuve de l'inégalité : Pour tout $x \in I$, $f(x) + g(x) \leq \sup(f) + \sup(g)$.
Donc $\sup(f + g) \leq \sup(f) + \sup(g)$

Corollaire I.4.

Soient a et $b \in \mathbb{R}$ tels que $a \leq b$. Alors l'application

$$\begin{aligned}\|\cdot\|_\infty : \mathcal{C}^0([a, b], \mathbb{R}) &\longrightarrow \mathbb{R} \\ f &\longmapsto \sup(|f|)\end{aligned}$$

est une norme.

Supremum d'un ensemble paramétré par deux variables

Soient A et B deux ensembles non vides, et $f : A \times B \longrightarrow \mathbb{R}$ une fonction majorée. Montrons que

$$\sup f = \sup_{x \in A} \left(\sup_{y \in B} (f(x, y)) \right) = \sup_{y \in B} \left(\sup_{x \in A} (f(x, y)) \right)$$

Posons $M = \sup f$, et pour tout $x \in A$, posons $\mu_x = \sup_{y \in B} (f(x, y))$. Pour tout $x \in A$, et pour tout $y \in B$, $f(x, y) \leq M$. Donc, pour tout $x \in A$, $\mu_x \leq M$. Donc $\sup_{x \in A} (\mu_x) \leq M$.

Par ailleurs, pour tout $(x, y) \in A \times B$, $f(x, y) \leq \mu_x \leq \sup_{x \in A} (\mu_x)$. Donc $M \leq \sup_{x \in A} (\mu_x)$. Donc

$$M = \sup_{x \in A} (\mu_x)$$

et la deuxième égalité se démontre de la même manière en échangeant les rôles de x et y .

Considérons maintenant un ensemble non vide Ω indexant une famille $(f_\lambda)_{\lambda \in \Omega}$ de fonctions d'une partie non vide I de \mathbb{R} à valeurs dans \mathbb{R} .

Définition I.5.

On dit que

- $(f_\lambda)_{\lambda \in \Omega}$ est majorée si pour tout $x \in I$, la famille de réels $(f_\lambda(x))_{\lambda \in \Omega}$ est majorée.
- $(f_\lambda)_{\lambda \in \Omega}$ est uniformément majorée s'il existe $M \in \mathbb{R}$ tel que pour tout $\lambda \in \Omega$ et pour tout $x \in I$, $f_\lambda(x) \leq M$.
- $(f_\lambda)_{\lambda \in \Omega}$ est uniformément bornée s'il existe $K \in \mathbb{R}$ tel que pour tout $\lambda \in \Omega$ et pour tout $x \in I$, $|f_\lambda(x)| \leq K$.

Si pour tout $x \in I$, $(f_\lambda(x))_{\lambda \in \Omega}$ est majorée, on appelle *enveloppe supérieure de la famille* $(f_\lambda)_{\lambda \in \Omega}$ la fonction

$$\begin{aligned}\sup_{\lambda \in \Omega} (f_\lambda) : I &\longrightarrow \mathbb{R} \\ x &\longmapsto \sup_{\lambda \in \Omega} (f_\lambda(x))\end{aligned}$$

Proposition I.6.

Si Ω est fini et si les f_λ sont continues, alors $\sup_{\lambda \in \Omega} (f_\lambda)$ est continue.

 **Preuve :** Soient f_1 et f_2 deux fonctions continues sur I et à valeurs réelles.

Il est aisément vérifiable – donc loisible de retenir – que  $\sup(f_1, f_2) = \frac{1}{2}(f_1 + f_2 + |f_1 - f_2|)$, ce qui assure sa continuité.

Le principe de récurrence finie assure alors que $\sup_{\lambda \in \Omega}(f_\lambda)$ est continue.

 **Contre-exemple avec une famille infinie :** Pour tout $n \in \mathbb{N}$ et pour tout $x \in [0, 1]$, posons $f_n(x) = 1 - x^n$. La famille de fonctions ainsi définie est uniformément bornée par 1 donc son enveloppe supérieure est bien définie.

Or, $\left(\sup_{n \in \mathbb{N}}(f_n)\right)(1) = 0$ et pour tout $x \in [0, 1[$, $\left(\sup_{n \in \mathbb{N}}(f_n)\right)(x) = 1$, donc l'enveloppe supérieure des f_n n'est pas continue.

II Encadrements

Proposition II.1.

Soient $a, b \in \mathbb{R}$. On a l'équivalence

$$a \leq b \iff \forall \varepsilon > 0, a \leq b + \varepsilon$$

 **Preuve :** (\Rightarrow) Cette implication est immédiate.

(\Leftarrow) Supposons que $a > b$ et posons $\varepsilon = \frac{a-b}{2}$. Alors, par hypothèse, $a \leq \frac{a+b}{2}$ mais $\frac{a+b}{2} < a$ car $b < a$. Donc $a \leq b$.

Encadrements de fractions

Si $0 \leq a' \leq a \leq a''$ et $0 < b' \leq b \leq b''$ alors $\frac{a'}{b''} \leq \frac{a}{b} \leq \frac{a''}{b'}$

Valeurs absolues

\rightarrow Si $x \in \mathbb{R}$, $|x| \leq M \iff -M \leq x \leq M$.

\rightarrow **Inégalité triangulaire :** Soit n un entier supérieur ou égal à 2. Soit $(z_1, \dots, z_n) \in (\mathbb{C}^*)^n$. Alors

$$||z_1| - |z_2|| \leq |z_1 + z_2| \leq |z_1| + |z_2| \quad \text{et} \quad \left| \sum_{k=1}^n z_k \right| \leq \sum_{k=1}^n |z_k|$$

 **Preuve de l'inégalité triangulaire :** Avec deux complexes,

$$|z_1 + z_2|^2 = |z_1|^2 + 2 \operatorname{Re}(z_1 \overline{z_2}) + |z_2|^2 \leq |z_1|^2 + 2|z_1 z_2| + |z_2|^2 = (|z_1| + |z_2|)^2$$

d'où la majoration. Remarquons qu'en l'appliquant à nouveau, il vient que

$$\begin{aligned} |z_1| &= |z_1 + z_2 - z_2| \leq |z_1 + z_2| + |z_2| \quad \text{et} \quad |z_2| = |z_2 + z_1 - z_1| \leq |z_2 + z_1| + |z_1| \end{aligned}$$

d'où la minoration. Une récurrence permet de généraliser la majoration à n complexes.

Extension : Si la série $\sum_{n \geq 0} |z_n|$ converge, alors $\sum_{n \geq 0} z_n$ converge également et $\left| \sum_{n=0}^{+\infty} z_n \right| \leq \sum_{n \geq 0} |z_n|$.

Application

Soit $(u_n) \in (\mathbb{C}^*)^\mathbb{N}$ telle que $u_n \xrightarrow{n \rightarrow +\infty} \ell \neq 0$. Alors $\frac{1}{u_n} \xrightarrow{n \rightarrow +\infty} \frac{1}{\ell}$.

En effet, pour tout $n \in \mathbb{N}$, $\left| \frac{1}{u_n} - \frac{1}{\ell} \right| = \frac{|u_n - \ell|}{|\ell u_n|}$. Par ailleurs, il existe $n_\ell \in \mathbb{N}$ tel que pour tout entier

$n \geq n_\ell$, $|\ell| - |u_n| \leq |u_n - \ell| \leq \frac{|\ell|}{2}$. Donc

$$0 \leq \left| \frac{1}{u_n} - \frac{1}{\ell} \right| \leq \frac{2|u_n - \ell|}{|\ell|^2} \xrightarrow{n \rightarrow +\infty} 0$$

ce qu'il fallait démontrer.

Cas d'égalité de l'inégalité triangulaire

Les points d'affixes z_1, \dots, z_n sont sur une même demi-droite d'origine O. En effet, raisonnons par récurrence en introduisant, pour tout entier $n \geq 2$, l'assertion

$$\mathcal{P}_n : \langle \forall (z_1, \dots, z_n) \in (\mathbb{C}^*)^n, \left(\left| \sum_{k=1}^n z_k \right| = \sum_{k=1}^n |z_k| \implies \forall k \in \llbracket 1; n \rrbracket, \exists \lambda_k \in \mathbb{R}^+, z_k = \lambda_k z_1 \right) \rangle$$

étant entendu que les implications réciproques sont immédiates.

→ Soient $z_1, z_2 \in \mathbb{C}^*$ tels que $|z_1 + z_2| = |z_1| + |z_2|$. En élevant l'égalité au carré, il vient que $\operatorname{Re}(z_1 \bar{z}_2) = |z_1 \bar{z}_2|$. Donc la partie imaginaire de $z_1 \bar{z}_2$ est nulle. Mieux, il existe $k \in \mathbb{R}^+$ tel que $z_1 \bar{z}_2 = k$, donc $\bar{z}_2 = \frac{k}{|z_1|^2} \bar{z}_1$ donc $z_2 = \frac{k}{|z_1|^2} z_1$. Donc \mathcal{P}_2 est vraie.

→ Soit n un entier supérieur ou égal à 2 tel que \mathcal{P}_n soit vraie.

Soit $(z_1, \dots, z_n, z_{n+1}) \in (\mathbb{C}^*)^{n+1}$ tel que $\left| \sum_{k=1}^{n+1} z_k \right| = \sum_{k=1}^{n+1} |z_k|$. Alors,

$$\left| \sum_{k=1}^{n+1} z_k \right| \leq |z_{n+1}| + \left| \sum_{k=1}^n z_k \right| \leq \sum_{k=1}^{n+1} |z_k|$$

L'égalité du majorant et du minorant assure que cet encadrement est une égalité, si bien que $\cancel{|z_{n+1}|} + \left| \sum_{k=1}^n z_k \right| = \cancel{|z_{n+1}|} + \sum_{k=1}^n |z_k|$. Or, \mathcal{P}_n est vraie, donc pour tout $k \in \llbracket 1; n \rrbracket$, il existe $\lambda_k \in \mathbb{R}^+$ tel que $z_k = \lambda_k z_1$.

Par le même raisonnement qu'à l'initialisation, l'égalité $|z_{n+1} + \sum_{k=1}^n z_k| = |z_{n+1}| + \left| \sum_{k=1}^n z_k \right|$ assure l'existence de $\lambda_{n+1} \in \mathbb{R}^+$ tel que $z_{n+1} = \lambda_{n+1} z_1$.
Donc \mathcal{P}_{n+1} est vraie.

→ Finalement, le principe de récurrence assure que le cas d'égalité est vérifié si, et seulement si, les vecteurs d'affixes z_1, \dots, z_n sont colinéaires et de même sens, donc que les points d'affixes z_1, \dots, z_n appartiennent à une même demi-droite d'origine O.

Exercice II.2.

Soit p un entier supérieur ou égal à 3. Soit $(u_n) \in \mathbb{C}^{\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$, $u_{n+p} = \frac{1}{p} \sum_{k=n}^{n+p-1} u_k$.

1. Montrer que toute racine du polynôme caractéristique de $(u_n)_{n \in \mathbb{N}}$ est simple.
2. Montrer que $(u_n)_{n \in \mathbb{N}}$ converge.

Cas d'égalité de l'inégalité triangulaire avec des sommes de séries

Soit $(z_n) \in (\mathbb{C}^*)^\mathbb{N}$ telle qu' $\sum_{n \geq 0} |z_n|$ converge. Donnons une condition nécessaire et suffisante pour que

$$\left| \sum_{n=0}^{+\infty} z_n \right| = \sum_{n=0}^{+\infty} |z_n|$$

 Montrons qu'il s'agit de la même condition que dans le cas réel *i.e.* pour tout $n \in \mathbb{N}$, il existe $\lambda_n \in \mathbb{R}^+$ tel que $z_n = \lambda_n z_0$.

C'est une condition suffisante car pour tout $N \in \mathbb{N}$, $\left| \sum_{n=0}^N z_n \right| = |z_0| \sum_{n=0}^N \lambda_n = \sum_{n=0}^N |\lambda_n z_0| = \sum_{n=0}^N |z_n|$.

Montrons qu'elle est nécessaire. Supposons qu'il existe $N \in \mathbb{N}^*$ tel que $\left| \sum_{n=0}^N z_n \right| < \sum_{n=0}^N |z_n|$.

Alors

$$\left| \sum_{n=0}^{+\infty} z_n \right| \leq \left| \sum_{n=0}^N z_n \right| + \left| \sum_{n=N+1}^{+\infty} z_n \right| < \sum_{n=0}^{+\infty} |z_n|$$

ce qui est faux. Donc pour tout $N \in \mathbb{N}$, $\left| \sum_{n=0}^N z_n \right| = \sum_{n=0}^N |z_n|$. Le cas d'égalité de l'inégalité triangulaire assure alors que tous les termes de $(z_n)_{n \in \mathbb{N}}$ sont sur une même demi-droite d'origine O.

Exercice II.3.

Soit n un entier supérieur ou égal à 2. Soit $(a_0, \dots, a_{n-1}) \in \mathbb{C}^n$, et posons $P = X^n + \sum_{k=0}^{n-1} a_k X^k$ et $\rho = \max\{|z| \mid P(z) = 0\}$.

1. Montrer que $\rho \leq 1 + \max_{k \in \llbracket 0; n-1 \rrbracket} (|a_k|)$.

2. Montrer que $\rho \leq \max \left(1, \sum_{k=0}^{n-1} |a_k| \right)$.

Application II.4.

Considérons une famille $(P_\lambda)_{\lambda \in \Omega}$ de polynômes unitaires et de même degré $n \geq 2$ définie par

$$\forall \lambda \in \Omega, \quad P_\lambda = X^n + \sum_{k=0}^{n-1} a_{k,\lambda} X^k$$

Si la famille de complexes $(a_{k,\lambda})_{k \in \llbracket 0; n-1 \rrbracket, \lambda \in \Omega}$ ainsi définie est bornée, alors les racines des P_λ forment une partie bornée du plan.

III Inégalités classiques

Théorème (Inégalité de Cauchy-Schwarz) III.1.

Soit $n \in \mathbb{N}^*$. Soient (x_1, \dots, x_n) et $(y_1, \dots, y_n) \in \mathbb{R}^n$. Alors

$$\left| \sum_{i=1}^n x_i y_i \right| \leq \sqrt{\sum_{i=1}^n x_i^2} \sqrt{\sum_{i=1}^n y_i^2}$$

 **Preuve :** Examinons la différence $\left(\sum_{i=1}^n x_i y_i \right)^2 - \left(\sum_{i=1}^n x_i^2 \right) \left(\sum_{j=1}^n y_j^2 \right)$. En développant, les termes $x_i^2 y_i^2$

se simplifient.

De la somme au carré il ne reste que les doubles produits $2x_i y_i x_j y_j$ avec $i < j$, et du produit de sommes il ne reste que les produits mixtes symétriquement regroupés $x_i^2 y_j^2 + x_j^2 y_i^2$ avec $i < j$. Ainsi,

$$\left(\sum_{i=1}^n x_i y_i \right)^2 - \left(\sum_{i=1}^n x_i^2 \right) \left(\sum_{j=1}^n y_j^2 \right) = \sum_{1 \leq i < j \leq n} (2(x_i y_j)(x_j y_i) - (x_i^2 y_j^2 + x_j^2 y_i^2)) = - \sum_{1 \leq i < j \leq n} (x_i y_j - x_j y_i)^2 \leq 0$$

Identité de Lagrange : Pour $n = 2$, on a l'identité remarquable valable dans tout anneau commutatif

$$(x_1 y_1 + x_2 y_2)^2 + (x_1 y_2 + x_2 y_1)^2 = (x_1^2 + x_2^2)(y_1^2 + y_2^2)$$

Inégalité de Cauchy-Schwarz pour les complexes : À l'aide de l'inégalité triangulaire, elle devient immédiate. Soient (z_1, \dots, z_n) et $(\omega_1, \dots, \omega_n) \in \mathbb{C}^n$. Alors

$$\left| \sum_{k=1}^n z_k \omega_k \right| \leq \sum_{k=1}^n |z_k| |\omega_k| \leq \sqrt{\sum_{k=1}^n |z_k|^2} \sqrt{\sum_{k=1}^n |\omega_k|^2}$$

Cas d'égalité de l'inégalité de Cauchy-Schwarz dans \mathbb{R}^n

Corollaire III.2.

Les propositions suivantes sont équivalentes :

- L'inégalité de Cauchy-Schwarz est une égalité.
- Tous les mineurs d'ordre 2 de la matrice $Z := \begin{pmatrix} x_1 & \dots & x_n \\ y_1 & \dots & y_n \end{pmatrix}$ sont nuls.
- $\text{rg}(Z) \leq 1$.
- (x_1, \dots, x_n) et (y_1, \dots, y_n) sont colinéaires.

L'exercice suivant nécessite des notions présentées dans un chapitre ultérieur

Exercice III.3.

Soit n un entier supérieur ou égal à 2. On considère l'espace des colonnes $\mathcal{M}_{n,1}(\mathbb{R})$ muni du produit scalaire canonique $\langle \cdot | \cdot \rangle$ et on note $\|\cdot\|$ sa norme euclidienne.

Soit $A \in \mathcal{S}_n^{++}$. Montrer que pour tout $X \in \mathcal{M}_{n,1}(\mathbb{R})$

$$\|X\|^2 \leq \sqrt{\langle AX | X \rangle} \sqrt{\langle A^{-1}X | X \rangle}$$

Exercice III.4.

Soit n un entier supérieur ou égal à 2. Notons E l'ensemble

$$\left\{ X = (x_1, \dots, x_n) \in (\mathbb{R}^+)^n \mid \sum_{i=1}^n x_i = 1 \right\}.$$

Calculer $m = \min_{X \in E} \left(\sum_{1 \leq i \neq j \leq n} x_i x_j \right)$ et $M = \max_{X \in E} \left(\sum_{1 \leq i \neq j \leq n} x_i x_j \right)$.

Inégalité de Cauchy-Schwarz pour les intégrales

Soient f et g deux fonctions continues par morceaux sur un segment réel $[a, b]$. Alors,

$$\left| \int_a^b f(t)g(t)dt \right| \leq \sqrt{\int_a^b |f(t)|^2 dt} \sqrt{\int_a^b |g(t)|^2 dt}$$

 **Preuve :** Soit $n \in \mathbb{N}^*$. Pour tout $k \in \llbracket 1; n \rrbracket$, posons $t_k = a + k \times \frac{b-a}{n}$.

Pour tout $k \in \llbracket 1; n \rrbracket$, posons $x_k = f(t_k)$ et $y_k = g(t_k)$. D'après l'inégalité de Cauchy-Schwarz,

$$\left| \frac{b-a}{n} \sum_{k=1}^n x_k y_k \right| \leq \sqrt{\frac{b-a}{n} \sum_{k=1}^n |x_k|^2} \sqrt{\frac{b-a}{n} \sum_{k=1}^n |y_k|^2}$$

En passant à la limite $n \rightarrow +\infty$, on obtient ce qu'on voulait démontrer.

Inégalité de Minkowski : $\sqrt{\sum_{i=1}^n (x_i + y_i)^2} \leq \sqrt{\sum_{i=1}^n x_i^2} + \sqrt{\sum_{i=1}^n y_i^2}$. En effet,

$$\sum_{i=1}^n (x_i + y_i)^2 = \sum_{i=1}^n x_i^2 + \sum_{i=1}^n y_i^2 + 2 \sum_{i=1}^n x_i y_i \stackrel{\text{Cauchy-Schwarz}}{\leq} \sum_{i=1}^n x_i^2 + \sum_{i=1}^n y_i^2 + 2 \sqrt{\sum_{i=1}^n x_i^2} \sqrt{\sum_{i=1}^n y_i^2} = \left(\sqrt{\sum_{i=1}^n x_i^2} + \sqrt{\sum_{i=1}^n y_i^2} \right)^2$$

et le cas d'égalité est également réalisé lorsque (x_1, \dots, x_n) et (y_1, \dots, y_n) sont colinéaires.
On a un énoncé analogue avec les intégrales de fonctions continues par morceaux.

Inégalité de réarrangement : Supposons que $x_1 \leq \dots \leq x_n$ et $y_1 \leq \dots \leq y_n$. Alors, pour toute $\sigma \in \mathfrak{S}_n$,

$$\sum_{i=1}^n x_{\sigma(i)} y_i \leq \sum_{i=1}^n x_i y_i$$

 **Preuve :** L'ensemble \mathfrak{S}_n est fini donc il existe une partie P de \mathfrak{S}_n tel que pour toute $\sigma \in P$, $\sum_{i=1}^n x_{\sigma(i)} y_i$ est maximale.

Si l'identité est dans P , il n'y a rien à démontrer. Supposons le contraire, et introduisons l'application

$$\begin{aligned} \varphi : P &\longrightarrow \llbracket 1; n \rrbracket \\ \sigma &\longmapsto \min\{j \in \llbracket 1; n \rrbracket \mid \sigma(j) \neq j\} \end{aligned}$$

puis, posons $i = \max(\varphi)$, et notons σ une permutation de P où ce maximum est atteint. Enfin, posons $k = \sigma^{-1}(i)$. Par construction $\sigma(i) > i$ et $k > i$. Alors, $(x_{\sigma(i)} - x_i)(y_k - y_i) \geq 0$, donc, en développant

$$x_i y_k + x_{\sigma(i)} y_i \leq x_{\sigma(i)} y_k + x_i y_i$$

Considérons la permutation $\tilde{\sigma} = \tau_{\sigma(k), \sigma(i)} \circ \sigma$. L'inégalité se réécrit à l'aide de $\tilde{\sigma}$:

$$x_{\sigma(k)}y_k + x_{\sigma(i)}y_i \leq x_{\tilde{\sigma}(k)}y_k + x_{\tilde{\sigma}(i)}y_i$$

et, étant donné que σ et $\tilde{\sigma}$ coïncident en tout point de $\llbracket 1; n \rrbracket$ distinct de i et de k , alors

$$\sum_{i=1}^n x_{\sigma(i)}y_j \leq \sum_{i=1}^n x_{\tilde{\sigma}(i)}y_j$$

Donc $\tilde{\sigma} \in P$. Mais, par construction, $\varphi(\tilde{\sigma}) > i = \max(\varphi)$ ce qui est faux. Donc l'identité est dans P , ce qu'il fallait démontrer.

IV Étude de fonctions

1. Fonctions homographiques

Soient $c \neq 0$, et $a, b, c \in \mathbb{R}$ tels que $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$. La fonction f définie par

$$\forall x \in \mathbb{R} \setminus \left\{ \frac{c}{d} \right\}, \quad f(x) = \frac{ax + b}{cx + d}$$

est une fonction homographique. Elle est strictement monotone car sa dérivée est de signe constant :

$$\forall x \in \mathbb{R} \setminus \left\{ \frac{c}{d} \right\}, \quad f'(x) = \frac{ad - bc}{(cx + d)^2}$$

2. Accroissements finis

Théorème (Théorème des accroissements finis) IV.1.

Soient a et $b \in \mathbb{R}$ tels que $a < b$. Soit $f \in \mathcal{C}([a, b], \mathbb{C})$, telle que f soit dérivable sur $]a, b[$. Si $f([a, b]) \subset \mathbb{R}$, alors il existe $c \in]a, b[$ tel que $f(b) - f(a) = f'(c)(b - a)$.

 **Contre-exemple dans \mathbb{C} :** Un tel c n'existe pas si $a = 0$, $b = 2\pi$, et si on choisit f telle que pour tout $x \in [0, 2\pi]$, $f(x) = e^{ix}$.

Théorème (Inégalité des accroissements finis) IV.2.

Soient a et $b \in \mathbb{R}$ tels que $a < b$. Soit $f \in \mathcal{C}([a, b], \mathbb{C})$, telle que f soit dérivable sur $]a, b[$. Si $|f'|$ est bornée par $M \geq 0$, alors

$$|f(b) - f(a)| \leq M(b - a)$$

Si de plus, f' est continue sur $[a, b]$, on a l'égalité $f(b) - f(a) = \int_a^b f'(t)dt$ donc

$$|f(b) - f(a)| \leq \int_a^b |f'(t)| dt \leq \|f'\|_{\infty, [a, b]} (b - a)$$

Remarque : Il est ais  de d montrer que $\left| \int_a^b f(t)dt \right| \leq \int_a^b |f(t)| dt$   partir de l'in galit  analogue r elle.

En effet, il existe $\theta \in \mathbb{R}$ tel que $\int_a^b f(t)dt = \left| \int_a^b f(t)dt \right| e^{i\theta}$.

Donc $\int_a^b e^{-i\theta} f(t)dt = \left| \int_a^b f(t)dt \right| = \left| \int_a^b e^{-i\theta} f(t)dt \right|$. Puis, en introduisant les fonctions r elles u et v telles que $u + iv = e^{-i\theta} f$, il vient

$$\int_a^b u(t)dt + i \int_a^b v(t)dt = \left| \int_a^b f(t)dt \right|$$

Donc $\int_a^b v(t)dt = 0$. Ainsi

$$\left| \int_a^b f(t)dt \right| \leq \left| \int_a^b u(t)dt \right| \leq \int_a^b |u(t)| dt \leq \int_a^b |e^{-i\theta} f(t)| dt = \int_a^b |f(t)| dt$$

3. Puissances

Exemple

Soit $(a_n) \in (\mathbb{R}^+)^{\mathbb{N}}$. Soit $r \in]0, 1[$ tel que $\sum_{n \geq 0} a_n^r$ converge. Montrons que $\sum_{n \geq 0} a_n$ converge.

Il suffit de remarquer qu'il existe $n_1 \in \mathbb{N}$ tel que pour tout entier $n \geq n_1$, $0 \leq a_n \leq a_n^r < 1$, car $a_n^r \xrightarrow[n \rightarrow +\infty]{} 0$. D'o  la convergence de $\sum_{n \geq 0} a_n$.

 Clairement, cet exemple sert   rappeler que $q \leq q^r$ si $q \in [0, 1]$.

Lemme IV.3.

Soit $r \in]0, 1[$. Alors, pour tous $x, y \in \mathbb{R}^+$,

$$(x + y)^r \leq x^r + y^r$$



Preuve : Sans perte de g nalit , soient $x > 0$ et $y > 0$. Consid rons la fonction φ d finie par

$$\forall t > 0, \varphi(t) = t^r + 1 - (1 + t)^r$$

φ est d rivable sur \mathbb{R}^{+*} et pour tout $t > 0$, $\varphi'(t) = r(t^{r-1} - (1 + t)^{r-1}) \geq 0$, donc φ est croissante.

Or $\varphi(0) = 0$ donc $\varphi\left(\frac{y}{x}\right) \geq 0$, ce qu'il fallait d montrer.

 **Exercice similaire :** On montre pareillement que si $r \geq 1$, pour tous $x, y \geq 0$, $(x + y)^r \geq x^r + y^r$.

4. Trigonom trie

Applications

- Une r currence et une formule d'addition permettent de montrer que pour tout $n \in \mathbb{N}^*$ et pour tout $x \in \mathbb{R}$, $|\sin(nx)| \leq n |\sin(x)|$.
- L'exploitation de la concavit  de la fonction sinus sur $\left[0, \frac{\pi}{2}\right]$ permet de montrer que pour tout $x \in \left[0, \frac{\pi}{2}\right]$, $\sin(x) \geq \frac{2}{\pi}x$.

3. Un calcul ais  permet de montrer que pour tout $x \in \mathbb{R} \setminus 2\pi\mathbb{Z}$, et pour tout $n \in \mathbb{N}^*$,

$$\left| \sum_{k=0}^n e^{ikx} \right| \leq \frac{1}{\left| \sin \left(\frac{x}{2} \right) \right|}$$

En effet, si $x \in \mathbb{R} \setminus 2\pi\mathbb{Z}$, et $n \in \mathbb{N}^*$

$$\begin{aligned} S_n(x) &:= \sum_{k=0}^n e^{ikx} = \frac{e^{i(n+1)x} - 1}{e^{ix} - 1} \\ &= \frac{e^{i(n+1)x/2}(e^{i(n+1)x/2} - e^{-i(n+1)x/2})}{e^{ix/2}(e^{ix/2} - e^{-ix/2})} \\ &= e^{inx/2} \times \frac{\sin \left(\frac{(n+1)x}{2} \right)}{\sin \left(\frac{x}{2} \right)} \end{aligned}$$

d'o  le r sultat. On dit alors que $(S_n)_{n \in \mathbb{N}^*}$ est uniform ment born e  en n   x fix .

Correction de l'exercice II.2. :

1. Le polynôme caractéristique de $(u_n)_{n \in \mathbb{N}}$ est

$$P = X^p - \frac{1}{p} \sum_{k=0}^{p-1} X^k = X^p - \frac{1}{p} \frac{X^p - 1}{X - 1} = \frac{\overbrace{pX^{p+1} - (p+1)X^p + 1}^{\text{noté } Q}}{p(X-1)}$$

et $Q' = p(p+1)X^{p-1}(X-1)$. 1 est une racine simple de P car c'est une racine double de Q . Par ailleurs, toute racine de P distincte de 1 est une racine de Q avec la même multiplicité dans les deux polynômes. Or 0 n'est pas racine de P , donc toute racine de P distincte de 1 est simple. Donc toute racine de P est simple.

2. Soit z une racine de P . Supposons que $|z| > 1$. Alors, pour tout entier naturel $k < p$, $|z|^p > |z|^k$,

$$\text{donc } p|z|^p > \sum_{k=0}^{p-1} |z|^k \geq \left| \sum_{k=0}^{p-1} z^k \right| = p|z|^p \text{ ce qui est faux.}$$

↑ inégalité triangulaire

Donc $|z| \leq 1$. Si $z \in \mathbb{U}$, $p|z|^p = \sum_{k=0}^{p-1} |z|^k$. Le cas d'égalité de l'inégalité triangulaire assure alors que pour tout $k \in \llbracket 1; p \rrbracket$, z^k appartient à la demi-droite réelle positive. Donc $z = 1$.

Les $p-1$ autres racines de P sont de modules strictement inférieurs à 1. Or, $(u_n)_{n \in \mathbb{N}}$ est une combinaison linéaire de suites géométriques dont les raisons sont les racines de P , et ces suites sont convergentes. Donc $(u_n)_{n \in \mathbb{N}}$ converge.

Correction de l'exercice II.3. :

1. Soit z une racine de P tel que $\rho = |z|$. Alors $z^n = -\sum_{k=0}^{n-1} a_k z^k$, donc

$$\rho^n = \left| \sum_{k=0}^{n-1} a_k z^k \right| \leq \sum_{k=0}^{n-1} |a_k| \rho^k \leq \underbrace{\max_{k \in \llbracket 0; n-1 \rrbracket} (|a_k|)}_{\text{noté } M} \sum_{k=0}^{n-1} \rho^k$$

↑ inégalité triangulaire

Si $\rho \leq 1$ alors, l'inégalité à démontrer est vraie. Sinon,

$$\rho^\alpha \leq M \times \frac{\rho^n - 1}{\rho - 1} \leq \frac{M \rho^\alpha}{\rho - 1}$$

donc $\rho \leq 1 + M$.

2. D'après le calcul de la question précédente,

$$\rho^n \leq \sum_{k=0}^{n-1} |a_k| \rho^k$$

→ Si $\rho \leq 1$, il n'y a rien à démontrer.

→ Si $\rho > 1$, alors $\rho \leq \sum_{k=0}^{n-1} \frac{|a_k|}{\rho^{n-1-k}} \leq \sum_{k=0}^{n-1} |a_k|$.

Correction de l'exercice III.3. :

Soit $X \in \mathcal{M}_{n,1}(\mathbb{R})$. Pour toute matrice diagonale $D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} \in \mathcal{M}_n(\mathbb{R}^{+*})$, et pour tout $U =$

$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{R})$ on a

$$\|U\|^2 = \sum_{i=1}^n u_i^2 = \sum_{i=1}^n \left| \sqrt{d_i} u_i \times \frac{u_i}{\sqrt{d_i}} \right| \leq \underbrace{\sqrt{\sum_{i=1}^n d_i u_i^2}}_{\substack{\text{Cauchy-Schwarz} \\ \uparrow}} \underbrace{\sqrt{\sum_{i=1}^n \frac{u_i^2}{d_i}}}_{\sqrt{\langle D^{-1} U | U \rangle}}$$

Or A est une matrice symétrique réelle définie positive, donc il existe $P \in \mathcal{O}_n(\mathbb{R})$ tel que $\underbrace{P^\top A P}_{\text{notée } \Delta}$ soit une matrice diagonale à coefficients diagonaux strictement positifs.

Donc

$$\|X\|^2 = \|P^\top X\|^2 \leq \sqrt{\langle \Delta P^\top X | P^\top X \rangle} \sqrt{\langle \Delta^{-1} P^\top X | P^\top X \rangle} = \sqrt{\langle P \Delta P^\top X | X \rangle} \sqrt{\langle P \Delta^{-1} P^\top X | X \rangle}$$

ce qu'il fallait démontrer.

Correction de l'exercice III.4. :

Pour tout $X \in E$, $\sum_{1 \leq i \neq j \leq n} x_i x_j \geq 0$. Or $(\underbrace{0, \dots, 0}_{n-1 \text{ zéros}}, 1) \in E$ et réalise ce minorant, donc $m = 0$. Soit $X \in E$.

$$\sum_{1 \leq i \neq j \leq n} x_i x_j = \left(\sum_{i=1}^n x_i \right)^2 - \sum_{i=1}^n x_i^2 = 1 - \sum_{i=1}^n x_i^2.$$

Or, par l'inégalité de Cauchy-Schwarz, $n \sum_{i=1}^n x_i^2 \geq \left(\sum_{i=1}^n x_i \right)^2 = 1$.

Donc, pour tout $X \in E$,

$$\sum_{1 \leq i \neq j \leq n} x_i x_j \leq 1 - \frac{1}{n} = \frac{n-1}{n}$$

Ce majorant est atteint en $\left(\frac{1}{n}, \dots, \frac{1}{n} \right) \in E$. En effet, $\sum_{1 \leq i \neq j \leq n} \frac{1}{n^2} = \frac{2}{n^2} \binom{n}{2} = \frac{n-1}{n}$, donc

$$M = \frac{n-1}{n}$$

 Le nombre de couples (i, j) de $\llbracket 1; n \rrbracket^2$ tel que $i \neq j$ est le double du nombre de couples (i, j) de $\llbracket 1; n \rrbracket^2$ tel que $i < j$, qui vaut le nombre d'issues possibles lors du choix simultané de 2 éléments distincts d'un ensemble à n éléments, et ce nombre de combinaisons vaut $\binom{n}{2}$.



CHAPITRE 3

Cardinaux

I Généralités

Définition I.1.

Soient E et F deux ensembles. On dit que E et F ont même cardinal ou sont équivalents lorsqu'il existe une application $f : E \rightarrow F$ qui soit bijective.



Remarquons que la relation introduite ci-dessus définit une relation d'équivalence.

Exercice I.2.

Soit E un ensemble. Montrer que E et $\mathcal{P}(E)$ ne sont pas équivalents.

1. Cardinaux finis et infinis

Définition I.3.

Un ensemble E est dit fini s'il existe $n \in \mathbb{N}$ tel que E est équivalent à $[0; n]$. Le cardinal de E est alors $n + 1$.

Dans ce cas, on note $|E| = n + 1$.

Convention : On convient que l'ensemble vide est fini et que $|\emptyset| = 0$.

Proposition I.4.

Soient E et F deux ensembles finis et f une application de E dans F . Si E et F sont équivalents et $f : E \rightarrow F$ est surjective ou injective, alors elle est bijective.

Définition I.5.

On dit qu'un ensemble est infini lorsqu'il n'est pas fini.

Exercice I.6.

Soit E un ensemble.

1. Montrer que si E est infini, alors il existe une application $f : \mathbb{N} \rightarrow E$ qui soit injective.
2. Montrer que E est infini si, et seulement si, il existe une application $f : E \rightarrow E$ qui soit injective mais non surjective.

II Ensembles dénombrables

Définition II.1.

Soit E un ensemble. On dit que E est dénombrable lorsqu'il est fini ou s'il existe une bijection f de \mathbb{N} dans E .

Remarque 1 : Dans la littérature, il existe deux définitions de la dénombrabilité. L'une d'entre elles est celle ci-dessus, l'autre se réduit uniquement à l'existence d'une bijection avec \mathbb{N} .

Remarque 2 : Si E et F sont deux ensembles équivalents, alors E est dénombrable si, et seulement si, F l'est.

Exemples :

→ \mathbb{N}^* est dénombrable. En effet, il suffit de considérer la bijection $f : x \mapsto x + 1$ de \mathbb{N} dans \mathbb{N}^* .

→ \mathbb{Z} est dénombrable. En effet, il suffit de considérer la bijection $f : x \mapsto \begin{cases} 2|x| - 1 & \text{si } x < 0 \\ 2x & \text{sinon} \end{cases}$ de \mathbb{Z} dans \mathbb{N} .

Remarque : Plutôt que de retenir cette bijection à l'aide de sa formule explicite, il est loisible de retenir comment elle est construite. Trouver une bijection entre un ensemble et \mathbb{N} , c'est trouver comment énumérer ses éléments. Pour énumérer les éléments de \mathbb{Z} , il suffit de poser que 0 est le 0-ième élément, 1 est le premier élément, -1 est le deuxième élément, 2 est le troisième élément et ainsi de suite : il s'agit d'énumérer tour à tour les entiers positifs et les entiers négatifs.

Proposition II.2.

Soit E et F deux ensembles.

1. Toute partie de \mathbb{N} est dénombrable.
2. S'il existe une application $f : E \rightarrow F$ qui soit injective et si F est dénombrable, alors E est dénombrable.
3. S'il existe une application $f : F \rightarrow E$ qui soit surjective et si F est dénombrable, alors E est dénombrable.
4. $\mathbb{N} \times \mathbb{N}$ est dénombrable.
5. Le produit cartésien de deux ensembles dénombrables est dénombrable.
6. \mathbb{Q} est dénombrable.
7. Soit I un ensemble dénombrable. Soit $(E_i)_{i \in I}$ une famille d'ensembles dénombrables.
Alors $\bigcup_{i \in I} E_i$ est dénombrable.

Preuves

1. Soit A une partie de \mathbb{N} . Si A est fini, il n'y a rien à prouver. On suppose donc que A est infini. Nous allons définir récursivement une bijection de \mathbb{N} dans A .
 - **Initialisation** : on pose $f(0) = \min A$.
 - **Hérédité** : Soit $n \in \mathbb{N}$, supposons que $f(0), f(1), \dots, f(n)$ soient correctement définis. On pose alors $f(n+1) = \min A \setminus \{f(0), \dots, f(n)\}$.

Montrons que f ainsi définie est bien une bijection de \mathbb{N} dans A .

- **Injectivité**
si $m > n$, alors m est le minimum d'un ensemble qui ne contient pas $f(n)$, donc $f(n) \neq f(m)$.
- **Surjectivité**
Pour montrer la surjectivité de f , on suppose par l'absurde qu'il existe un élément $a \in A$ qui

n'est pas atteint par f , i.e. $a \notin f(\mathbb{N})$. On a alors pour tout $n \in \mathbb{N}$, $a \in A \setminus \{f(0), \dots, f(n)\}$, donc

$$a > \min A \setminus \{f(0), \dots, f(n)\} = f(n+1)$$

ce qui est absurde, car la quantité $\min A \setminus \{f(0), \dots, f(n)\}$ peut être arbitrairement grande pour n assez grand.

Le lecteur pourra vérifier que f est croissante pour s'exercer.

2. Si F est fini, alors E aussi. Si F est infini, alors il est en bijection avec \mathbb{N} . Soit ϕ une bijection de F dans \mathbb{N} . $\phi \circ f : E \rightarrow \mathbb{N}$ est injective, donc en posant $A = \phi \circ f(E)$, l'application $\phi \circ f : E \rightarrow A$ est bijective. Or A est inclus dans F et F est dénombrable, donc A l'est et finalement E aussi puisqu'ils sont en bijection.
3. f étant surjective, on peut affirmer que pour tout $x \in E$, $f^{-1}(\{x\})$ est non vide et donc écrire F sous forme de l'union d'ensembles disjoints suivante $F = \bigcup_{x \in E} f^{-1}(\{x\})$. On définit une application $S : E \rightarrow F$ de la manière suivante : pour tout $x \in E$, $S(x) \in f^{-1}(\{x\})$ (on choisit un élément quelconque de $f^{-1}(\{x\})$, ce qui est possible car cet ensemble est non vide). Les ensembles $(f^{-1}(\{x\}))_{x \in E}$ étant disjoints, on a pour tous $x, y \in E$, si $x \neq y$ alors $S(x) \neq S(y)$. Donc $S : E \rightarrow F$ est injective. Il suffit alors d'appliquer le point (2).
4. On considère l'application de $\mathbb{N} \times \mathbb{N}$ dans \mathbb{N} $f : (m, n) \mapsto 2^m(2n+1)$. Montrons qu'elle est injective. Soit $m, n, m', n' \in \mathbb{N}$. On suppose sans perte de généralité que $m \geq m'$. Si $f(m, n) = f(m', n')$, alors on a $2^{m-m'}(2n+1) = (2n'+1)$. $2^{m-m'}$ divise un nombre impair, donc nécessairement $m = m'$ et par conséquent $n = n'$. Donc f est injective. On peut alors appliquer le point (2).

5. **Lemme :** E est dénombrable si et seulement si existe une surjection de \mathbb{N} dans E . Appliquons ce lemme. Soit E et F dénombrables, alors il existe deux applications $s_E : \mathbb{N} \rightarrow E$ et $s_F : \mathbb{N} \rightarrow F$ surjectives. On considère alors l'application

$$s : \begin{cases} \mathbb{N} \times \mathbb{N} & \longrightarrow E \times F \\ (m, n) & \mapsto (s_E(m), s_F(n)) \end{cases}$$

Cette application est surjective et $\mathbb{N} \times \mathbb{N}$ est dénombrable, on peut donc appliquer le point (3).

6. Il suffit de considérer l'application

$$f : \begin{cases} \mathbb{Z} \times \mathbb{N}^* & \rightarrow \mathbb{Q} \\ (p, q) & \mapsto \frac{p}{q} \end{cases}$$

Cette application est surjective et $\mathbb{Z} \times \mathbb{N}^*$ est dénombrable d'après le point (5), donc \mathbb{Q} est dénombrable d'après le point (3).

7. On pose $A = \bigcup_{i \in I} E_i$. Pour tout $i \in I$ E_i est dénombrable, donc on peut considérer une surjection $s_i : \mathbb{N} \rightarrow E_i$. On considère donc l'application

$$s : \begin{cases} I \times \mathbb{N} & \rightarrow A \\ (i, n) & \mapsto s_i(n) \end{cases}$$

cette application est une surjection et $I \times \mathbb{N}$ est dénombrable, on peut alors appliquer le point (3).

III Exercices

Exercice III.1.

Soit $n \in \mathbb{N}^*$ et $X \subset [1; 2n]$. On suppose que $|X| \geq n + 1$. Montrer qu'il existe $a, b \in X$ tels que $a \neq b$ et $a|b$.

Exercice III.2.

Montrer que \mathbb{R} n'est pas dénombrable.

Exercice III.3.

Soit Λ un ensemble. Soit $(I_\lambda)_{\lambda \in \Lambda}$ une famille d'intervalles ouverts non vides de \mathbb{R} . Montrer que si les intervalles $(I_\lambda)_{\lambda \in \Lambda}$ sont deux à deux disjoints, alors Λ est dénombrable.

Exercice III.4.

On dit qu'une partie Ω de \mathbb{R} est ouverte au sens topologique lorsque pour tout $x \in \Omega$, il existe $\varepsilon > 0$ tel que $]x - \varepsilon, x + \varepsilon[\subset \Omega$. Montrer qu'un intervalle est ouvert au sens topologique si et seulement si il est ouvert au sens de l'ordre.

Exercice III.5.

Soit $f \in \mathcal{C}(\mathbb{R}, \mathbb{R})$. Montrer que $A = \{x \in \mathbb{R}, f(x) \neq 0\}$ est ouvert.

Exercice III.6.

Soit Ω un ouvert non vide de \mathbb{R} . Montrer que Ω est réunion dénombrable d'intervalles ouverts deux à deux disjoints.

Exercice III.7.

Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ monotone et Δ_f l'ensemble des points de discontinuité de f . Montrer que Δ_f est dénombrable.

Exercice III.8.

Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ convexe. Montrer que $A = \{a \in \mathbb{R}, f \text{ n'est pas dérivable en } a\}$ est dénombrable.

Exercice III.9.

On dit que $\alpha \in \mathbb{C}$ est algébrique s'il existe $P \in \mathbb{Q}[X] \setminus \{0\}$ tel que $P(\alpha) = 0$. Montrer que l'ensemble des nombres algébriques est dénombrable.

Remarque : la définition ci dessus du fait que α soit algébrique est équivalente à $\exists P \in \mathbb{Z}[X] \setminus \{0\} P(\alpha) = 0$.

Correction de l'exercice I.2. :

Supposons qu'il existe une application surjective $S : E \rightarrow \mathcal{P}(E)$. On pose $A = \{x \in E, x \notin S(x)\}$. Si A admet un antécédant a par S , alors si $a \in S(a)$, $a \notin A = S(a)$ ce qui est absurde. De même, si $a \notin S(a)$, alors $a \in A = S(a)$ ce qui est encore absurde. Il n'existe pas de surjection de E dans $\mathcal{P}(E)$, ils ne sont donc pas équivalents.

Correction de l'exercice I.6. :

1. Nous allons construire $f : \mathbb{N} \rightarrow E$ récursivement.

- **Initialisation :** E est infini donc non vide. On peut donc choisir $a_0 \in E$ et on pose $f(0) = a_0$.
- **Héritéité :** Soit $n \in \mathbb{N}$. Supposons que $f(0), \dots, f(n)$ sont correctement définis. $A_n = E \setminus \{f(0), \dots, f(n)\}$ est non vide car E est infini, on peut donc choisir $a_{n+1} \in A_n$ et on pose $f(n+1) = a_{n+1}$.

L'application f définie ci dessus est injective. En effet, si $m > n$, alors $f(m) \in E \setminus \{f(0), \dots, f(m-1)\}$ ce qui donne que $f(m) \neq f(n)$.

2. → (\Leftarrow) Soit $f : E \rightarrow E$ injective mais non sujective. E est fini équivalent à lui même, donc la proposition I.4 nous permet d'affirmer que f est bijective donc surjective, ce qui est absurde.
- (\Rightarrow) Supposons que E est infini. D'après la question précédente, on dispose d'une injection $i : \mathbb{N} \rightarrow E$. On définit

$$f : \begin{cases} E & \longrightarrow E \\ x & \longmapsto \begin{cases} x & \text{si } x \in E \setminus i(\mathbb{N}) \\ i(n+1) & \text{si } x = i(n) \text{ avec } n \in \mathbb{N} \end{cases} \end{cases}$$

Montrons que f est injective et non surjective.

Soit $(x, y) \in E^2$ tel que $f(x) = f(y)$.

- Si $x \in i(\mathbb{N})$, alors y aussi, car sinon on disposerait d'un entier $n \in \mathbb{N}$ tel que $f(x) = i(n)$, et donc $f(y) = y = f(x) = i(n) \in i(\mathbb{N})$ ce qui est absurde. On dispose alors de $a, b \in \mathbb{N}$ tels que $f(x) = i(a+1)$, $f(y) = i(b+1)$, $x = i(a)$ et $x = i(b)$. On a alors $i(a+1) = i(b+1)$. Par injectivité de i , on a $a = b$ et donc $i(a) = i(b)$ et finalement $x = y$.
- Si $x \notin i(\mathbb{N})$, alors y aussi, sinon on disposerait d'un $n \in \mathbb{N}$ tel que $f(y) = i(n+1)$ et donc $f(x) = x = f(y) = i(n+1) \in i(\mathbb{N})$ ce qui est absurde. L'égalité $f(x) = f(y)$ devient donc $x = y$. D'où l'injectivité de f .

En ce qui concerne la non-surjectivité, il suffit de remarquer que $i(0)$ n'admet pas d'antécédant. En effet, s'il existe $x \in E$ tel que $f(x) = i(0)$, alors nécessairement on dispose d'un entier $n \in \mathbb{N}$ tel que $x = i(n)$, et donc on a $i(n+1) = i(0)$. Ceci nous donne que $n = -1$ ce qui est absurde.

Correction de l'exercice III.1. :

Pour tout $x \in X$, on écrit $x = 2^{k(x)}(2l(x)+1)$. Les nombres de la forme $2l(x)+1$ sont tous dans $\llbracket 1; 2n \rrbracket$ et il y en au plus n . Par le lemme des tiroirs (car $|X| \geq n+1 > n$), il existe donc $a \neq b$ éléments de X tels que $2l(a)+1 = 2l(b)+1$. En supposant sans perte de généralité que $k(a) \geq k(b)$, on obtient que $a = 2^{k(a)-k(b)}b$, donc $b|a$.

Correction de l'exercice III.2. :

On va montrer que $[0, 1[$ n'est pas dénombrable. On suppose par l'absurde qu'on dispose d'une énumération dénombrable de $[0, 1[$, i.e. il existe une suite injective $(x_n)_{n \in \mathbb{N}}$ telle que $[0, 1[= \{x_n\}_{n \in \mathbb{N}}$.

On pose pour tout $n \in \mathbb{N}$ l'écriture décimale propre de x_n comme $x_n = 0, x_{1,n}x_{2,n}x_{3,n}\dots$. On construit alors une suite $(y_q)_{q \in \mathbb{N}^*} \in \{1, \dots, 8\}^{\mathbb{N}^*}$ telle que pour tout $q \in \mathbb{N}^*$, $y_q \neq x_{q,q}$. On pose $y = 0, y_1y_2y_3\dots$

Par hypothèse, il existe $n_0 \in \mathbb{N}^*$ tel que $y = x_{n_0}$. L'écriture de y_{n_0} étant également propre, on a que $y_{n_0} = x_{n_0, n_0}$ ce qui est absurde.

Correction de l'exercice III.3. :

Pour tout $\lambda \in \Lambda$, il existe $r_\lambda \in I_\lambda \cap \mathbb{Q}$. Pour tous $\lambda, \lambda' \in \Lambda$, si $\lambda \neq \lambda'$, par hypothèse $I_\lambda \cap I_{\lambda'} = \emptyset$ donc $r_\lambda \neq r_{\lambda'}$. L'application $\lambda \mapsto r_\lambda$ est une injection de Λ dans \mathbb{Q} , donc d'après la propriété 2 de la proposition II.2, Λ est dénombrable.

Correction de l'exercice III.4. :

- (\Leftarrow) On pose $\Omega =]a, b[$ avec $a < b$. Soit $x \in \Omega$. On pose $\varepsilon = \frac{1}{2} \min(x - a, b - x)$. On a alors $]x - \varepsilon, x + \varepsilon[\subset \Omega$. Donc Ω est ouvert au sens topologique.
- (\Rightarrow) Soit I un intervalle non vide dont les bornes sont $a, b \in \mathbb{R}$ tel que $a < b$. Supposons que I est ouvert au sens topologique. Pour tout $\varepsilon > 0$ $]a - \varepsilon, a + \varepsilon[\not\subset I$. De même, $]b - \varepsilon, b + \varepsilon[\not\subset I$. On a alors par hypothèse $a, b \notin I$. I est donc ouvert au sens de l'ordre. Le cas des bornes infinies est laissé comme exercice au lecteur.

Correction de l'exercice III.5. :

Soit $x_0 \in \mathbb{R}$ tel que $f(x_0) \neq 0$. On suppose sans perte de généralité que $f(x_0) > 0$. Par continuité de f , il existe $\eta > 0$ tel que pour tout $x \in]x_0 - \eta, x_0 + \eta[$

$$|f(x) - f(x_0)| < \frac{1}{2}f(x_0)$$

Ceci implique que pour tout $x \in]x_0 - \eta, x_0 + \eta[$

$$f(x) > \frac{f(x_0)}{2} > 0$$

On en déduit que pour tout $x_0 \in A$, il existe $\eta > 0$ tel que $]x_0 - \eta, x_0 + \eta[\subset A$. Donc A est ouvert.

Correction de l'exercice III.6. :

Uniquement pour cet exercice, pour tout $x, y \in \Omega$, on utilise l'abus de notation suivant

$$[x, y] = [y, x] = [\min(x, y), \max(y, x)]$$

On introduit la relation d'équivalence \sim sur Ω définie par

$$x \sim y \iff [x, y] \subset \Omega$$

Le lecteur pourra vérifier par lui-même qu'il s'agit bien d'une relation d'équivalence.

Soit I une classe d'équivalence selon \sim . Si $x, y \in I$, alors pour tout $z \in [x, y]$, $[x, z] \subset [x, y] \subset \Omega$, donc alors $[x, y] \subset I$. I est donc convexe, et par conséquent c'est un intervalle.

Montrons que I est ouvert. Soit $x \in I$. Ω étant ouvert, il existe $\varepsilon > 0$ tel que $]x - \varepsilon, x + \varepsilon[\subset \Omega$. Donc pour tout $y \in]x - \varepsilon, x + \varepsilon[$, $[x, y] \subset \Omega$ et par conséquent $y \in I$. I est alors ouvert.

Conclusion : Ω est réunion disjointe de classes d'équivalences selon \sim qui sont toutes des intervalles ouverts. D'après l'exercice III.3, cette réunion est dénombrable.

Correction de l'exercice III.7. :

Pour tout $x \in \mathbb{R}$, on note $f(x^+)$ et $f(x^-)$ respectivement la limite à droite et à gauche de f en x . Supposons sans perte de généralité que f est croissante. Soit $a \in \mathbb{R}$. On sait que $f(a^-) \leq f(a) \leq f(a^+)$. Ainsi, pour tout $a \in \Delta_f$, $f(a^-) < f(a^+)$. Posons pour tout $a \in \Delta_f$, $I_a =]f(a^-), f(a^+)[]$. Soit $b \in \Delta_f$ différent de a . Si $a < b$, alors $f(a^+) \leq f(b^-)$. De même si $a > b$, alors $f(a^-) \geq f(b^+)$. Les intervalles $(I_a)_{a \in \Delta_f}$ sont ouverts, non vides et disjoints. D'après l'exercice III.3, on déduit que Δ_f est dénombrable.

Correction de l'exercice III.8. :

Soit $a \in A$. On pose $I_a =]f'_g(a), f'_d(a)[$. On pose pour tous $x \neq y$, $p_x(y) = \frac{f(x)-f(y)}{x-y}$. Si $a, b \in A$ avec $a < b$, alors pour tout $x \in]a, b[$ (voir chapitre précédent sur les fonctions convexes)

$$f'_d(a) \leq p_a(x) = p_x(a) \leq p_x(b) = p_b(x) \leq f'_g(b)$$

et alors $I_a \cap I_b = \emptyset$ et pour tout $x \in A$, I_a est non vide. Il suffit donc d'appliquer l'exercice III.3.

Correction de l'exercice III.9. :

On note $\overline{\mathbb{Q}}$ l'ensemble des nombres algébriques. On pose pour tout $n \in N$,

$$H_n = \{P(X) = \sum_{k=0}^d a_k X^k \in \mathbb{Z}[X], \text{ } d \leq n \text{ et } \forall k \in \llbracket 1; d \rrbracket, |a_k| \leq n\}$$

Un simple raisonnement combinatoire permet d'affirmer que pour tout $n \in \mathbb{N}$, $|H_n| \leq (2n+1)^{n+1}$. H_n est donc fini pour tout n . Or pour tout $P \in \mathbb{Z}[X]$, pour n assez grand $P \in H_n$. Donc $\mathbb{Z}[X] = \bigcup_{n \in \mathbb{N}} H_n$. $\mathbb{Z}[X]$ est union d'ensembles finis, donc d'après la propriété 7 de la proposition II.2, $\mathbb{Z}[X]$ est dénombrable. Enfin, on écrit $\overline{\mathbb{Q}} = \bigcup_{P \in \mathbb{Z}[X] \setminus \{0\}} Z(P)$ (avec pour tout P , $Z(P)$ l'ensemble des zéros de P). $\overline{\mathbb{Q}}$ est donc réunion dénombrable d'ensembles finis donc d'après la proposition 7 de la propriété II.2, $\overline{\mathbb{Q}}$ est dénombrable.



CHAPITRE 11.1

Espaces vectoriels normés et espaces métriques

I Espaces vectoriels normés

Dans toute cette partie, on considère \mathbb{K} un corps égal à \mathbb{R} ou \mathbb{C} et E un \mathbb{K} -espace vectoriel.

Définition I.1.

Une norme sur E est une application $N : E \rightarrow \mathbb{R}^+$ vérifiant les trois conditions suivantes.

- (N_1) $\forall x \in E, N(x) = 0 \iff x = 0$ (séparation)
- (N_2) $\forall (\lambda, x) \in \mathbb{K} \times E, N(\lambda x) = |\lambda| N(x)$ (homogénéité)
- (N_3) $\forall (x, y) \in E^2, N(x + y) \leq N(x) + N(y)$ (sous-additivité)

Vocabulaire : une application $N : E \rightarrow \mathbb{R}^+$ vérifiant (2) et (3) est appelée semi-norme.

Proposition I.2.

1. Si $x \neq 0, N(x) > 0$ et $N\left(\frac{x}{N(x)}\right) = 1$
2. Si $\mathbb{K} = \mathbb{R}$ et $x \neq 0$, alors pour tout $\lambda \in \mathbb{K}$,

$$N(\lambda x) = 1 \iff |\lambda| = \frac{1}{N(x)} \iff \lambda \in \left\{-\frac{1}{N(x)}, \frac{1}{N(x)}\right\}$$

L'espace $\mathbb{R}x$ contient donc deux vecteurs unitaires.

3. Pour tout $x \in E, N(x) = 1 \implies \forall \theta \in \mathbb{R}, N(e^{i\theta}x) = 1$
4. $\forall (x_1, \dots, x_n) \in E^n, N\left(\sum_{i=1}^n x_i\right) \leq \sum_{i=1}^n N(x_i)$

Exemples : voici quelques normes usuelles pour $E = \mathbb{K}^n$. On pose pour tout $x \in E, x = (x_1, \dots, x_n)$.

$$\rightarrow \|x\|_\infty = \sup_{1 \leq k \leq n} |x_k|$$

$$\rightarrow \|x\|_1 = \sum_{k=1}^n |x_k|$$

$$\rightarrow \|x\|_2 = \left(\sum_{k=1}^n |x_k|^2 \right)^{\frac{1}{2}}$$

$$\rightarrow \text{Pour tout } p \in \mathbb{N}^*, \|x\|_p = \left(\sum_{k=1}^n |x_k|^p \right)^{\frac{1}{p}}$$

Remarque : la sous-additivité pour la norme $\|\cdot\|_2$ n'est autre que l'inégalité de Minkowski.

Exercice I.3.

Montrer que pour tout $x \in E, \|x\|_p \rightarrow \|x\|_\infty$ lorsque p tends vers l'infini.

Exemples : pour $E = \mathcal{C}([a, b], \mathbb{C})$.

$$\rightarrow \|f\|_\infty = \sup_{x \in [a, b]} |f(x)|$$

$$\rightarrow \|f\|_1 = \int_a^b |f(x)| dx$$

$$\rightarrow \|f\|_2 = \left(\int_a^b |f(x)|^2 dx \right)^{\frac{1}{2}}$$

$$\rightarrow \text{Pour } p \in \mathbb{N}^*, \|f\|_p = \left(\int_a^b |f(x)|^p dx \right)^{\frac{1}{p}}$$

Exemples : quelques sous espaces normés de l'espace des suites

$$\rightarrow E = l^\infty(\mathbb{N}, \mathbb{K}) = \{(u_n) \in \mathbb{K}^\mathbb{N}, u_n \text{ est bornée}\}, \text{ muni de } \| (u_n) \|_\infty = \sup_{n \in \mathbb{N}} |u_n|$$

$$\rightarrow E = \mathcal{C}_0(\mathbb{N}) = \{(u_n) \in \mathbb{K}^\mathbb{N}, u_n \rightarrow 0\} \text{ muni de } \|\cdot\|_\infty$$

$$\rightarrow \text{Pour } p \geq 1, l^p(\mathbb{N}, \mathbb{K}) = \{(u_n) \in \mathbb{K}^\mathbb{N}, \sum_{n=0}^{+\infty} |u_n|^p \text{ converge}\}$$

Remarque : on a les inclusions suivantes

$$\rightarrow \mathcal{C}_0(\mathbb{N}) \subset l^\infty(\mathbb{N}, \mathbb{K})$$

En effet, si $u_n \xrightarrow{n \rightarrow +\infty} 0$, alors il existe $N \in \mathbb{N}$ pour lequel pour tout $n \geq N$, $|u_n| \leq 1$. Donc pour tout $n \in \mathbb{N}$, $|u_n| \leq \max\{1, |u_0|, |u_1|, \dots, |u_N|\}$, donc $(u_n)_{n \in \mathbb{N}} \in l^\infty(\mathbb{N}, \mathbb{K})$.

$$\rightarrow l^1(\mathbb{N}, \mathbb{K}) \subset l^2(\mathbb{N}, \mathbb{K})$$

En effet, si on considère une suite $(u_n)_{n \in \mathbb{N}} \in l^1(\mathbb{N}, \mathbb{K})$ alors $u_n \rightarrow 0$, et alors à partir d'un certain rang, $|u_n| \leq 1$ et alors $|u_n|^2 \leq |u_n|$. On trouve donc immédiatement que la convergence de la série $\sum_{n=0}^{+\infty} |u_n|$ implique celle de $\sum_{n=0}^{+\infty} |u_n|^2$, donc $(u_n)_{n \in \mathbb{N}} \in l^2(\mathbb{N}, \mathbb{K})$.

II Géométrie

Définition II.1.

Une partie A de E est dite convexe si pour tout $x, y \in A$ et $\lambda \in [0, 1]$

$$\lambda x + (1 - \lambda)y \in A$$

Exercice II.2.

Montrer que tout sous espace affine de E (i.e. les ensembles de la forme $a + F$ avec $a \in E$ et F sous espace vectoriel de E) est convexe.

Remarque : la boule unité fermée de E , $B_f(0, 1) = \{x \in E, \|x\| \leq 1\}$ est convexe.

En effet, si $x, y \in B_f(0, 1)$, alors pour tout $\lambda \in [0, 1]$ on a

$$\|\lambda x + (1 - \lambda)y\| \leq \lambda \|x\| + (1 - \lambda) \|y\| \leq \lambda + 1 - \lambda = 1$$

Donc $\lambda x + (1 - \lambda)y \in B_f(0, 1)$.

Exercice II.3.

Soit $N : E \rightarrow \mathbb{R}$ qui vérifie (N_1) et (N_2) . Soit $A = \{x \in E, N(x) \leq 1\}$. Montrer que si A est convexe, alors N vérifie (N_3) .

Exercice II.4.

Soit $\|\cdot\|$ une norme sur E . Montrer que pour tous $x, y \in E \setminus \{0\}$

$$\|x - y\| \geq \frac{1}{2} \max(\|x\|, \|y\|) \left\| \frac{x}{\|x\|} - \frac{y}{\|y\|} \right\|$$

Exercice II.5.

Une norme $\|\cdot\|$ sur E est dite de somme stricte lorsque pour tous $x, y \in E$

$$\|x + y\| = \|x\| + \|y\| \implies (x, y) \text{ est liée}$$

1. Parmi les normes suivantes, lesquelles sont de somme stricte ?
 - (a) $\|\cdot\|_p$ sur \mathbb{K}^n avec $n \geq 2$ et $p \in \{1, 2, \infty\}$.
 - (b) $\|\cdot\|_p$ sur $C([0, 1], \mathbb{R})$ avec $p \in \{1, 2, \infty\}$.
2. Soit $\|\cdot\|$ une norme sur E . Soit $x, y \in E$. Montrer que si $\|x\| = \|y\| = 1$ et $\|x + y\| = 2$, alors $[x, y] \subset S(0, 1) = \{x \in E, \|x\| = 1\}$.
3. Montrer l'équivalence

$$\|\cdot\| \text{ est stricte sur } E \iff S(0, 1) \text{ ne contient pas de segment non trivial}$$

III Espaces métriques

Définition III.1.

Soit X un ensemble. On dit qu'une application $d : X^2 \rightarrow \mathbb{R}^+$ est une distance sur X lorsqu'elle vérifie les propriétés suivantes

- (D₁) $\forall (x, y) \in X^2, d(x, y) = 0 \Leftrightarrow x = y$ (séparation)
- (D₂) $\forall (x, y) \in X^2, d(x, y) = d(y, x)$ (symétrie)
- (D₃) $\forall (x, y, z) \in X^3, d(x, y) \leq d(x, z) + d(z, y)$ (inégalité triangulaire)

Exemple 1 : soit $\|\cdot\|$ une norme sur E . On appelle distance induite par $\|\cdot\|$ sur E l'application $d : (x, y) \mapsto \|x - y\|$.

La distance induite définit bien une distance. En effet, il est facile de montrer les implications suivantes :

- $\rightarrow (N_1) \implies (D_1)$
- $\rightarrow (N_2) \implies (D_2)$
- $\rightarrow (N_3) \implies (D_3)$

Exemple 2 : on considère le cas où $X = l^\infty(\mathbb{N}, \mathbb{K})$. L'application $d : ((x_n), (y_n)) \mapsto \sum_{n=0}^{+\infty} \frac{|x_n - y_n|}{2^n}$ définit bien une distance sur X .

Proposition III.2.

Soit X une espace métrique et $d : X^2 \rightarrow \mathbb{R}^+$ une distance sur X . d vérifie les propriétés suivantes

1. $\forall n \in \mathbb{N}^* \setminus \{1\}, \forall (x_1, \dots, x_n) \in X^n, d(x_1, x_n) \leq \sum_{i=1}^{n-1} d(x_i, x_{i+1})$
2. $\forall (x, y, z) \in X^3, |d(x, y) - d(x, z)| \leq d(y, z)$

Preuve

1. Il s'agit d'une simple récurrence. L'initialisation ($n = 2$) correspond à la propriété (D_3) . Soit $n \in \mathbb{N}^* \setminus \{1\}$, supposons l'hypothèse de récurrence vérifiée :

$$\forall n \in \mathbb{N}^* \setminus \{1\}, \forall (x_1, \dots, x_n) \in X^n, d(x_1, x_n) \leq \sum_{i=1}^{n-1} d(x_i, x_{i+1})$$

Soit $x_1, \dots, x_{n+1} \in X$, on a

$$d(x_1, x_{n+1}) \leq d(x_1, x_n) + d(x_n, x_{n+1}) \leq \sum_{i=1}^{n-1} d(x_i, x_{i+1}) + d(x_n, x_{n+1}) = \sum_{i=1}^n d(x_i, x_{i+1})$$

On en déduit donc immédiatement le résultat voulu.

2. Soit $(x, y, z) \in X^3$, il s'agit de montrer que

- (a) $d(x, y) - d(x, z) \leq d(y, z)$
- (b) $d(x, z) - d(x, y) \leq d(y, z)$

Le point (a) est équivalent à $d(x, y) \leq d(x, z) + d(y, z)$, ce qui est vrai d'après (D_3) . On peut dire la même chose du point (b).

IV Boules ouvertes, fermées, sphères ...

Dans toute la suite X est espace métrique muni d'une distance d .

Définition IV.1.

Soit $(a, r) \in X \times]0, +\infty[$. On appelle boule ouverte de centre a et rayon r l'ensemble

$$B(a, r) = \{x \in X, d(x, a) < r\}$$

De même, on appelle boule fermée de centre a et de rayon r l'ensemble

$$B_f(a, r) = \{x \in X, d(x, a) \leq r\}$$

On appelle aussi sphère de centre a et de rayon r l'ensemble

$$S(a, r) = \{x \in X, d(x, a) = r\}$$

Exemple : En espace vectoriel normé muni d'une norme $\|\cdot\|$, lorsqu'on prend d égal à la distance induite par la norme, ces ensembles s'écrivent :

- $\rightarrow B(a, r) = \{x \in X, \|x - a\| < r\}$
- $\rightarrow B_f(a, r) = \{x \in X, \|x - a\| \leq r\}$

$$\rightarrow S(a, r) = \{x \in X, \|x - a\| = r\}$$

Définition IV.2.

Soit $A \subset X$. On appelle distance induite sur A la restriction de d à A^2 . Cette distance est notée d_A .

Notation : En remplaçant la distance d par d_A dans les définitions d'une boule et d'une sphère, pour $(a, r) \in A \times \mathbb{R}^+$

$$\rightarrow B_A(a, r) = \{x \in A, d_A(x, a) < r\} = B(a, r) \cap A$$

$$\rightarrow B_{fA}(a, r) = \{x \in A, d_A(x, a) \leq r\} = B_f(a, r) \cap A$$

$$\rightarrow S_A(a, r) = \{x \in A, d_A(x, a) = r\} = S(a, r) \cap A$$

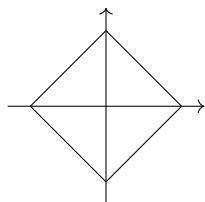
Exemples :

→ Pour $X = \mathbb{R}$, $A = [0, 1]$ et d la distance induite par la valeur absolue, $B_A(1, \frac{1}{2}) =]\frac{1}{2}, 1]$.

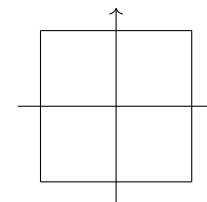
→ Pour $X = \mathbb{C}$, $A = S(0, 1)$ et d la distance induite par le module, $B_A(i, 1) = \{e^{i\theta}, \theta \in [\frac{\pi}{6}, \frac{5\pi}{6}]\}$.

Dessins en espace vectoriel normé : voici des dessins de la boule unité $B_f(0, 1)$ pour quelques exemples de X .

$X = \mathbb{R}^2$ et d la distance induite par $\|\cdot\|_1$



$X = \mathbb{R}^2$ et d la distance induite par $\|\cdot\|_\infty$



Proposition IV.3.

Lorsque X est un espace vectoriel normé muni d'une norme $\|\cdot\|$ et de la distance induite par cette norme, on a les égalités suivantes pour tout $(a, r) \in X \times \mathbb{R}_+^*$

1. $B(a, r) = a + B(0, r) = a + rB(0, 1)$
2. $B_f(a, r) = a + B_f(0, r) = a + rB_f(0, 1)$

Preuve : nous allons montrer le point (1). La preuve du point 2 est identique : il suffit de remplacer les inégalités strictes par des inégalités larges.

Soit $(a, r) \in X \times \mathbb{R}_+^*$, on a

$$\begin{aligned} x \in B(a, r) &\iff \|x - a\| < r \\ &\iff \left\| \frac{1}{r}(x - a) \right\| < 1 \\ &\iff \frac{1}{r}(x - a) \in B(0, 1) \\ &\iff x \in a + rB(0, 1) \end{aligned}$$

V Bornitude

Proposition V.1.

Soit A une partie de X . Les propriétés suivantes sont équivalentes.

1. $\{d(x, y), (x, y) \in A^2\}$ est une partie bornée de \mathbb{R}^+ .
2. Il existe une boule ouverte de X qui contient A .
3. Pour tout $a \in X$, il existe r tel que $A \subset B(a, r)$.

Si A vérifie l'une de ces trois propriétés, on dit que A est borné et on note

$$\text{diam}(A) = \sup\{d(x, y), (x, y) \in A^2\}$$

Preuve

$\rightarrow (1) \implies (2)$

Soit $a \in A$. L'ensemble $D = \{d(x, y), (x, y) \in A^2\}$ est une partie bornée de \mathbb{R} donc admet une borne supérieure. On pose alors $r = 1 + \sup D$. Pour tout $x \in A$, $d(x, a) \leq \sup D < r$.

On en déduit donc que $A \subset B(a, r)$.

$\rightarrow (2) \implies (3)$

Soit $B(b, \varepsilon)$ une boule qui contient A . Soit $a \in X$. On pose $r = \varepsilon + d(a, b)$.

Pour tout $x \in A$, on a $d(x, b) \leq d(x, a) + d(a, b) < \varepsilon + d(a, b) = r$. Donc $A \subset B(a, r)$.

$\rightarrow (3) \implies (1)$

Soit $B(a, r)$ une boule qui contient A . Pour tout $(x, y) \in A^2$,

$$d(x, y) \leq d(x, a) + d(a, y) < 2r$$

L'ensemble D est alors majoré par $2r$.

Exercice V.2.

Soit E un espace vectoriel normé différent de $\{0\}$.

1. Montrer que pour tout $(a, r) \in E \times \mathbb{R}^+$, $\text{diam}(B(a, r)) = \text{diam}(B_f(a, r))$
2. Montrer que le rayon et le centre d'une boule ouverte ou fermée sont uniques.

Définition V.3.

Soit A une partie de X . On dit qu'une fonction $f : A \rightarrow X$ est bornée lorsque $f(A)$ est borné.

Notation : On désigne par $\mathcal{B}(A, X)$ l'ensemble des fonctions bornées de A dans X .

Définition V.4.

Soit $(u_n)_{n \in \mathbb{N}}$ une suite à valeurs dans X . On dit que $(u_n)_{n \in \mathbb{N}}$ est bornée lorsque l'ensemble $\{u_n, n \in \mathbb{N}\}$ est borné.

VI Suites dans un espace métrique et dans un espace vectoriel normé

Définition VI.1.

Soit $(u_n)_{n \in \mathbb{N}}$ une suite à valeurs dans X . On dit que (u_n) converge lorsque

$$\exists l \in X \quad \forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall n \geq N \quad d(u_n, l) \leq \varepsilon$$

Proposition VI.2.

On suppose que X est un \mathbb{K} -espace vectoriel normé muni d'une norme $\|\cdot\|$ et que d est la distance induite par cette norme.

Soit $(u_n)_{n \in \mathbb{N}}$ et $(v_n)_{n \in \mathbb{N}}$ deux suites à valeurs dans X .

1. Pour tout $(l, l') \in \mathbb{R}^2$, Si (u_n) converge vers l et l' , alors $l = l'$.
2. pour tous $a, b, l, l' \in \mathbb{R}$, si $u_n \xrightarrow[n \rightarrow +\infty]{} l$ et $v_n \xrightarrow[n \rightarrow +\infty]{} l'$ alors $au_n + bv_n \xrightarrow[n \rightarrow +\infty]{} al + bl'$
3. Si $(\lambda_n)_{n \in \mathbb{N}}$ est une suite à valeurs dans \mathbb{K} qui converge vers $\lambda \in \mathbb{K}$, et $(u_n)_{n \in \mathbb{N}}$ converge vers l , alors la suite $(\lambda_n u_n)_{n \in \mathbb{N}}$ converge vers λl .

VII Algèbres normées

Définition VII.1.

Soit \mathcal{A} un ensemble. On dit que $(\mathcal{A}, +, ., *)$ est une \mathbb{K} -algèbre lorsque

- $(\mathcal{A}, +, .)$ est un \mathbb{K} -espace vectoriel.
- $*$ est une loi de composition interne.
- $*$ est bilinéaire.

Vocabulaire :

- Si $*$ est associative, on dit que \mathcal{A} est une algèbre associative.
- Si $*$ admet un élément neutre, on dit que \mathcal{A} est une algèbre unitaire.

Définition VII.2.

Soit \mathcal{A} une algèbre munie d'une norme $\|\cdot\|$. On dit que $\|\cdot\|$ est une norme d'algèbre lorsque pour tous $(a, b) \in \mathcal{A}^2$

$$\|a * b\| \leq \|a\| \|b\|$$

Proposition VII.3.

Soit \mathcal{A} une algèbre munie d'une norme d'algèbre $\|\cdot\|$. Soit $(a_n)_{n \in \mathbb{N}}$ et $(b_n)_{n \in \mathbb{N}}$ deux suites à valeurs dans \mathcal{A} . L'implication suivante est vraie

$$a_n \xrightarrow[n \rightarrow +\infty]{} a \text{ et } b_n \xrightarrow[n \rightarrow +\infty]{} b \implies a_n * b_n \xrightarrow[n \rightarrow +\infty]{} a * b$$

Preuve : Soit $(a_n)_{n \in \mathbb{N}}$ et $(b_n)_{n \in \mathbb{N}}$ deux suites vérifiant les hypothèses. On a

$$\begin{aligned}\|a_n * b_n - a * b\| &= \|a_n * b_n - a * b_n + a * b_n - a * b\| \\ &\leq \|(a_n - a) * b_n\| + \|a * (b_n - b)\| \\ &\leq \|a_n - a\| \|b_n\| + \|a\| \|b_n - b\| \xrightarrow{n \rightarrow +\infty} 0\end{aligned}$$

Exercice VII.4.

Soit \mathcal{A} une algèbre munie d'une norme d'algèbre $\|\cdot\|$. Soit $a \in \mathcal{A} \setminus \{0\}$ non nilpotent, montrer que la suite $(\|a^n\|^{\frac{1}{n}})_{n \in \mathbb{N}}$ est convergente.

VIII Suites de fonctions

Dans toute cette partie, on considère A un ensemble et E un espace vectoriel normé muni d'une norme $\|\cdot\|$.

Définition VIII.1.

Soit $(f_n)_{n \in \mathbb{N}}$ une suite de fonctions de A dans E . On dit que la suite $(f_n)_{n \in \mathbb{N}}$ est simplement convergente lorsque pour tout $x \in A$, la suite $(f_n(x))_{n \in \mathbb{N}}$ est convergente.

Vocabulaire : la fonction $f : x \mapsto \lim_n f_n(x)$ est appelée limite simple de $(f_n)_{n \in \mathbb{N}}$.

Exemple : On considère ici le cas où $A = [0, 1]$, $E = \mathbb{R}$ et $(f_n) = (x \mapsto x^n)$. $(f_n)_{n \in \mathbb{N}}$ converge simplement vers f qui est définie par

$$f : x \mapsto \begin{cases} 0 & \text{si } x \in [0, 1[\\ 1 & \text{sinon} \end{cases}$$

Définition VIII.2.

Soit $(f_n)_{n \in \mathbb{N}}$ une suite de fonctions de A dans E . On dit que $(f_n)_{n \in \mathbb{N}}$ est uniformément convergente lorsqu'il existe une fonction f de A dans E telle que

$$\sup_{x \in A} \|f_n(x) - f(x)\| \xrightarrow{n \rightarrow +\infty} 0$$

Remarque : une formulation équivalente à la définition précédente est la suivante

$$\forall \varepsilon > 0 \exists N \in \mathbb{N} \forall n \geq N \forall x \in A \|f_n(x) - f(x)\| \leq \varepsilon$$

La convergence uniforme implique évidemment la convergence simple, mais la réciproque est fausse. En effet, il suffit de considérer la suite de fonctions $(x \mapsto x^n)_{n \in \mathbb{N}}$. Cette suite de fonctions converge simplement vers la fonction f définie juste avant la définition précédente, qui vaut 0 sur $[0, 1[$ et 1 en 1. Mais f ne converge pas uniformément vers f car pour tout $n \in \mathbb{N}$, $\sup_{x \in A} \|f_n(x) - f(x)\| = 1$. Cette quantité ne peut donc pas tendre vers 0.

Proposition VIII.3.

On considère le cas où $E = \mathcal{C}([a, b], \mathbb{C})$, avec $a < b$. Soit $(f_n)_{n \in \mathbb{N}} \in E^{\mathbb{N}}$. Si (f_n) converge uniformément vers $f \in \mathcal{C}([a, b], \mathbb{C})$, alors on a

$$\|f_n - f\|_1 \xrightarrow[n \rightarrow +\infty]{} 0 \text{ et } \|f_n - f\|_2 \xrightarrow[n \rightarrow +\infty]{} 0$$

Preuve

Pour tout $n \in \mathbb{N}$, on a

$$\|f_n - f\|_1 = \int_a^b |f_n(t) - f(t)| dt \leq (b-a) \|f_n - f\|_\infty \xrightarrow[n \rightarrow \infty]{} 0$$

et

$$\|f_n - f\|_2 = \sqrt{\int_a^b |f_n(t) - f(t)|^2 dt} \leq \sqrt{(b-a) \|f_n - f\|_\infty^2} = \sqrt{b-a} \|f_n - f\|_\infty \xrightarrow[n \rightarrow +\infty]{} 0$$

Correction de l'exercice I.3. :

Soit $x = (x_1, \dots, x_n) \in E$. Si $\|x\|_\infty = 0$, on a $x = 0$ et alors pour tout $p \in \mathbb{N}^*$, $\|x\|_p = 0$. La proposition qu'on veut démontrer est donc vraie. Supposons donc à présent que $\|x\|_\infty > 0$. On pose $r = |\{i \in \llbracket 1; n \rrbracket, x_i = \|x\|_\infty\}|$. Quitte à permute les x_i , on suppose sans perte de généralité que $x_1 = x_2 = \dots = x_r = \|x\|_\infty$ et pour tout $k \geq r+1$, $|x_k| < \|x\|_\infty$.

On a alors pour tout $p \in \mathbb{N}^*$,

$$\begin{aligned}\|x\|_p &= \left(\sum_{k=1}^n |x_k|^p \right)^{\frac{1}{p}} \\ &= \|x\|_\infty \left(r + \sum_{k=r+1}^n \left| \frac{x_k}{\|x\|_\infty} \right|^p \right)^{\frac{1}{p}}\end{aligned}$$

Pour tout $k \geq r+1$, $\left| \frac{x_k}{\|x\|_\infty} \right| \in [0, 1[$, donc $\left| \frac{x_k}{\|x\|_\infty} \right|^p \xrightarrow[p \rightarrow +\infty]{} 0$. On a alors

$$r + \sum_{k=r+1}^n \left| \frac{x_k}{\|x\|_\infty} \right|^p \xrightarrow[p \rightarrow +\infty]{} r$$

Or

$$\|x\|_p = \|x\|_\infty \left(r + \sum_{k=r+1}^n \left| \frac{x_k}{\|x\|_\infty} \right|^p \right)^{\frac{1}{p}} \in [\|x\|_\infty, n^{\frac{1}{p}} \|x\|_\infty]$$

et finalement, par le lemme des gendarmes

$$\|x\|_p \xrightarrow[p \rightarrow +\infty]{} \|x\|_\infty$$

Correction de l'exercice II.2. :

Soit F un sous espace vectoriel de E et $a \in E$. On pour $F' = a + F$. Soit $x, y \in F'$ et $\lambda \in [0, 1]$. Par définition, il existe $u, v \in F$ tels que $x = a + u$ et $y = a + v$. On a alors

$$\begin{aligned}\lambda x + (1 - \lambda)y &= \lambda a + \lambda u + (1 - \lambda)a + (1 - \lambda)v \\ &= a + \underbrace{\lambda u + (1 - \lambda)v}_{\in F} \in F'\end{aligned}$$

Correction de l'exercice II.3. :

Supposons que A est convexe. Soit $x, y \in E \setminus \{0\}$, $\frac{x}{N(x)}$ et $\frac{y}{N(y)}$ sont deux éléments de A , donc en posant $\lambda = \frac{N(x)}{N(x) + N(y)} \in [0, 1]$ on a

$$N \left(\lambda \frac{x}{N(x)} + (1 - \lambda) \frac{y}{N(y)} \right) \leq 1$$

Or

$$\begin{aligned}N \left(\lambda \frac{x}{N(x)} + (1 - \lambda) \frac{y}{N(y)} \right) &= N \left(\frac{N(x)}{N(x) + N(y)} \frac{x}{N(x)} + \frac{N(y)}{N(x) + N(y)} \frac{y}{N(y)} \right) \\ &= \frac{N(x+y)}{N(x) + N(y)}\end{aligned}$$

On en déduit donc finalement que

$$N(x+y) \leq N(x) + N(y)$$

On a donc montré la propriété (N_3) pour N .

Correction de l'exercice II.4. :

Quitte à permutez x et y supposons que $\max(\|x\|, \|y\|) = \|x\|$. On a alors

$$\begin{aligned} \frac{1}{2} \max(\|x\|, \|y\|) \left\| \frac{x}{\|x\|} - \frac{y}{\|y\|} \right\| &= \frac{1}{2\|y\|} (\|y\| x - \|x\| y) \\ &= \frac{1}{2\|y\|} (\|y\| x - \|y\| y + \|y\| y - \|x\| y) \\ &\leq \frac{1}{2\|y\|} (\|y\| \|x - y\| + \|y\| \|x\| - \|y\| \|y\|) \\ &= \frac{1}{2\|y\|} (\|y\| \|x - y\| + \|y\| \|x\| - \|y\| \|y\|) \\ &\leq \frac{1}{2\|y\|} (\|y\| \|x - y\| + \|y\| \|x - y\|) \\ &= \|x - y\| \end{aligned}$$

Correction de l'exercice II.5. :

1. Nous allons séparer les cas $p = 1$, $p = 2$ et $p = \infty$.

(a) Mettons nous sur \mathbb{K}^n

→ Si $p = \infty$, la norme $\|\cdot\|_\infty$ n'est pas de somme stricte.

En effet, il suffit de considérer le cas $n = 2$ pour voir que ce n'est pas le cas :

$$\|(1, 0) + (1, 1)\|_\infty = 2 = \|(1, 0)\|_\infty + \|(1, 1)\|_\infty$$

mais $((1, 0), (1, 1))$ n'est pas liée.

→ Si $p = 1$, la norme $\|\cdot\|_1$ n'est pas de somme stricte.

En effet, il suffit de considérer le cas $n = 2$ pour voir que ce n'est pas le cas :

$$\|(1, 0) + (0, 1)\|_1 = 2 = \|(1, 0)\|_1 + \|(0, 1)\|_1$$

mais $((1, 0), (0, 1))$ n'est pas liée.

→ Si $p = 2$, la norme $\|\cdot\|_2$ est de somme stricte.

En effet, si on considère $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbb{K}^n$,

$$\begin{aligned} \|x + y\|_2 = \|x\|_2 + \|y\|_2 &\iff \|x + y\|_2^2 = (\|x\|_2 + \|y\|_2)^2 \\ &\iff \|x\|_2^2 + \|y\|_2^2 + 2 \sum_{k=1}^n x_k y_k = \|x\|_2^2 + \|y\|_2^2 + 2 \|x\| \|y\| \\ &\iff \sum_{k=1}^n x_k y_k = \sqrt{\left(\sum_{k=1}^n x_k^2 \right) \left(\sum_{k=1}^n y_k^2 \right)} \end{aligned}$$

La dernière ligne implique le cas d'égalité de l'inégalité de Cauchy-Schwarz (il suffit de majorer la somme des $x_k y_k$ par la somme des $|x_k y_k|$, qui est équivalent au fait que (x, y) soit liée).

(b) Mettons nous sur $\mathcal{C}([0, 1], \mathbb{R})$

→ Si $p = \infty$, la norme $\|\cdot\|_\infty$ n'est pas de somme stricte.

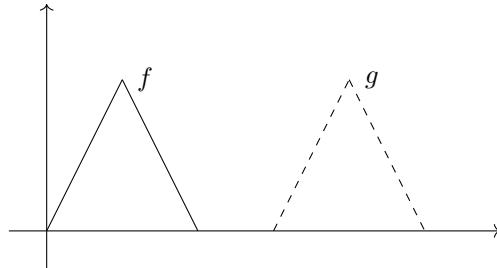
En effet, il suffit de considérer les deux fonctions continues sur $[0, 1]$ $f : t \mapsto t$ et $g : t \mapsto 1$.

$$\|f + g\|_\infty = 2 = \|f\|_\infty + \|g\|_\infty$$

alors que (f, g) n'est pas liée.

→ Si $p = 1$, la norme $\|\cdot\|_1$ n'est pas de somme stricte.

En effet, il suffit de prendre f et g respectivement décrites par les courbes ci dessous.



Il est clair que

$$\|f + g\|_1 = \|f\|_1 + \|g\|_1$$

alors que (f, g) n'est pas liée.

→ Si $p = 2$, la norme $\|\cdot\|_2$ est de somme stricte.

En effet, si on considère $f, g \in \mathcal{C}([0, 1], \mathbb{R})$,

$$\begin{aligned} \|f + g\|_2 &= \|f\|_2 + \|g\|_2 \iff \|f + g\|_2^2 = (\|f\|_2 + \|g\|_2)^2 \\ &\iff \|f\|_2^2 + \|g\|_2^2 + 2 \int_0^1 f(t)g(t)dt = \|f\|_2^2 + \|g\|_2^2 + 2 \|f\| \|g\| \\ &\iff \int_0^1 f(t)g(t)dt = \sqrt{\left(\int_0^1 f(t)^2 dt\right) \left(\int_0^1 g(t)^2 dt\right)} \end{aligned}$$

La dernière ligne implique le cas d'égalité de l'inégalité de Cauchy-Schwarz (il suffit de majorer l'intégrale de fg par l'intégrale de $|fg|$), qui est équivalent au fait que (f, g) soit liée.

2. Soit $x, y \in E$ vérifiant $\|x + y\| = 2$ et $\|x\| = \|y\| = 1$.

Soit $\lambda \in [0, 1]$, on a

$$\underbrace{\|\lambda x + (1 - \lambda)y\|}_{\leq 1} + \underbrace{\|(1 - \lambda)x + \lambda y\|}_{\leq 1} \geq \|x + y\| = 2$$

Donc

$$\|\lambda x + (1 - \lambda)y\| = \|(1 - \lambda)x + \lambda y\| = 1$$

et finalement $[x, y] \subset S(0, 1)$.

3. (\implies) Supposons que $\|\cdot\|$ est stricte.

Soit $x, y \in S(0, 1)$. Supposons que $[x, y] \subset S(0, 1)$. On a

$$\left\| \frac{1}{2}x + \frac{1}{2}y \right\| = 1 = \left\| \frac{1}{2}x \right\| + \left\| \frac{1}{2}y \right\|$$

Donc (x, y) est liée et x et y sont de même norme, pour $\mathbb{K} = \mathbb{R}$, deux cas se présentent

→ $x = -y$ ce qui donne $\left\| \frac{1}{2}x + \frac{1}{2}y \right\| = 0$, chose qui n'est clairement pas possible.

→ $x = y$ et donc le segment $[x, y]$ est trivial.

On en déduit alors immédiatement que $S(0, 1)$ ne contient aucun segment non trivial.

(\Leftarrow) Nous allons procéder par contraposée. Supposons que $\|\cdot\|$ est non stricte, i.e. il existe (x, y) libre telle que $\|x + y\| = \|x\| + \|y\|$.

On suppose sans perte de généralité de que $\|x\| \leq \|y\|$. On a

$$\begin{aligned} 2 &\geq \left\| \frac{x}{\|x\|} + \frac{y}{\|y\|} \right\| = \left\| \frac{x}{\|x\|} + \frac{y}{\|x\|} - \frac{y}{\|x\|} + \frac{y}{\|y\|} \right\| \\ &\geq \frac{1}{\|x\|} (\|x\| + \|y\|) - \|y\| \left(\frac{1}{\|x\|} - \frac{1}{\|y\|} \right) \\ &= 2 \end{aligned}$$

Donc $\left\| \frac{x}{\|x\|} + \frac{y}{\|y\|} \right\| = 2$ et $\frac{x}{\|x\|}, \frac{y}{\|y\|} \in S(0, 1)$. On en déduit d'après la question précédente que $\left[\frac{x}{\|x\|}, \frac{y}{\|y\|} \right] \subset S(0, 1)$. Ce segment est non trivial puisque (x, y) est libre.

$S(0, 1)$ contient donc bien un segment non trivial.

Correction de l'exercice V.2. :

- Soit $(a, r) \in E \times \mathbb{R}^+$. On sait déjà que $\text{diam}(B(a, r)) \leq 2r$ et $\text{diam}(B_f(a, r)) \leq 2r$ (il suffit d'appliquer l'inégalité triangulaire).

Comme $E \neq \{0\}$, on peut considérer $u \in X$ tel que $\|u\| = 1$. On pose alors

$$x = a + ru \in B_f(a, r) \text{ et } y = a - ru \in B_f(a, r)$$

On a donc $\|x - y\| = 2r$ ce qui donne $\text{diam}(B_f(a, r)) = 2r$.

De même, on pose $(r_n)_{n \geq N} = (r - \frac{1}{n})_{n \geq N}$ avec N assez grand pour qu'on ait $r - \frac{1}{N} \geq 0$ et

$$x_n = a + r_n u \in B(a, r) \text{ et } y_n = a - r_n u \in B(a, r)$$

On a alors $\|x_n - y_n\| = 2r_n \xrightarrow{n \rightarrow +\infty} 2r$. La suite $(\|x_n - y_n\|)_{n \geq N}$ est à valeurs dans $\{\|x - y\|, (x, y) \in E^2\}$ qui est majoré par $2r$, donc $\text{diam}(B(a, r)) = 2r$.

- L'unicité du rayon d'une boule vient tout simplement de la question précédente. En effet, en espace vectoriel normé, on peut définir de manière unique le rayon d'une boule fermée ou ouverte comme le diamètre de la boule. Il reste donc à montrer l'unicité du centre. Nous allons le faire pour le cas d'une boule fermée. Le cas d'une boule ouverte peut être traité de la même manière.

Soit $(a, r) \in E \times \mathbb{R}^+$. On suppose que $b \in E$ est aussi un centre de $B_f(a, r)$ tel que $b \neq a$. On a alors pour tout $x \in B_f(a, r)$, $\|x - b\| < r$ et $\|x - a\| < r$. Posons $v = \frac{a - b}{\|a - b\|}$. On a $a - rv \in B_f(a, r)$, donc

$$\begin{aligned} r &\geq \|a - rv - b\| = \left\| \left(\frac{r}{\|a - b\|} + 1 \right) (a - b) \right\| \\ &= r + \|a - b\| \end{aligned}$$

donc $\|a - b\| = 0$ ce qui est absurde. On a donc bien l'unicité du centre.

Correction de l'exercice VII.4. :

On a pour tout $n \in \mathbb{N}^*$, $\|a^n\|^{\frac{1}{n}} \leq (\|a\|^n)^{\frac{1}{n}}$ et pour tout $n, m \in \mathbb{N}^*$, $\|a^{n+m}\| \leq \|a^n\| \|a^m\|$. Donc si on pose pour tout n , $v_n = \log \|a^n\|$, on a pour tout $m, n \in \mathbb{N}^*$, $v_{n+m} \leq v_n + v_m$.

Posons également pour tout n , $u_n = \log(\|a^n\|^{\frac{1}{n}})$. On a alors $(v_n)_{n \in \mathbb{N}}$ est sous additive et pour tout n , $u_n = \frac{v_n}{n}$. Donc d'après le théorème de Fekete (hors programme, mais très classique)

$$u_n \xrightarrow{n \rightarrow +\infty} \inf_{k \in \mathbb{N}^*} u_k = \alpha$$

et finalement

$$\|a^n\|^{\frac{1}{n}} \xrightarrow[n \rightarrow +\infty]{} e^\alpha$$

Remarque : ici, on suppose implicitement par convention que $e^{-\infty} = 0$.



CHAPITRE 11.2

Ouverts et fermés

Dans tout le chapitre, on considère X un espace métrique muni d'une distance d .

I Ouverts

Définition I.1.

Soit O un sous ensemble de X . On dit que O est ouvert lorsque

$$\forall a \in O, \exists r > 0, B(a, r) \subset O$$

Exemples

- \emptyset et les intervalles ouverts sont des ouverts de \mathbb{R} .
- \mathbb{R} n'est pas ouvert dans \mathbb{C} .

Proposition I.2.

Soit I un ensemble et $(O_i)_{i \in I}$ est une famille d'ouverts de X .

1. \emptyset et X sont des ouverts de X .
2. $\bigcup_{i \in I} O_i$ est ouvert.
3. Si I est fini, alors $\bigcap_{i \in I} O_i$ est ouvert.

Preuve

1. La proposition est évidente par définition.
2. Soit $a \in \bigcup_{i \in I} O_i$. Il existe $i_0 \in I$ tel que $a \in O_{i_0}$. Donc il existe $r > 0$ tel que $B(a, r) \subset O_{i_0} \subset \bigcup_{i \in I} O_i$.
 $\bigcup_{i \in I} O_i$ est donc bien ouvert.
3. Supposons que I soit fini. Soit $a \in \bigcap_{i \in I} O_i$. On a alors pour tout $i \in I$, il existe $r_i > 0$ tel que $B(a, r_i) \subset O_i$. I est fini, donc on peut définir $r = \min\{r_i\}_{i \in I} > 0$. Par construction, on a bien $B(a, r) \subset \bigcap_{i \in I} O_i$. $\bigcap_{i \in I} O_i$ est donc bien ouvert.

Attention : si I est infini, $\bigcap_{i \in I} O_i$ n'est pas forcément ouvert. En effet, si on prend $I = \mathbb{N}^*$ et pour tout $k \in I$, $O_k =]-\frac{1}{k}, \frac{1}{k}[$. On a $\bigcap_{k \in \mathbb{N}^*} \left] -\frac{1}{k}, \frac{1}{k} \right[= \{0\}$ qui n'est pas ouvert.

Définition I.3.

Soit $a \in X$. Une partie U de X est appelée voisinage de a s'il existe $r > 0$ tel que $B(a, r) \subset U$.

Remarque : un ouvert est voisinage de tous ses points.

Exemple : Pour tout $(b, r) \in X \times \mathbb{R}_+^*$, $B(b, r)$ est un ouvert.

Montrons ce résultat. Soit $a \in B(b, r)$. Posons $\varepsilon = r - d(a, b)$. On a alors pour tout $x \in B(a, \varepsilon)$,

$$d(x, b) \leq d(x, a) + d(a, b) < \varepsilon + d(a, b) = r$$

donc $B(a, \varepsilon) \subset B(b, r)$. On en déduit donc que $B(b, r)$ est ouvert.

Proposition I.4.

Soit $a \in X$. On note $\mathcal{V}(a)$ l'ensemble des voisinages de a .

1. Si $U \in \mathcal{V}(a)$ et $U \subset V$, alors $V \in \mathcal{V}(a)$.
2. L'intersection d'une famille finie d'éléments de $\mathcal{V}(a)$ appartient à $\mathcal{V}(a)$.
3. Si $a \neq b$, alors il existe $(U, V) \in \mathcal{V}(a) \times \mathcal{V}(b)$ tel que $U \cap V = \emptyset$.

Preuve

1. Soit U voisinage de a et V un ensemble contenant U . U étant un voisinage de a , il existe $r > 0$ tel que $B(a, r) \subset U \subset V$. Donc V est aussi un voisinage de a .
2. Soit $p \in \mathbb{N}^*$ et $V_1, \dots, V_p \in \mathcal{V}(a)$. Pour tout $i \in \llbracket 1; p \rrbracket$, il existe $r_i > 0$ tel que $B(a, r_i) \subset V_i$. On pose $r = \min\{r_1, \dots, r_p\} > 0$. On a alors $B(a, r) \subset \bigcap_{i=1}^p V_i$, donc $\bigcap_{i=1}^p V_i \in \mathcal{V}(a)$.
3. Soit $r = \frac{d(a, b)}{10}$. Prenons $U = B(a, r)$ et $V = B(b, r)$. Si $x \in U \cap V$, alors $d(x, a) < r$ et $d(x, b) < r$. En sommant les deux inégalités, on obtient

$$d(a, b) \leq d(x, a) + d(x, b) < 2r = \frac{d(a, b)}{5}$$

ce qui est impossible. On en déduit donc que $U \cap V = \emptyset$.

II Fermés

Définition II.1.

Soit F une partie de X . On dit que F est fermé si $X \setminus F$ est ouvert.

Exemples

- Si $a \leq b$, alors $[a, b]$ est un fermé.
- Pour tout $(b, r) \in X \times \mathbb{R}^+$, $B_f(b, r)$ est fermé.
En effet, si on prend $a \in X \setminus B_f(b, r)$, on peut considérer $\varepsilon = \frac{d(a, b) - r}{2} > 0$ (ε est non nul car sinon on aurait $a \in B_f(b, r)$). Si $x \in B(a, \varepsilon)$, alors $d(x, b) \geq d(a, b) - d(x, a) \geq \frac{d(a, b) + r}{2} > r$ donc $B(a, \varepsilon) \subset X \setminus B_f(b, r)$ et alors $B_f(b, r)$ est fermé.
- Une réunion finie de points est un fermé.

Proposition II.2.

Soit F une partie de X . F est fermée si et seulement si pour toute suite $(x_n)_{n \in \mathbb{N}}$ à valeurs dans F , si (x_n) est convergente, alors sa limite est dans F .

Preuve

- (\Rightarrow) Supposons que F soit fermé. Soit $(x_n)_{n \in \mathbb{N}}$ une suite à valeurs dans F convergente, supposons que la limite l de (x_n) est dans $X \setminus F$. $X \setminus F$ étant ouvert, il existe $\varepsilon > 0$ tel que $B(l, \varepsilon) \subset X \setminus F$. Or par construction, il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $d(x_n, l) \leq \frac{\varepsilon}{2}$ et donc $x_n \in B(l, \varepsilon) \subset X \setminus F$ ce qui est absurde.
- (\Leftarrow) Réciproquement, supposons que toute suite à valeurs dans F convergente converge dans F . supposons de plus que F n'est pas fermé, i.e. $X \setminus F$ n'est pas ouvert. Il existe donc $a \in X \setminus F$ tel que pour tout $\varepsilon > 0$, $B(a, \varepsilon) \not\subset X \setminus F$ i.e. $B(a, \varepsilon) \cap F \neq \emptyset$. Cette propriété étant vraie pour $\varepsilon = \frac{1}{n}$ et tout $n \in \mathbb{N}$, on peut définir une suite $(x_n)_{n \in \mathbb{N}}$ à valeurs dans F qui vérifie pour tout $n \in \mathbb{N}^*$, $d(a, x_n) \leq \frac{1}{n}$. (x_n) est à valeurs dans F et converge vers a qui n'est pas dans F , ce qui est en contradiction avec les hypothèses.

Proposition II.3.

1. X et \emptyset sont fermés dans X .
2. Soit I un ensemble. Si $(F_i)_{i \in I}$ est une famille de fermés de X , alors $\bigcap_{i \in I} F_i$ est un fermé.
3. Si I est fini, alors $\bigcup_{i \in I} F_i$ est un fermé.

Preuve : pour montrer ces trois propriétés, il suffit de montrer que les complémentaires de ces ensembles sont ouverts en utilisant les propriétés vu sur les ouverts au début du chapitre.

Exercice II.4.

Soit $(u_n)_{n \in \mathbb{N}}$ une suite à valeurs dans X . Montrer que l'ensemble des valeurs d'adhérence de (u_n) est fermé.

Exercice II.5.

Soit $E = l^1(\mathbb{N}, \mathbb{C})$ muni de $\|\cdot\|_1$ et $N \in \mathbb{N}$. Montrer que $A = \{(u_n) \in E^{\mathbb{N}}, u_0 \neq 0, \dots, u_N \neq 0\}$ est ouvert.

Exercice II.6.

Soient $E = C([0, 1], \mathbb{R})$, $O = \{f \in E, \forall x \in [0, 1], f(x) > 0\}$ et $F = \{f \in E, \forall x \in [0, 1], f(x) \geq 0\}$.

1. O est-il ouvert pour la distance induite par $\|\cdot\|_\infty$? $\|\cdot\|_1$?
2. F est-il fermé pour la distance induite par $\|\cdot\|_\infty$? $\|\cdot\|_1$?

III Topologie induite

Dans cette partie on considère A une partie de X et on considère d_A la restriction de d à A^2 . (A, d_A) ainsi défini est un espace métrique, et pour tout $(a, r) \in A \times \mathbb{R}^+$, $B_{d_A}(a, r) = B(a, r) \cap A$.

Proposition III.1.

1. Une partie O de A est ouverte pour d_A si et seulement si il existe $\Omega \subset X$ ouvert tel que $O = A \cap \Omega$.
2. Une partie F de A est fermée pour d_A si et seulement si il existe $G \subset X$ fermé tel que $F = A \cap G$.

Preuve

1. (\Leftarrow) Soit $a \in A \cap \Omega$. Puisque Ω est ouvert dans X , il existe $r > 0$ tel que $B(a, r) \subset \Omega$. Donc $B_{d_A}(a, r) = B(a, r) \cap A \subset \Omega \cap A$. $O = A \cap \Omega$ est donc ouvert.
 (\Rightarrow) Soit $a \in O$. Il existe $r_a > 0$ tel que $B_{d_A}(a, r_a) \subset O$. On a donc

$$O = \bigcup_{a \in O} B_{d_A}(a, r_a) = \bigcup_{a \in O} (B(a, r_a) \cap A) = \underbrace{\left(\bigcup_{a \in O} B(a, r) \right)}_{\Omega} \cap A$$

Ω est une union d'ouverts, donc est un ouvert de X , ce qui nous permet de conclure.

2. Il suffit d'utiliser le résultat précédent en passant au complémentaire.

(\Leftarrow) Si $F = A \cap G$, alors $A \setminus F = A \cap \underbrace{(X \setminus G)}_{\Omega}$. Ω est ouvert, donc en appliquant la propriété précédente, $A \setminus F$ est ouvert pour d_A et donc F est fermé pour d_A .

(\Rightarrow) Si F est fermé pour la distance d_A , alors $A \setminus F$ est ouvert pour cette distance. D'après ce qui précéde, il existe Ω un ouvert de X tel que $A \setminus F = \Omega \cap A$, ce qui donne $F = A \setminus (\Omega \cap A) = A \cap \underbrace{(X \setminus \Omega)}_G$.
 G est un fermé de X , ce qui nous permet de conclure.

Conséquences

- Tout ouvert de A est ouvert dans X si et seulement si A est ouvert dans X
- Tout fermé de A est fermé dans X si et seulement si A est fermé dans X .

IV Intérieur**Définition IV.1.**

Soit A une partie de X . On dit que le point $a \in A$ est intérieur à A lorsqu'il existe $\varepsilon > 0$ tel que $B(a, \varepsilon) \subset A$ (i.e. $A \in \mathcal{V}(a)$). On note $\overset{\circ}{A}$ ou $Int(A)$ l'ensemble des points intérieurs à A .

Exemples

- Dans \mathbb{R} , $\overset{\circ}{\mathbb{Q}} = \emptyset$ car $\mathbb{R} \setminus \mathbb{Q}$ est dense dans \mathbb{R} .
- Dans \mathbb{C} , $\overset{\circ}{\mathbb{R}} = \emptyset$.

Proposition IV.2.

Soit A une partie de X . $\overset{\circ}{A}$ est le plus grand ouvert inclus dans A .

Preuve : Si $a \in \overset{\circ}{A}$, alors il existe $\varepsilon > 0$ tel que $B(a, \varepsilon) \subset A$. $B(a, \varepsilon)$ est ouvert, donc pour tout $b \in B(a, \varepsilon)$, il existe $\eta > 0$ tel que $B(b, \eta) \subset B(a, \varepsilon) \subset A$. b est donc un élément de $\overset{\circ}{A}$ et alors $B(b, \eta) \subset \overset{\circ}{A}$. On peut donc conclure que $\overset{\circ}{A}$ est ouvert. Le fait que A soit le plus grand ouvert inclus dans A découle du fait que tout point appartenant à un ouvert inclus dans A est dans $\overset{\circ}{A}$ par définition de l'intérieur de A .

Exercice IV.3.

Soient A et B deux parties de X . Dans chaque cas, comparer les deux ensembles.

1. $\text{Int}(A \cap B)$ et $\text{Int}(A) \cap \text{Int}(B)$.
2. $\text{Int}(A \cup B)$ et $\text{Int}(A) \cup \text{Int}(B)$.

Exercice IV.4.

Soit E un espace vectoriel normé non réduit à $\{0\}$. Soit $(a, r) \in E \times \mathbb{R}_+^*$. Montrer que

$$\text{Int}(B_f(a, r)) = B(a, r)$$

Attention : cette propriété n'est pas toujours vraie quand on est pas dans le cadre d'espaces vectoriels normés. Par exemple, pour $X = \mathbb{Z}$ et d la distance induite par la valeur absolue, on a

- $B_f(0, 1) = \{-1, 0, 1\}$
- $B(0, 1) = \{0\} \neq \text{Int}(B_f(0, 1)) = \{-1, 0, 1\}$

V Adhérence**Définition V.1.**

Soit $b \in X$. On dit que b est adhérent à A lorsque

$$\forall \varepsilon > 0, B(b, \varepsilon) \cap A \neq \emptyset$$

On note \overline{A} l'ensemble des points adhérents à A .

Proposition V.2.

Soit A une partie de X . Les propriétés suivantes sont vérifiées.

1. \overline{A} est fermé.
2. \overline{A} est le plus petit fermé contenant A .
3. $X \setminus \overline{A} = \text{Int}(X \setminus A)$

Preuve

On a

$$\begin{aligned} x \notin \overline{A} &\iff \exists \varepsilon > 0, B(x, \varepsilon) \cap A = \emptyset \\ &\iff \exists \varepsilon > 0, B(x, \varepsilon) \subset X \setminus A \\ &\iff x \in \text{Int}(X \setminus A) \end{aligned}$$

Ceci montre le point 3 et le point 1 car $\text{Int}(X \setminus A)$ est ouvert. Montrons le deuxième point.

Soit B un fermé contenant A . $X \setminus A$ contient $X \setminus B$ qui est ouvert. $\text{Int}(X \setminus A)$ étant le plus grand ouvert inclus dans $X \setminus A$, $X \setminus B \subset \text{Int}(X \setminus A) = X \setminus \overline{A}$ et finalement $\overline{A} \subset B$. \overline{A} est donc bien le plus petit fermé contenant A .

Proposition V.3.

Soit $b \in X$ et A une partie de X . L'équivalence suivante est vraie.

$$b \in \overline{A} \iff \exists (a_n) \in A^{\mathbb{N}}, a_n \xrightarrow[n \rightarrow +\infty]{} b$$

Preuve

(\Leftarrow) Soit $\varepsilon > 0$. Il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $d(a_n, b) < \frac{\varepsilon}{2}$. (a_n) est à valeurs dans A donc $B(b, \varepsilon) \cap A \neq \emptyset$, donc $b \in \overline{A}$.

(\Rightarrow) Soit $b \in \overline{A}$. On va construire la suite (a_n) par récurrence. On prend a_0 égal à n'importe quel élément de X . Soit $n \in \mathbb{N}$. Supposons a_0, \dots, a_n bien définis. b étant adhérent à A , on a $B(b, \frac{1}{n+1}) \cap A \neq \emptyset$. On peut donc prendre $a_{n+1} \in B(b, \frac{1}{n+1}) \cap A$. On a alors par construction,

$$\forall n \in \mathbb{N}^*, d(a_n, b) \leq \frac{1}{n} \text{ et } (a_n) \in A^{\mathbb{N}}$$

et alors $a_n \xrightarrow[n \rightarrow +\infty]{} b$.

Corollaire V.4.

Soit $A \subset X$. L'équivalence suivante est vraie

$$A \text{ fermé} \iff (\forall (a_n) \in A^{\mathbb{N}}, a_n \xrightarrow[n \rightarrow +\infty]{} l \implies l \in A)$$

Preuve : d'après ce qui précéde, on a

$$A \text{ fermé} \iff A = \overline{A} \iff (\forall (a_n) \in A^{\mathbb{N}}, a_n \xrightarrow[n \rightarrow +\infty]{} l \implies l \in A)$$

Exercice V.5.

Trouver un ensemble $A \subset \mathbb{R}$ tel que $A, \overline{A}, \mathring{A}, \mathring{\overline{A}}, \overline{\mathring{A}}$ et $\mathring{\overline{A}}$ soient deux à deux distincts.

Exercice V.6.

Soit E un espace vectoriel normé et $(a, r) \in E \times \mathbb{R}_+^*$. Montrer que

$$\overline{B(a, r)} = B_f(a, r)$$

Exercice V.7.

Soit C un partie convexe d'un espace vectoriel normé E .

1. Montrer que \overline{C} et \mathring{C} sont convexes.
2. Soit $a \in \mathring{C}$ et $b \in \overline{C}$. Montrer que $[a, b] \subset \mathring{C}$.

Exercice V.8.

On pose $E = \mathcal{C}([0, 1], \mathbb{R})$ et $F = \{f \in E, \forall x \in [0, 1] f(x) \geq 0\}$.

1. Montrer que F est un fermé pour $\|\cdot\|_\infty$ et $\|\cdot\|_1$.
2. Donner $\overset{\circ}{F}$ pour $\|\cdot\|_\infty$ et $\|\cdot\|_1$.

VI Densité**Définition VI.1.**

Soient A et B deux parties de X . On dit que B est dense dans A lorsque $A \subset \overline{B}$. De même, on dit que B est partout dense dans X lorsque $\overline{B} = X$.

Exemples

- \mathbb{Q} et $\mathbb{R} \setminus \mathbb{Q}$ sont denses dans \mathbb{R} .
- Pour tout $n \in \mathbb{N}$, \mathbb{Q}^n est dense dans \mathbb{R}^n pour les normes usuelles ($\|\cdot\|_1, \|\cdot\|_2, \|\cdot\|_\infty, \dots$).

Proposition VI.2.

Soient A et B deux parties de X . Les propositions suivantes sont équivalentes.

1. B est dense dans A
2. Pour tout élément $a \in A$, il existe une suite (b_n) à valeurs dans B qui converge vers a .
3. Pour tout $a \in A$ et $\varepsilon > 0$, il existe $b \in B$ tel que $b \in B(x, \varepsilon)$.

Remarque : Ces caractérisations de la densité sont quelques fois plus commode à utiliser en exercice.

Proposition VI.3.

La propriété de densité est transitive, i.e. si A , B et C sont trois parties de X et si B est dense dans A et C est dense dans B alors C est dense dans A .

Exemple : si E est un espace vectoriel normé et F est un sous espace stricte de E (i.e. $F \neq E$), alors $E \setminus F$ est dense dans E .

Montrons ce résultat. Soit $x \notin F$ et $a \in F$. Soit $\varepsilon > 0$. On a $a + \varepsilon \frac{x}{2\|x\|} \in F \setminus E$ (car sinon, on aurait $a + \varepsilon \frac{x}{2\|x\|} - a \in F$, i.e. $x \in F$). De plus $a + \varepsilon \frac{x}{2\|x\|} \in B(a, \varepsilon)$ et alors $B(a, \varepsilon) \cap (E \setminus F) \neq \emptyset$.

On a montré que $F \subset \overline{F \setminus E}$. On a aussi $E \setminus F \subset \overline{F \setminus E}$. On en déduit donc que $\overline{E \setminus F} = E$, i.e. $E \setminus F$ est dense dans E .

Remarque : le résultat montré ci dessus peut être aussi formulé de la manière suivante :

$$A \text{ est un sous espace vectoriel de } E \text{ et } \overset{\circ}{A} \neq \emptyset \iff A = E$$

ou encore :

Si F est un sous espace stricte d'un espace vectoriel normé E , alors F est d'intérieur vide

Cette propriété se voit facilement en dimension 3 par exemple. Un sous espace stricte de \mathbb{R}^3 est soit un plan, soit une droite, ou alors un point qui dans tous les cas sont d'intérieur vide.

Conséquence : Si H est un hyperplan de E , alors soit H est fermé soit H est dense dans E . En effet, on a $H \subset \overline{H} \subset E$ donc soit $H = \overline{H}$, i.e. H est fermé, soit $\overline{H} = E$, i.e. H est dense dans E .

Exemple : l'hyperplan $H = \{f \in \mathcal{C}([0, 1], \mathbb{R}), f(0) = 0\}$ n'est pas fermé pour la distance induite par $\|\cdot\|_1$ car il est dense dans $\mathcal{C}([0, 1], \mathbb{R})$.

En effet, si $f \in \mathcal{C}([0, 1], \mathbb{R})$, on considère $g \in H$ la fonction définie par

$$g(x) = \begin{cases} \frac{x}{\varepsilon} f(\varepsilon) & \text{si } x \in [0, \varepsilon[\\ f(x) & \text{si } x \in [\varepsilon, 1] \end{cases}$$

Pour montrer que cet exemple est naturel, voici un dessin de la courbe de g à droite et celle de f à gauche



Montrons que g est proche de f . On a

$$\begin{aligned} \|f - g\|_1 &= \int_0^1 |f(x) - g(x)| dx \\ &= \int_0^\varepsilon |f(x) - g(x)| dx \leq 2 \|f\|_\infty \varepsilon \end{aligned}$$

donc quitte à remplacer ε par $\frac{\varepsilon}{4\|f\|_\infty}$, on peut dire que $g \in B(f, \varepsilon)$ et donc H est dense dans $\mathcal{C}([0, 1], \mathbb{R})$ pour la distance induite par $\|\cdot\|_1$.

Exercice VI.4.

Soit G un sous groupe additif de \mathbb{R} . On note $A = \{x \in G, x > 0\}$.

1. Montrer que si $G \neq \{0\}$, alors A est non vide. On pose alors $a = \inf A$.
2. Montrer que si $a = 0$, alors G est dense dans \mathbb{R} .
3. Montrer que si $a > 0$, alors $G = a\mathbb{Z}$.
4. Application 1 : en utilisant ce qui précéde, montrer que $\{\cos n, n \in \mathbb{N}\}$ est dense dans $[-1, 1]$.
5. Application 2 : soit $f \in \mathcal{C}(\mathbb{R}, \mathbb{R})$ admettant 1 et $\sqrt{2}$ comme périodes. Montrer que f est constante.

Définition VI.5.

On dit que X est un espace séparable si et seulement si il existe un sous ensemble A de X dense dans X et dénombrable.

Exercice VI.6.

Montrer que X est séparable si et seulement si il existe une famille dénombrable d'ouverts $(\Omega_i)_{i \in I}$ telle que pour tout ouvert O de X $\exists J \subset I$, $O = \bigcup_{j \in J} \Omega_j$.

Définition VI.7.

Soit A une partie de X . Un point $a \in X$ est dit

→ isolé lorsque

$$\exists \varepsilon > 0, B(a, \varepsilon) \cap A = \{a\}$$

→ d'accumulation lorsque

$$\forall \varepsilon > 0, (B(a, \varepsilon) \setminus \{a\}) \cap A \neq \emptyset$$

L'ensemble des points d'accumulation et isolés de A sont respectivement notés A^{aci} et A^i .

Notation : On note A^{aci} l'ensemble des points d'accumulation de A qui sont dans A .

Proposition VI.8.

Soit A une partie de X .

1. $A^{aci} \cup A^i = A$
2. $a \in A^{aci} \iff \forall \varepsilon > 0, B(a, \varepsilon) \cap A$ est infini
3. $a \in A^{aci} \iff$ il existe une suite injective à valeurs dans A qui converge vers a

Preuve

1. En regardant les définitions d'un point isolé et d'un point d'accumulation, on peut aisément remarquer que le fait qu'un point soit isolé est exactement la négation du fait qu'un point soit d'accumulation, donc naturellement, un point a de A est soit d'accumulation, soit isolé, d'où le fait que $A^{aci} \cup A^i = A$.
2. (\Rightarrow) Supposons que $a \in A^{aci}$. Supposons de plus que $\exists \varepsilon > 0, B(a, \varepsilon) \cap A$ est fini. On pose donc $(B(a, \varepsilon) \setminus \{a\}) \cap A = \{x_1, \dots, x_p\}$ avec $p \in \mathbb{N}^*$. En posant $\tilde{\varepsilon} = \min\{d(a, x_i), i \in \llbracket 1; p \rrbracket\}$, il est facile de remarquer que $(B(a, \frac{\tilde{\varepsilon}}{2}) \setminus \{a\}) \cap A = \emptyset$, ce qui est en contradiction avec le fait que a soit un point d'accumulation.
(\Leftarrow) Si pour tout $\varepsilon > 0, B(a, \varepsilon) \cap A$ est infini, alors d'une manière évidente $(B(a, \varepsilon) \cap A) \setminus \{a\} = (B(a, \varepsilon) \setminus \{a\}) \cap A$ est non vide, donc a est un point d'accumulation.

3. (\Rightarrow) Supposons que $a \in A^{aci}$, i.e. $\forall \varepsilon > 0, B(a, \varepsilon) \cap A$ est infini.

Construisons une suite (x_n) qui vérifie la propriété voulue par récurrence. On définit x_0 comme un point pris au hasard dans A différent de a .

Soit $n \in \mathbb{N}$, supposons que x_n est bien défini. On prend alors x_{n+1} dans $B(a, \frac{1}{2} \min(\frac{1}{n+2}, d(a, x_n))) \cap A$ (c'est possible car cet ensemble est non vide). Par construction (x_n) est injective et pour tout $n \in \mathbb{N}^*$ $d(x_n, a) \leq \frac{1}{n+1}$ et donc $x_n \xrightarrow{n \rightarrow +\infty} a$, d'où le résultat voulu.

(\Leftarrow) Supposons l'existence d'une telle suite qu'on note (x_n) . Soit $\varepsilon > 0$. Supposons que $B(a, \varepsilon) \cap A$ est fini. Il existe alors $p \in \mathbb{N}^*$ tel que $(B(a, \varepsilon) \setminus \{a\}) = \{x_1, \dots, x_p\}$. En posant $\tilde{\varepsilon} = \min\{d(a, x_i), i \in \llbracket 1; p \rrbracket\}$, il est facile de remarquer que $(B(a, \frac{\tilde{\varepsilon}}{2}) \setminus \{a\}) \cap A = \emptyset$, ce qui est absurde car pour n assez grand, x_n est dans $(B(a, \frac{\tilde{\varepsilon}}{2}) \setminus \{a\}) \cap A$.

Proposition VI.9.

En dimension finie, tout ensemble borné infini admet un point d'accumulation.

Correction de l'exercice II.4. :

Soit $a \in X$. Le fait que a ne soit pas une valeur d'adhérence de (u_n) est équivalent au fait qu'il existe $\varepsilon > 0$ tel que $B(a, \varepsilon) \cap \{u_n, n \in \mathbb{N}\}$ soit fini. Soit $b \in B(a, \varepsilon)$. Posons $\eta = \frac{\varepsilon - d(a, b)}{2}$. La boule $B(b, \eta)$ est incluse dans $B(a, \varepsilon)$ et donc $B(b, \eta) \cap \{u_n, n \in \mathbb{N}\}$ est fini car inclus dans $B(a, \varepsilon) \cap \{u_n, n \in \mathbb{N}\}$. Donc $b \in X \setminus \text{Adh}(u_n)$, et alors $B(a, \varepsilon) \subset X \setminus \text{Adh}(u_n)$ ce qui donne finalement que $X \setminus \text{Adh}(u_n)$ soit ouvert i.e. $\text{Adh}(u_n)$ est fermé.

Correction de l'exercice II.5. :

Soit $(u_n) \in A$. Posons $\varepsilon = \min\{|u_0|, \dots, |u_N|\}$. Montrons que $B((u_n), \frac{\varepsilon}{2}) \subset A$. Soit $(v_n) \in B((u_n), \frac{\varepsilon}{2})$. Pour tout $i \in \llbracket 0; N \rrbracket$, on a

$$|u_i - v_i| \leq \sum_{k=0}^{+\infty} |u_k - v_k| < \frac{\varepsilon}{2}$$

donc

$$0 < |u_i| - \frac{\varepsilon}{2} \leq |v_i|$$

ce qui nous donne que pour tout $i \in \llbracket 0; N \rrbracket$, $v_i \neq 0$ et alors $(v_n) \in A$, donc $B((u_n), \frac{\varepsilon}{2}) \subset A$. A est donc ouvert.

Correction de l'exercice II.6. :

On se place dans l'espace vectoriel normé $E = \mathcal{C}([0, 1], \mathbb{R})$.

1. Etudions $O = \{f \in E, \forall x \in [0, 1], f(x) > 0\}$.

(a) O est ouvert pour la distance induite par $\|\cdot\|_\infty$.

En effet, si on considère $f \in O$, alors on a $\varepsilon = \min_{x \in [0, 1]} f(x) > 0$.

Soit $g \in B(f, \frac{\varepsilon}{2})$, alors

$$\|g - f\|_\infty \leq \frac{\varepsilon}{2}$$

et alors

$$\forall x \in [0, 1], |g(x)| \geq |f(x)| - \frac{\varepsilon}{2} \geq \frac{\varepsilon}{2} > 0$$

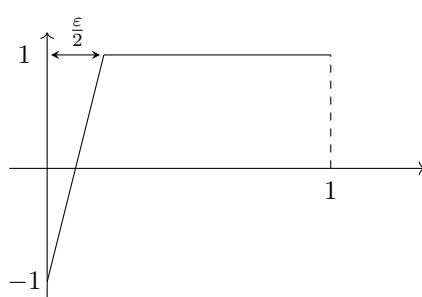
donc $g \in O$ et alors $B(f, \frac{\varepsilon}{2}) \subset O$. D'où le fait que O soit ouvert pour $\|\cdot\|_\infty$.

- (b) O n'est pas ouvert pour la distance induite par $\|\cdot\|_1$.

Exhibons un contre-exemple qui permet d'affirmer cela. Soit $\varepsilon > 0$, considérons la fonction f partout égale à 1 sur $[0, 1]$, et g une fonction de E définie de la manière suivante :

$$g(x) = \begin{cases} \frac{4x}{\varepsilon} - 1 & \text{si } x \in [0, \frac{\varepsilon}{2}[\\ 1 & \text{si } x \in [\frac{\varepsilon}{2}, 1] \end{cases}$$

Pour rendre ce choix plus parlant, voici un dessin de la fonction g :



On a alors

$$\begin{aligned}\|f - g\|_1 &= \int_0^1 |f(x) - g(x)| dx \\ &= \int_0^{\frac{\varepsilon}{2}} \left| \frac{4x}{\varepsilon} - 2 \right| dx \\ &= \left[2x - \frac{2x^2}{\varepsilon} \right]_0^{\frac{\varepsilon}{2}} \\ &= \frac{\varepsilon}{2}\end{aligned}$$

donc $g \in B(f, \varepsilon)$ mais $g \notin O$. On en déduit que O n'est pas ouvert pour la distance induite par $\|\cdot\|_1$.

2. Etudions $F = \{f \in E, \forall x \in [0, 1], f(x) \geq 0\}$.

- (a) F est fermé pour la distance induite par $\|\cdot\|_\infty$.

Pour montrer cela, on va montrer que $E \setminus F = \{f \in E, \exists x \in [0, 1], f(x) < 0\}$ est ouvert.

Soit $f \in E \setminus F$. Soit $a \in [0, 1]$ tel que $f(a) < 0$. On pose $\varepsilon = \frac{|f(a)|}{2}$. Montrons que $B(f, \varepsilon) \subset E \setminus F$. soit $g \in B(f, \varepsilon)$, on a

$$\|g - f\|_\infty < \varepsilon$$

et donc

$$g(a) \leq f(a) + \varepsilon < 0$$

on a alors $g \in B(f, \varepsilon)$ et donc $B(f, \varepsilon) \subset E \setminus F$. On en déduit finalement que $E \setminus F$ est ouvert, i.e. F est fermé pour la distance induite par $\|\cdot\|_\infty$.

- (b) F est fermé pour la distance induite par $\|\cdot\|_1$.

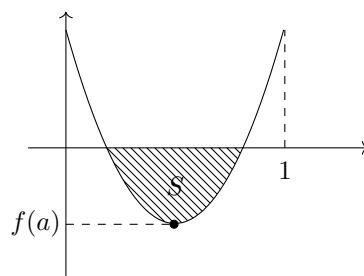
On va procéder de la même manière qu'avant. Soit $f \in E \setminus F$. Soit $a \in [0, 1]$ tel que $f(a) < 0$.

Par continuité de f , il existe $\eta > 0$ tel que pour tout $x \in [a - \eta, a + \eta]$, $f(x) < \frac{f(a)}{2}$. Donc pour tout $g \in F$,

$$\begin{aligned}\|f - g\|_1 &= \int_0^1 |f(x) - g(x)| dx \\ &\geq \int_{a-\eta}^{a+\eta} |f(x) - g(x)| dx \\ &\geq - \int_{a-\eta}^{a+\eta} f(x) dx \\ &\geq -\eta f(a)\end{aligned}$$

En prenant donc $\varepsilon = -\eta f(a)$, on a $B(f, \varepsilon) \subset E \setminus F$ et donc $E \setminus F$ est ouvert, i.e. F est fermé pour la distance induite par $\|\cdot\|_1$.

Pour comprendre un peu ce qui se passe, considérons le cas où f est décrite par la courbe ci-dessous :



La distance en norme 1 entre f et une fonction partout positive ou nulle va être au moins égale à la surface S hachurée sur la figure. Ici, on a minoré cette surface par $-\eta f(a)$ ce qui nous a permis de trouver une boule incluse dans $E \setminus F$ de centre f .

Correction de l'exercice IV.3. :

1. On a $\text{Int}(A \cap B) = \text{Int}(A) \cap \text{Int}(B)$.

Montrons ce résultat. Soit $x \in X$.

(\subset) Supposons que $x \in \text{Int}(A \cap B)$. On dispose alors de $r > 0$ tel que $B(x, r) \subset A \cap B$, i.e. $B(x, r) \subset A$ et $B(x, r) \subset B$ et donc $x \in \text{Int}(A)$ et $x \in \text{Int}(B)$. On a alors $x \in \text{Int}(A) \cap \text{Int}(B)$

(\supset) Supposons que $x \in \text{Int}(A) \cap \text{Int}(B)$. On dispose alors de $r_A > 0$ et $r_B > 0$ tels que $B(x, r_A) \subset A$ et $B(x, r_B) \subset B$. En posant $r = \min\{r_A, r_B\} > 0$, on a $B(x, r) \subset A \cap B$ et finalement $x \in \text{Int}(A \cap B)$.

2. On a $\text{Int}(A) \cup \text{Int}(B) \subset \text{Int}(A \cup B)$.

Pour montrer ce résultat, on va commencer par supposer que $x \in \text{Int}(A) \cup \text{Int}(B)$. Sans perte de généralité, on suppose que $x \in \text{Int}(A)$, on dispose alors de $r > 0$ tel que $B(x, r) \subset A \subset A \cup B$, donc $x \in \text{Int}(A \cup B)$.

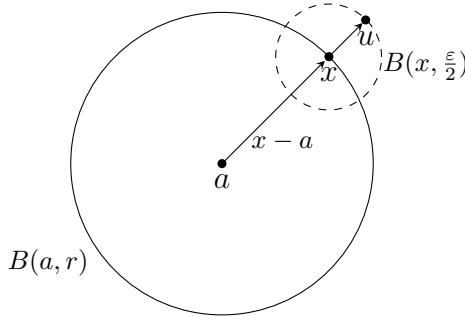
L'inclusion réciproque est fausse. Pour le voir, il suffit de prendre $A = \mathbb{Q}$ et $B = \mathbb{R} \setminus \mathbb{Q}$. On a $\text{Int}(\mathbb{Q}) = \text{Int}(\mathbb{R} \setminus \mathbb{Q}) = \emptyset$ et $\text{Int}((\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q}) = \mathbb{R} \not\subset \text{Int}(\mathbb{Q}) \cup \text{Int}(\mathbb{R} \setminus \mathbb{Q}) = \emptyset$.

Correction de l'exercice IV.4. :

On a $B(a, r) \subset B_f(a, r)$ et est ouvert, donc $B(a, r) \subset \text{Int}(B_f(a, r)) \subset B_f(a, r)$. Montrons l'inclusion réciproque. Pour cela, nous allons montrer que $\text{Int}(B_f(a, r)) \setminus B(a, r) = \emptyset$. Supposons le contraire, on dispose alors de $x \in \text{Int}(B_f(a, r)) \setminus B(a, r) \subset B_f(a, r) \setminus B(a, r)$. On a alors nécessairement $\|x - a\| = r$. Soit $\varepsilon > 0$ tel que $B(x, \varepsilon) \subset B_f(a, r)$, posons $u = x + \varepsilon \frac{x-a}{\|x-a\|}$. On a $u \in B(x, \varepsilon)$, mais

$$\begin{aligned}\|a - u\| &= \left\| a - x + \varepsilon \frac{x-a}{\|x-a\|} \right\| \\ &= \|x-a\| \left(1 + \frac{\varepsilon}{2\|x-a\|} \right) \\ &= \|x-a\| + \frac{\varepsilon}{2} \\ &= r + \frac{\varepsilon}{2} > r\end{aligned}$$

Ce qui est en contradiction avec le fait que $B(x, \varepsilon) \subset B_f(a, r)$. Donc finalement on a $\text{Int}(B_f(a, r)) = B(a, r)$. Pour comprendre l'intuition derrière le choix de u , jetons un coup d'œil au dessin ci-dessous.



On souhaite sortir de la boule $B(a, r)$, donc à partir de x , on va se déplacer vers la direction opposée à l'origine, d'où la présence du vecteur directeur unitaire $\frac{x-a}{\|x-a\|}$, mais on veut rester dans $B(x, \varepsilon)$, on va donc multiplier ce vecteur "déplacement" par $\frac{\varepsilon}{2}$.

Correction de l'exercice V.5. :

Il suffit de prendre $A = [0, 1] \cup]1, 2[\cup (]3, 4] \cap \mathbb{Q}) \cup \{5\}$.

En effet, on a

$$\rightarrow \mathring{A} =]0, 1] \cup]1, 2[$$

$$\rightarrow \overline{\mathring{A}} = [0, 2]$$

$$\rightarrow \bar{A} = [0, 2] \cup [3, 4] \cup \{5\}$$

$$\rightarrow \overset{\circ}{\bar{A}} =]0, 2[\cup]3, 4[$$

$$\rightarrow \overset{\circ}{\bar{A}} = [0, 2] \cup [3, 4]$$

$$\rightarrow \overset{\circ}{\bar{A}} =]0, 2[$$

Tous ces ensembles sont bien deux à deux distincts.

Correction de l'exercice V.6. :

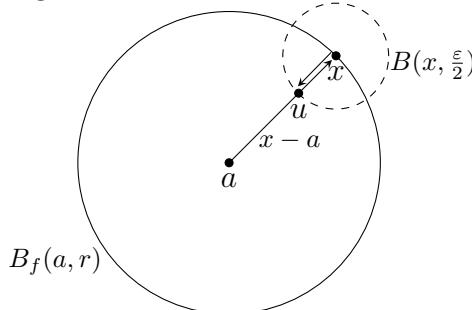
On va procéder d'une manière similaire à l'exercice 5. $\overline{B(a, r)}$ étant le plus petit fermé qui contient $B(a, r)$, on a $B(a, r) \subset \overline{B(a, r)} \subset B_f(a, r)$. Il reste donc à montrer l'inclusion réciproque.

Soit $x \in B_f(a, r) \setminus B(a, r)$. soit $\varepsilon > 0$, posons $u = x + \varepsilon \frac{a-x}{2\|a-x\|}$. On a

$$\begin{aligned}\|a - u\| &= \left\|a - x - \varepsilon \frac{a-x}{2\|a-x\|}\right\| \\ &= \|a - x\| \left(1 - \frac{\varepsilon}{2\|a-x\|}\right) \\ &= \|a - x\| - \frac{\varepsilon}{2} \\ &= r - \frac{\varepsilon}{2} < r\end{aligned}$$

On suppose bien sûr ici que ε est suffisemment petit pour que $r - \frac{\varepsilon}{2}$ soit positif. On a donc $u \in B(a, r)$ et de même on a $\|x - u\| = \frac{\varepsilon}{2}$, donc $u \in B(x, \varepsilon)$ ce qui montre enfin que $B_f(a, r) \subset \overline{B(a, r)}$ et finalement que $B_f(a, r) = \overline{B(a, r)}$.

Pour faire le lien avec l'exercice 5, regardons le dessin suivant.



Ici, au lieu de partir dans la direction du vecteur $x - a$, on va vers la direction opposée puisqu'on veut rester dans la boule $B(a, r)$. Mais on veut aussi être dans la boule $B(x, \varepsilon)$, on multiplie alors pour cela le vecteur directeur $\frac{a-x}{\|a-x\|}$ par $\frac{\varepsilon}{2}$.

Correction de l'exercice V.7. :

1. Montrons que \overline{C} et $\overset{\circ}{C}$ sont convexes.

→ Convexité de \overline{C}

Soit $x, y \in \overline{C}$. On dispose de deux suites $(x_n)_{n \in \mathbb{N}}$ et $(y_n)_{n \in \mathbb{N}}$ à valeurs dans C telles que

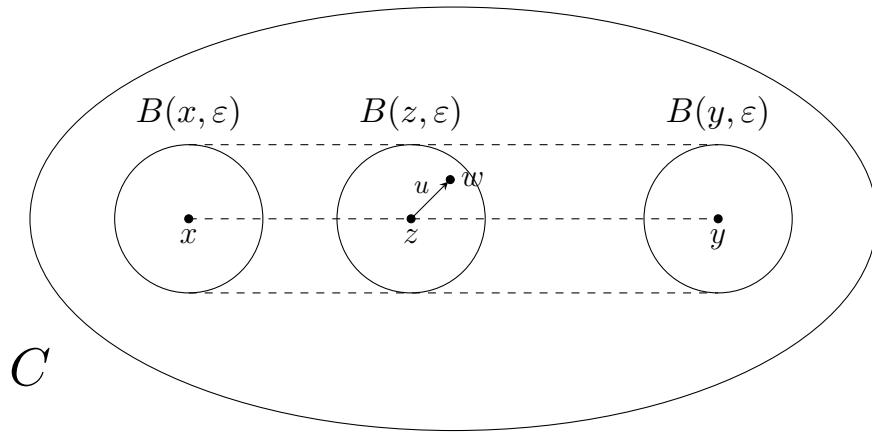
$$x_n \xrightarrow[n \rightarrow +\infty]{} x \text{ et } y_n \xrightarrow[n \rightarrow +\infty]{} y$$

Soit $\lambda \in [0, 1]$, on a $\lambda x_n + (1-\lambda)y_n \xrightarrow[n \rightarrow +\infty]{} \lambda x + (1-\lambda)y$, donc $\lambda x + (1-\lambda)y \in \overline{C}$ et finalement \overline{C} est convexe.

→ Convexité de $\overset{\circ}{C}$

Soit $x, y \in \overset{\circ}{C}$. On dispose de $\varepsilon > 0$ tel que $B(x, \varepsilon) \subset C$ et $B(y, \varepsilon) \subset C$ (quitte à prendre le

minimum des rayons des deux boules). Soit $\lambda \in [0, 1]$, montrons que $z = \lambda x + (1 - \lambda)y \in \overset{\circ}{C}$. Pour cela, regardons d'abord le dessin suivant.



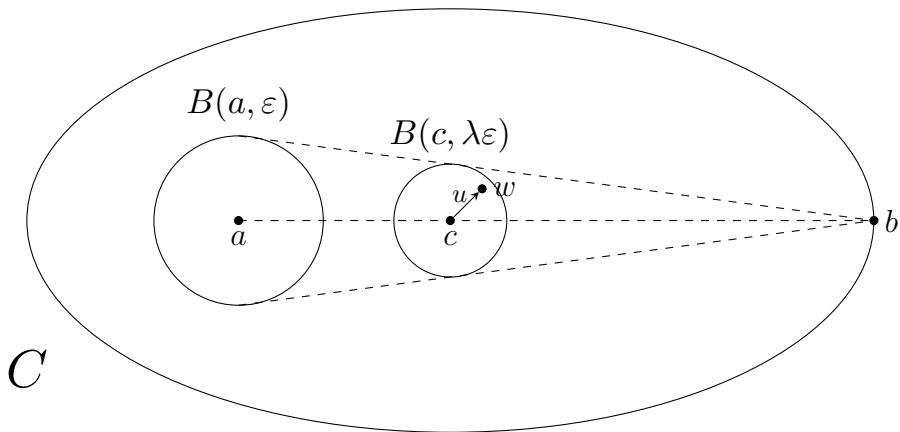
Le dessin ci-dessus suggère de montrer que $B(z, \varepsilon) \subset C$. Soit $w \in B(z, \varepsilon)$. Posons $u = w - z$, on a alors $w = z + u = \lambda(x + u) + (1 - \lambda)(y + u)$, et

$$\|x + u - x\| = \|w - z\| < \varepsilon \text{ et } \|y + u - y\| = \|w - z\| < \varepsilon$$

on a alors $y + u \in B(y, \varepsilon) \subset C$ et $x + u \in B(x, \varepsilon) \subset C$. Or w est combinaison linéaire convexe de $x + u$ et $y + u$, donc par convexité de C , $w \in C$ et alors $z \in \overset{\circ}{C}$ et finalement $\overset{\circ}{C}$ est convexe.

2. Cette question est similaire à la question précédente. Soit $\lambda \in [0, 1]$. On pose $c = \lambda a + (1 - \lambda)b$. $a \in \overset{\circ}{C}$, donc on dispose de $\varepsilon > 0$ tel que $B(a, \varepsilon) \subset C$. Si $\lambda = 0$, il n'y a rien à montrer puisque la question revient à montrer que $\emptyset \subset C$, on considère dorénavant donc que $\lambda \in]0, 1]$

→ Commençons par le cas $b \in C$. Observons le dessin suivant.



Le rayon de la boule du milieu peut être trouvé en utilisant des théorèmes de géométrie élémentaire (Thalès par exemple). Ce dessin suggère de montrer que $B(c, \lambda\varepsilon) \subset C$.

Soit $w \in B(c, \lambda\varepsilon)$, on pose $u = w - c$. On a alors $w = c + u = \lambda(a + \frac{u}{\lambda}) + (1 - \lambda)b$. Or

$$\left\| a + \frac{u}{\lambda} - a \right\| = \left\| \frac{w - c}{\lambda} \right\| < \varepsilon$$

donc $a + \frac{u}{\lambda} \in B(a, \varepsilon) \subset C$ et $b \in C$ et w est combinaison convexe de $a + \frac{u}{\lambda}$ et b , donc par convexité de C , $w \in C$ et alors $B(c, \lambda\varepsilon) \subset C$ et finalement $[a, b] \subset \overset{\circ}{C}$.

→ Passons au cas plus général où $b \in \overline{C}$.

On reprend les notations du cas où $b \in C$, et on considère une suite (b_n) à valeurs dans C qui tends vers b . Posons pour tout $n \in \mathbb{N}$, $c_n = \lambda a + (1 - \lambda)b_n$. La preuve du cas $b \in C$ nous permet

d'affirmer que $B(c_n, \lambda\varepsilon) \subset C$. On a alors

$$\begin{aligned}\|w - c_n\| &= \|w - c + c - c_n\| \\ &\leq \|w - c\| + \|c - c_n\| \xrightarrow{n \rightarrow +\infty} \|w - c\| < \lambda\varepsilon\end{aligned}$$

on peut alors affirmer l'existence de $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $\|w - c_n\| < \lambda\varepsilon$ et donc $w \in B(c_n, \lambda\varepsilon) \subset C$. Ceci nous permet de dire que $B(c, \lambda\varepsilon) \subset C$ et que $c \in \overset{\circ}{C}$. Finalement on conclut que $[a, b] \subset \overset{\circ}{C}$.

L'intuition derrière le passage au cas où $b \in \overline{C}$ était de prendre n assez grand pour que la boule $B(c_n, \lambda\varepsilon) \subset C$ soit quasi-confondue avec $B(c, \lambda\varepsilon)$ pour dire que tous les points de $B(c, \lambda\varepsilon)$ sont dans C .

Correction de l'exercice V.8. :

1. Cette question a été déjà faite dans la correction de l'exercice 3.
2. Trouvons $\overset{\circ}{F}$ pour $\|\cdot\|_1$ et $\|\cdot\|_\infty$.

→ Pour $\|\cdot\|_\infty$

On pose $O = \{f \in E, \forall x \in E, f(x) > 0\}$. On a d'après l'exercice 3, O est ouvert et $O \subset F$, donc $O \subset \overset{\circ}{F}$. Il reste donc à voir si $(F \setminus O) \cap \overset{\circ}{F} = \emptyset$.

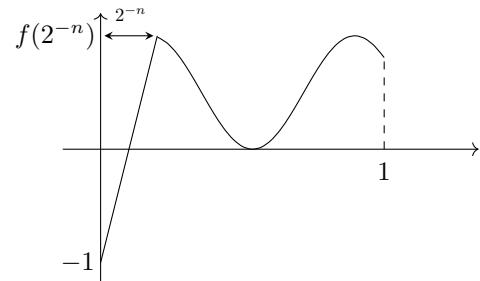
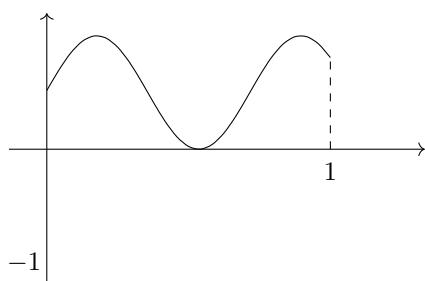
Soit $f \in F \setminus O$ et soit $\varepsilon > 0$. Le fait que $f \in F \setminus O$ implique $\exists a \in [0, 1], f(a) = 0$. En considérant $g = f - \frac{\varepsilon}{2}$, on peut voir immédiatement que $g \notin F$ (car $g(a) = -\frac{\varepsilon}{2} < 0$) et $g \in B(f, \varepsilon)$. Donc $f \notin \overset{\circ}{F}$ et finalement $\overset{\circ}{F} = O$.

→ Pour $\|\cdot\|_1$

Soit $f \in F$. On considère la suite de fonctions $(g_n)_{n \in \mathbb{N}}$ définie sur $[0, 1]$ pour tout $n \in \mathbb{N}$ par

$$g(x) = \begin{cases} \frac{x}{2^{-n}}(f(2^{-n}) + 1) - 1 & \text{si } x \in [0, 2^{-n}[\\ f(x) & \text{si } x \in [2^{-n}, 1] \end{cases}$$

Voici un dessin d'un terme de cette suite de fonctions à droite et de la courbe de f à gauche.



Bien sûr, pour tout $n \in \mathbb{N}$, g_n est bien une fonction continue sur $[0, 1]$. Il s'agit de la même idée que la question 1 de l'exercice 3 où on a montré que O n'est pas ouvert, sauf que la fonction considérée est f au lieu d'une fonction qui est identiquement égale à 1 à laquelle on a ajouté une petite perturbation au voisinage de 0, qui fait sortir g_n de F sans trop s'éloigner de f . On

a pour tout $n \in \mathbb{N}$, $g_n(0) = -1$, donc (g_n) est valeurs dans $E \setminus F$. De plus, on a

$$\begin{aligned}\|f - g_n\|_1 &= \int_0^1 |f(x) - g_n(x)| dx \\ &= \int_0^{2^{-n}} |f(x) - g_n(x)| dx \\ &\leq 2^{-n} (\|f\|_\infty + \|g_n\|_\infty) \\ &= 2^{-n} (\|f\|_\infty + \max\{1, f(2^{-n})\}) \\ &\leq 2^{-n} (\|f\|_\infty + \max\{1, \|f\|_\infty\}) \xrightarrow{n \rightarrow +\infty} 0\end{aligned}$$

Donc pour tout $\varepsilon > 0$, $B(f, \varepsilon) \not\subset F$. On conclut que $\mathring{F} = \emptyset$.

Correction de l'exercice VI.4. :

1. Supposons que $G \neq \{0\}$ et que A est vide. Alors nécessairement, on dispose de $x \in G$ tel que $x < 0$. Or $-x \in G$ et $-x > 0$ donc $-x \in A$ ce qui est absurde.
2. Supposons que $a = 0$. Soit $x \in \mathbb{R}$. Etant donné que $\inf A = 0$, A contient des éléments aussi petits qu'on veut. Soit $\varepsilon > 0$, on dispose donc de $\theta \in A$ tel que $\theta < \varepsilon$. Or, pour tout $n \in \mathbb{Z}$, $n\theta \in G$. On a alors

$$\left| x - \left\lfloor \frac{x}{\theta} \right\rfloor \theta \right| = \left(\frac{x}{\theta} - \left\lfloor \frac{x}{\theta} \right\rfloor \right) \theta \leq \theta < \varepsilon$$

et $\left\lfloor \frac{x}{\theta} \right\rfloor \theta \in G$, donc on a trouvé un élément de G aussi proche qu'on veut de x , ce qui signifie que G est dense dans \mathbb{R} .

3. Supposons que $a > 0$.

→ Montrons d'abord que $a \in G$.

Supposons par l'absurde que $a \notin G$. On dispose alors de $b, c \in A$ tels que $b > c$ et $|b - a| \leq \frac{a}{4}$ et $|c - a| \leq \frac{a}{4}$. Donc on a

$$\begin{aligned}b - c &= |b - a + a - c| \\ &\leq |b - a| + |a - c| \leq \frac{a}{2}\end{aligned}$$

or $b - c \in A$, donc on a

$$a < b - c \leq \frac{a}{2}$$

ce qui est absurde, donc $a \in G$.

→ Montrons ensuite que $G = a\mathbb{Z}$.

Par stabilité par addition et soustraction, on a évidemment $a\mathbb{Z} \subset G$.

Supposons que $G \neq a\mathbb{Z}$. On dispose donc de $x \in G \setminus a\mathbb{Z}$. Quitte à passer à l'opposé, on suppose que $x > 0$. On a alors

$$0 < x - \left\lfloor \frac{x}{a} \right\rfloor a = a \left(\frac{x}{a} - \left\lfloor \frac{x}{a} \right\rfloor \right) < a$$

Donc $x - \left\lfloor \frac{x}{a} \right\rfloor a \in A$ et $x - \left\lfloor \frac{x}{a} \right\rfloor a < a$ ce qui est absurde. On en déduit donc que $G = a\mathbb{Z}$.

4. Commençons par remarquer que par parité du cos, $\{\cos(n), n \in \mathbb{N}\} = \{\cos(n), n \in \mathbb{Z}\}$.

→ Montrons d'abord que $G = \mathbb{Z} + 2\pi\mathbb{Z}$ est dense dans \mathbb{R} .

G est un sous groupe additif de \mathbb{R} . Supposons qu'il existe $a \in \mathbb{R}^*$ tel que $G = a\mathbb{Z}$. Il existe alors $n, m \in \mathbb{Z}^*$ tel que $1 = an$ et $2\pi = am$, donc, $\frac{2\pi}{1} = \frac{an}{am}$, i.e. $\pi = \frac{n}{2m}$ ce qui implique que π est rationnel, absurde. Donc d'après les questions précédentes, G est dense dans \mathbb{R} .

→ Montrons à présent que $\{\cos(n), n \in \mathbb{N}\}$ est dense dans \mathbb{R} .

On a

$$B = \{\cos(n), n \in \mathbb{N}\} = \{\cos(n), n \in \mathbb{Z}\} = \{\cos(n), n \in G\}$$

Soit $x \in [-1, 1]$ et y un antécédant de x par \cos . G étant dense dans \mathbb{R} , on dispose d'une suite (y_n) à valeurs dans G qui tend vers y . Donc la suite $(\cos(y_n))$ est à valeurs dans B et tend vers x par continuité du cos. On en déduit donc que $\{\cos(n), n \in \mathbb{N}\}$ est bien dense dans $[-1, 1]$.

5. Commençons par remarquer que $f(\mathbb{Z} + \sqrt{2}\mathbb{Z}) = \{f(1)\}$ par périodicité de f . $\sqrt{2}$ étant irrationnel, on peut montrer comme on l'a fait pour $\mathbb{Z} + 2\pi\mathbb{Z}$ que $H = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ est dense dans \mathbb{R} . Soit $x \in \mathbb{R}$, on dispose d'une suite (x_n) à valeurs dans H telle que (x_n) converge vers x . On a donc par continuité de f

$$f(1) = f(x_n) \xrightarrow{n \rightarrow +\infty} f(x)$$

On en déduit donc que f est constante égale à $f(1)$.

Correction de l'exercice VI.6. :

(\Leftarrow) Supposons que pour tout i , $\Omega_i \neq \emptyset$ et considérons pour tout i , a_i un élément de Ω_i .

Posons $A = \{a_i, i \in I\}$, c'est un ensemble dénombrable. Montrons que A est dense dans X . Soit $x \in X$ et $\varepsilon > 0$. Par hypothèse, il existe $J \subset I$ tel que $B(x, \varepsilon) = \bigcup_{i \in J} \Omega_i$, il suffit donc de prendre $i \in J$ pour voir que a_i est dans $B(x, \varepsilon) \cap A$. D'où la densité de A dans X .

(\Rightarrow) Soit $A = \{a_i, i \in \mathbb{N}\}$ une partie dénombrable dense de X . Considérons la famille d'ouverts $(\Omega_{n,m})_{n,m \in \mathbb{N}} = (B(a_n, \frac{1}{m+1}))_{n,m \in \mathbb{N}}$ et montrons qu'elle vérifie la propriété voulue.

Soit O un ouvert de X . Considérons l'ensemble $J = \{(n, m) \in \mathbb{N}^2, B(a_n, \frac{1}{m+1}) \subset O\}$.

On a $\bigcup_{(n,m) \in J} \Omega_{n,m} \subset O$. Montrons l'inclusion réciproque. Soit $x \in O$. Comme A est dense dans X , il existe $a_n \in A$ (avec $n \in \mathbb{N}$) et $m \in \mathbb{N}$ arbitrairement grand tel que $x \in B(a_n, \frac{1}{m+1})$. On prend alors m assez grand pour qu'on ait $B(a_n, \frac{1}{m+1}) \subset O$, i.e. $(n, m) \in J$ ce qui nous donne $x \in \bigcup_{(m,n) \in J} \Omega_{n,m}$.

On a donc bien obtenu le résultat voulu.



CHAPITRE 11.3

Limites et continuité

Dans tout ce chapitre, on considère X et Y deux espaces métriques respectivement munis des distances d et δ , A une partie de X , $a \in \overline{A}$ et f une fonction de A dans Y .

I Limites

Définition I.1.

On dit que f admet une limite en a selon A lorsqu'il existe $l \in Y$ tel que

$$\forall V \in \mathcal{V}(l), \exists U \in \mathcal{V}(a), f(U \cap A) \subset V (*)$$

Remarques

→ une formulation équivalente à la définition ci-dessous est la suivante.

f admet une limite en a selon A s'il existe $l \in Y$ tel que

$$\forall \varepsilon > 0, \exists \eta > 0, \forall x \in A, d(a, x) < \eta \implies \delta(f(x), l) < \varepsilon$$

→ La propriété (*) est équivalente à

$$\forall V \in \mathcal{V}(l), f^{-1}(V) \cap A \in \{U \cap A, U \in \mathcal{V}(a)\}$$

Proposition I.2.

1. Si f tends vers l et l' , alors $l = l'$.
2. Si f admet une limite l en a selon A et $a \in A$, alors nécessairement $f(a) = l$.
3. Si f admet une limite en a selon A , elle est bornée au voisinage de a (dans A).

Preuve

1. Soit $l, l' \in Y$ telles que f tends vers l et l' en a selon A . Supposons que $l \neq l'$. Appliquons la définition de limite avec $\varepsilon = \frac{\delta(l, l')}{10}$. Il existe $\eta, \eta' > 0$ tel que
 - $\forall x \in A, d(a, x) < \eta \implies \delta(f(x), l) < \frac{\delta(l, l')}{10}$
 - $\forall x \in A, d(a, x) < \eta' \implies \delta(f(x), l') < \frac{\delta(l, l')}{10}$
 On a alors pour tout $x \in A$ tel que $d(x, a) < \min(\eta, \eta')$

$$\delta(l, l') < \delta(f(x), l) + \delta(f(x), l') < \frac{\delta(l, l')}{5}$$

ce qui est absurde et finalement $l = l'$.

2. Si a admet une limite en a selon A , alors $\forall \varepsilon > 0, \exists \eta > 0, \forall x \in A, d(x, a) < \eta \implies \delta(f(x), l) < \varepsilon$. Or pour tout $\eta > 0$, $d(a, a) = 0 < \eta$, donc pour tout $\varepsilon > 0$, $d(f(a), l) < \varepsilon$ ce qui donne directement que $d(f(a), l) = 0$ et finalement $f(a) = l$.
3. Il suffit d'appliquer la définition avec $\varepsilon = 1$. En effet, il existe $\eta > 0$ tel que pour tout $x \in A$, $d(x, a) < \eta \implies \delta(f(x), l) < 1$. Ceci implique que $f(A \cap B(a, \eta)) \subset B(l, 1)$ qui est borné. $B(a, \eta)$ est un voisinage de a , donc f est bien bornée au voisinage de a dans A .

Proposition I.3.

Les propositions suivantes sont équivalentes

1. f possède une limite en a selon A .
2. Pour toute suite $(x_n) \in A^{\mathbb{N}}$ qui converge vers a , la suite $(f(x_n))$ converge.

Preuve

(1) \Rightarrow (2) Soit $(x_n) \in A^{\mathbb{N}}$ tel que $x_n \xrightarrow{n \rightarrow +\infty} a$.

Soit $\varepsilon > 0$. Il existe $\eta > 0$ tel que $\forall x \in B(a, \eta) \cap A$, $\delta(f(x), l) < \varepsilon$.

(x_n) converge vers a , il existe donc $N \in \mathbb{N}$ tel que $\forall n \geq N$, $d(x_n, a) < \eta$ et alors $\delta(f(x_n), l) < \varepsilon$.

On en déduit donc que $(f(x_n))$ converge vers l .

(2) \Rightarrow (1)

→ Montrons tout d'abord que toutes les suites de la forme $(f(x_n))$ avec (x_n) une suite à valeurs dans A convergeant vers a convergent vers une même limite l .

Soit (x_n) et (y_n) deux suites à valeurs dans A convergeant vers a . A partir de ces deux suites, on construit la suite (z_n) définie de la manière suivante : $\forall n \in \mathbb{N}$, $\begin{cases} z_{2n} = x_n \\ z_{2n+1} = y_n \end{cases}$

On a alors bien évidemment $z_n \xrightarrow{n \rightarrow +\infty} a$ et alors par hypothèse $f(z_n)$ converge vers une limite qu'on notera l . En considérant les deux suites extraites $(f(z_{2n+1})) = (f(y_n))$ et $(f(z_{2n})) = (f(x_n))$, on en déduit immédiatement que $(f(x_n))$ et $(f(y_n))$ admettent la même limite que $(f(z_n))$.

→ Il reste à montrer maintenant que la limite de f en a selon A est bien l .

Supposons que f ne converge pas vers l , i.e.

$$\exists \varepsilon > 0, \forall \eta > 0, \exists x \in B(a, \eta) \cap A, \delta(f(x), l) \geq \varepsilon$$

cette proposition peut être reformulée de la manière suivante

$$\exists \varepsilon > 0, \forall n \in \mathbb{N}, \exists x \in B\left(a, \frac{1}{n+1}\right) \cap A, \delta(f(x), l) \geq \varepsilon$$

On peut alors construire une suite (x_n) à valeurs dans A telle que pour tout $n \in \mathbb{N}$, $d(x_n, a) < \frac{1}{n+1}$ et $\delta(f(x_n), l) \geq \varepsilon$.

En résumé, on a

- (x_n) est une suite à valeurs dans A qui converge vers a .
- Pour tout n , $\delta(f(x_n), l) \geq \varepsilon$ donc $(f(x_n))$ ne peut pas tendre vers l .

ce qui est absurde par hypothèse.

Proposition I.4.

Soit B une partie de Y et Z un espace métrique. Si

- $a \in \overline{A}$ et f est une fonction de A dans Y qui admet une limite b en a selon A .
- $b \in \overline{B}$ et g est une fonction de B dans Z qui admet une limite l en b selon B
- $f(A) \subset B$

Alors $g \circ f$ admet la limite l en a selon A .

Preuve : soit $W \in \mathcal{V}(l)$.

- Il existe $V \in \mathcal{V}(b)$ tel que $g(V \cap B) \subset W$.
- Il existe $U \in \mathcal{V}(a)$ tel que $f(U \cap A) \subset V$.

On a aussi $f(U \cap A) \subset f(A) \subset B$, donc $f(U \cap A) \subset V \cap B$ et alors $g \circ f(U \cap A) \subset W$.
En résumé, on a montré que

$$\forall W \in \mathcal{V}(l), \exists U \in \mathcal{V}(a), g \circ f(U \cap A) \subset W$$

Attention : la condition $f(A) \subset B$ est nécessaire.

En effet, si on prend $A = \mathbb{R}^*$, $B = \mathbb{R}^*$, $Y = \mathbb{R}$, $Z = \mathbb{R}$ tous munis de la distance induite par la valeur absolue. On considère le cas où

- f est une fonction de A dans Y , définie par $\forall x \neq 0, f(x) = x \sin\left(\frac{1}{x}\right)$.
- g est une fonction de \mathbb{R} dans Z , définie par $\forall x \in \mathbb{R}, g(x) = 1_{x=0}$.

On a alors

- f admet une limite 0 en 0 selon $A = \mathbb{R}^*$.
- g admet une limite 0 en 0 selon $B = \mathbb{R}^*$
- $f(A) = f(\mathbb{R}^*)$ contient 0 donc $f(A) \not\subset \mathbb{R}^* = B$.

Mais $g \circ f$ n'admet pas de limite en 0 selon \mathbb{R}^* . En effet, si on considère les suites à valeurs dans \mathbb{R}^* , $(u_n)_{n \in \mathbb{N}} = \left(\frac{1}{2\pi n}\right)$ et $(v_n)_{n \in \mathbb{N}} = \left(\frac{1}{2\pi n + \frac{\pi}{2}}\right)$, on a

- $g \circ f(u_n) \xrightarrow[n \rightarrow +\infty]{} 1$.
- $g \circ f(v_n) \xrightarrow[n \rightarrow +\infty]{} 0$.

On en déduit donc que $g \circ f$ n'admet pas de limite en 0.

Exercice I.5.

Soit $f \in \mathcal{C}([-1, 1], \mathbb{R})$ telle que

$$\frac{f(x) - f\left(\frac{x}{2}\right)}{x} \xrightarrow[x \rightarrow 0]{} l \in \mathbb{R}$$

Montrer que f est dérivable en 0.

Exercice I.6.

Soit $f \in \mathcal{C}(\mathbb{R}, \mathbb{R})$ telle que

$$f(x+1) - f(x) \xrightarrow[x \rightarrow +\infty]{} L \in \mathbb{R}$$

Montrer que $x \mapsto \frac{f(x)}{x}$ admet une limite en $+\infty$.

II Continuité

Dans cette partie, on considère que l'ensemble de départ de f est X et que $a \in X$. Nous nous allons donc dire " f admet une limite l en a " au lieu de " f admet une limite l en a selon X " lorsqu'il n'y a pas ambiguïté.

1. Continuité locale

Proposition II.1.

Soit f une fonction de X dans Y . Les propositions suivantes sont équivalentes

1. f admet une limite en a .
2. $\forall V \in \mathcal{V}(f(a)), \exists U \in \mathcal{V}(a), f(U) \subset V$
3. $\forall \varepsilon > 0, \exists \eta > 0, \forall x \in X, d(a, x) < \eta \implies \delta(f(x), f(a)) < \varepsilon$

Lorsque f vérifie l'une de ces propriétés, on dit que f est continue en a .

Preuve

(1) \Rightarrow (2) Si f admet une limite en a selon X , alors nécessairement, d'après ce qui précéde, puisque $a \in X$, cette limite est égale à $f(a)$. Le point (2) est tout simplement l'application de la définition de limite pour $l = f(a)$.

(2) \Rightarrow (3) soit $\varepsilon > 0$. On considère le voisinage de $f(a)$, $B(f(a), \varepsilon)$. Par hypothèse, il existe $U \in \mathcal{V}(a)$ tel que $f(U) \subset B(f(a), \varepsilon)$. U étant un voisinage de a , il existe $\eta > 0$ tel que $B(a, \eta) \subset U$. et alors on a $f(B(a, \eta)) \subset U$. En résumé,

$$\forall \varepsilon > 0, \exists \eta > 0, f(B(a, \eta)) \subset B(f(a), \varepsilon)$$

i.e.

$$\forall \varepsilon > 0, \exists \eta > 0, d(x, a) < \eta \implies \delta(f(x), f(a)) < \varepsilon$$

(3) \Rightarrow (1) Il s'agit tout simplement de l'une des formulations du fait que f admet une limite $f(a)$ en a selon X .

Proposition II.2.

Les propositions suivantes sont équivalentes

1. f est continue en a .
2. Pour tout suite $(x_n) \in X^{\mathbb{N}}$, $x_n \xrightarrow[n \rightarrow +\infty]{} a \implies (f(x_n))$ converge.

Remarques

La composition de deux fonctions continues est continue.

lorsque Y est un espace vectoriel normé muni d'une norme $\|\cdot\|$ et δ la distance induite par $\|\cdot\|$, alors les opérations conservent la continuité :

→ La somme de deux fonctions continues est continue.

→ Lorsque $\|\cdot\|$ est une norme d'algèbre, le produit de deux fonctions continues est continu.

Exercice II.3.

Soit a, b deux réels tels que $a < b$. On dit qu'une fonction $f : [a, b] \rightarrow \mathbb{R}$ est réglée lorsque f admet une limite à droite et à gauche en tout point de $[a, b]$. Par exemple, les fonctions monotones sont réglées.

Supposons que f soit réglée. Montrer que l'ensemble des points de discontinuité de f est dénombrable.

2. Continuité globale

Commençons par énoncer un résultat qui sera utile par la suite.

Lemme II.4.

Les propositions suivantes sont équivalentes

1. f est continue en a .
2. $\forall V \in \mathcal{V}(f(a)), f^{-1}(V) \in \mathcal{V}(a)$

Preuve

(1) \Rightarrow (2) Si f est continue en a , alors par définition

$$\forall V \in \mathcal{V}(f(a)), \exists U \in \mathcal{V}(a), f(U) \subset V$$

et donc

$$\forall V \in \mathcal{V}(f(a)), \exists U \in \mathcal{V}(a), f^{-1}(f(U)) \subset f^{-1}(V)$$

or $U \subset f^{-1}(f(U)) \subset f^{-1}(V)$ et finalement pour tout $V \in \mathcal{V}(f(a))$, on a $f^{-1}(V) \in \mathcal{V}(a)$ car contient U un voisinage de a .

(2) \Rightarrow (1) Soit $V \in \mathcal{V}(f(a))$, posons $U = f^{-1}(V) \in \mathcal{V}(a)$. On a $f(U) = f(f^{-1}(V)) \subset V$, d'où la continuité de f en a .

Proposition II.5.

Les propositions suivantes sont équivalentes.

1. f est continue en tout point de X .
2. Pour tout ouvert Ω de Y , $f^{-1}(\Omega)$ est un ouvert de X .
3. pour tout fermé F de Y , $f^{-1}(F)$ est un fermé de X .

Preuve

(1) \Rightarrow (2) Soit Ω un ouvert de Y et $x \in f^{-1}(\Omega)$. Ω est un ouvert contenant $f(x)$, donc $\Omega \in \mathcal{V}(f(x))$, alors par continuité de f et le lemme précédent, $f^{-1}(\Omega) \in \mathcal{V}(x)$. Il existe alors $\varepsilon > 0$ tel que $B(x, \varepsilon) \subset f^{-1}(\Omega)$ et finalement $f^{-1}(\Omega)$ est ouvert.

(2) \Rightarrow (1) Soit $\varepsilon > 0$ et $b \in X$. Posons $\Omega = B(f(b), \varepsilon)$. Par hypothèse, $f^{-1}(\Omega)$ est ouvert et donc il existe $\eta > 0$ tel que $B(b, \eta) \subset f^{-1}(\Omega)$, i.e. $f(B(b, \eta)) \subset B(f(b), \varepsilon)$, ce qui donne directement la continuité de f en b , donc en tout point de X .

(2) \Rightarrow (3) Soit F un fermé de Y . $Y \setminus F$ est ouvert de Y , donc $f^{-1}(Y \setminus F) = X \setminus f^{-1}(F)$ est ouvert et finalement $f^{-1}(F)$ est fermé.

(3) \Rightarrow (2) Le sens réciproque peut être fait de la même manière et est laissé comme exercice au lecteur.

Applications

- Si f est une fonction continue de X dans Y , alors pour tout $b \in Y$, $f^{-1}(\{b\})$ est fermé car $\{b\}$ est fermé.
- Si de plus $Y = \mathbb{R}$, alors $\{x \in X, f(x) < 0\}$ est ouvert car il est égal à $f^{-1}(]-\infty, 0[)$ et $]-\infty, 0[$ est ouvert.
- Si Y est un espace vectoriel normé et g une fonction continue de X dans Y , alors l'ensemble où f coïncide avec g est un fermé car il est égal à

$$\{x \in X \mid f(x) = g(x)\} = \{x \in X \mid (f - g)(x) = 0\} = (f - g)^{-1}(\{0\})$$

le fait que $f - g$ continue et $\{0\}$ est fermé permet de conclure.

Exemple (principe des prolongements des indentités)

Soit E un espace vectoriel normé et $f, g \in \mathcal{C}(X, E)$. Si f et g coïncident sur une partie A dense dans X , alors $f = g$.

En effet, si B est l'ensemble où f coïncide avec g , alors d'après le troisième point des application de la proposition précédente, B est fermé. On a alors $A \subset B$ et donc $X = \overline{A} \subset \overline{B} = B$ car B est fermé. On obtient donc que $B = X$ et que finalement $f = g$.

Exercice II.6.

Soit f une fonction de X dans Y . Montrer que les propositions suivantes sont équivalentes.

1. f est continue en tout point de X .
2. Pour toute partie A de X , $f(\overline{A}) \subset \overline{f(A)}$.

Exercice II.7.

Soit $f : (\mathbb{R}, +) \rightarrow (\mathbb{R}, +)$ un morphisme de groupe. Montrer que les propriétés suivantes sont équivalentes.

1. f est continue.
2. $\exists \lambda \in \mathbb{R}, \forall x \in \mathbb{R}, f(x) = \lambda x$
3. f est continue en un point.
4. f est continue en 0.
5. f est bornée au voisinage de 0.

Exercice II.8.

Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ un morphisme de corps continu. Montrer que $f = Id$.

Exercice II.9.

Soit $f : \mathbb{C} \rightarrow \mathbb{C}$ un morphisme de corps continu. Montrer que $f = Id$ ou $f = (z \mapsto \bar{z})$.

3. Homéomorphismes

Définition II.10.

Soit f une application de X dans Y . Si

- f est continue.
- f est bijective.
- f^{-1} est continue.

alors on dit que f est un homéomorphisme de X dans Y .

Exemples

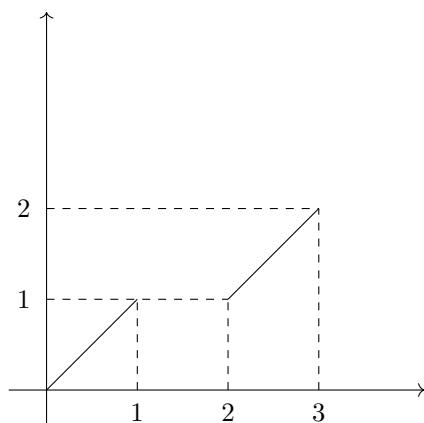
- Soit E un \mathbb{K} -espace vectoriel normé et $(\lambda, a) \in \mathbb{K}^* \times E$. L'application $h_{\lambda,a} : \begin{cases} E \longrightarrow E \\ x \longmapsto \lambda x + a \end{cases}$ est un homéomorphisme.
- La fonction tangente est un homéomorphisme de $]-\frac{\pi}{2}, \frac{\pi}{2}[$ dans \mathbb{R} .

Proposition II.11.

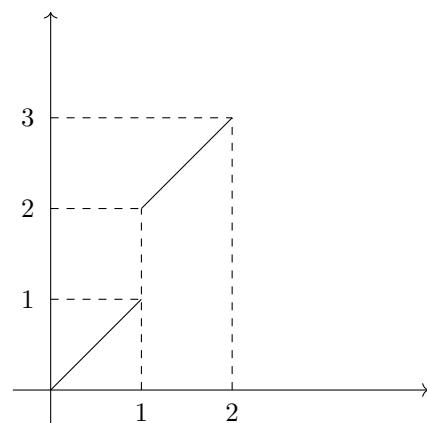
Soit I et J deux intervalles de \mathbb{R} . Si $f : I \longrightarrow J$ est une bijection continue, alors f^{-1} est continue.

Attention : cette propriété n'est plus vraie lorsque I et J ne sont pas des intervalles. En effet, si on considère la fonction de $[0, 1] \cup [2, 3]$ dans $[0, 2]$ $f : x \longmapsto \begin{cases} x & \text{si } 0 \leq x < 1 \\ x - 1 & \text{si } 2 \leq x \leq 3 \end{cases}$, cette fonction est continue bijective mais sa bijection réciproque n'est pas continue.

Courbe de f



Courbe de f^{-1}



Proposition II.12.

Soient Ω et Ω' deux ouverts de \mathbb{R} . Si $f : \Omega \longrightarrow \Omega'$ est une bijection continue, alors f^{-1} est continue.

4. Applications lipschitziennes

Définition II.13.

Soit f une application de X dans Y . On dit que f est lipschitzienne ou k -lipschitzienne s'il existe $k \in \mathbb{R}^+$ tel que

$$\forall (x, y) \in X^2, \delta(f(x), f(y)) \leq kd(x, y)$$

Exemples

→ Soit E un espace vectoriel normé muni d'une norme $\|\cdot\|$. L'application $x \mapsto \|x\|$ est 1-lipschitzienne. En effet, pour tout $x, y \in E$, on a

$$|\|x\| - \|y\|| \leq \|x - y\|$$

→ Soit $a \in X$. L'application $x \mapsto d(a, x)$ est 1-lipschitzienne. En effet, pour tout $x, y \in X$

$$|d(a, x) - d(a, y)| \leq d(x, y)$$

Exercice II.14.

Soit I un intervalle de \mathbb{R} et $f \in \mathcal{C}^1(I, \mathbb{C})$. Montrer que les deux propriétés suivantes sont équivalentes.

1. f est lipschitzienne.
2. f' est bornée.

Vocabulaire : lorsque f est lipschitzienne, on appelle rapport de lipschitzianité le nombre

$$k = \inf\{\alpha \in \mathbb{R}^+, f \text{ est } \alpha\text{-lipschitzienne}\}$$

Exercice II.15.

Soit A une partie non vide de X . Posons pour tout $x \in X$

$$d(x, A) = \inf_{a \in A} d(x, a)$$

1. Montrer que pour tout $x \in X$, $d(x, A) = 0 \iff x \in \overline{A}$.
2. Montrer que $x \mapsto d(x, A)$ est 1-lipschitzienne.
3. Montrer que si A et B sont deux fermés disjoints non vides de X , alors il existe deux ouverts U et V de X tels que $A \subset U$, $B \subset V$, et $U \cap V = \emptyset$.

Exercice II.16.

Soit $k \in \mathbb{R}^+$, I un ensemble, et $(f_i)_{i \in I}$ une famille de fonctions k -lipschitziennes. Supposons qu'il existe $a \in X$ tel que la famille $(f_i(a))_{i \in I}$ est majorée.

Montrer que $f : \begin{cases} X & \rightarrow \mathbb{R} \\ x & \mapsto \sup_{i \in I} f_i(x) \end{cases}$ est correctement définie et est k -lipschitzienne.

Exercice II.17.

Soit A une partie de X et $f : A \rightarrow \mathbb{R}$ une application k -lipschitzienne. Posons pour tout $x \in A$

$$g(x) = \inf_{y \in A} (f(y) + kd(x, y))$$

Montrer que g est k -lipschitzienne et que $g|_A = f$.

5. Uniforme continuité

Définition II.18.

Soit f une application de X dans Y . On dit que f est uniformément continue lorsque

$$\forall \varepsilon > 0, \exists \eta > 0, \forall (x, y) \in X^2, d(x, y) < \eta \implies \delta(f(x), f(y)) < \varepsilon$$

Exemples

- Si $f \in C([a, b], \mathbb{C})$, alors f est uniformément continue d'après le théorème de Heine.
- Si f est une application de X dans Y k -lipschitzienne, alors f est uniformément continue. La preuve de ce résultat est laissée comme exercice au lecteur.

Attention : il n'y a pas de réciproque pour le point précédent. Une fonction uniformément continue n'est pas nécessairement lipschitzienne.

En effet, il suffit de considérer la fonction de $[0, 1]$ dans $[0, 1]$ $f : x \mapsto \sqrt{x}$. C'est une fonction continue sur un segment, donc elle est uniformément continue d'après le théorème de Heine.

Supposons que f est lipschitzienne. On dispose alors de $k \geq 0$ tel que pour tout $x \in]0, 1]$,

$$\left| \frac{f(x) - f(0)}{x - 0} \right| \leq k$$

i.e.

$$\frac{1}{\sqrt{x}} \leq k$$

ce qui est absurde.

Théorème (Théorème de Heine) II.19.

Une fonction f continue sur un segment $[a, b]$ est uniformément continue.

Preuve : formulons tout d'abord la négation de l'uniforme continuité

$$\exists \varepsilon > 0, \forall \eta > 0, \exists x, y \in [a, b], |x - y| < \eta \text{ et } |f(x) - f(y)| \geq \varepsilon$$

Supposons donc cette proposition vérifiée. On dispose alors de deux suites $(x_n)_{n \in \mathbb{N}}$ et $(y_n)_{n \in \mathbb{N}}$ telles que pour tout $n \in \mathbb{N}$, $|x_n - y_n| \leq \frac{1}{n}$ (*) et $|f(x_n) - f(y_n)| \geq \varepsilon$. (x_n) et (y_n) étant à valeurs dans un fermé borné de \mathbb{R} , le théorème de Bolzano-Weierstrass nous permet d'affirmer l'existence d'une extractrice φ telle que $(x_{\varphi(n)})$ converge. De même, on dispose d'une extractrice ψ telle que $(y_{\varphi \circ \psi(n)})$ soit convergente. L'inégalité (*) impose que $(x_{\varphi \circ \psi(n)})$ et $(y_{\varphi \circ \psi(n)})$ admettent la même limite qu'on note l .

On a alors

$$\left| f(x_{\varphi \circ \psi(n)}) - f(y_{\varphi \circ \psi(n)}) \right| \xrightarrow{n \rightarrow +\infty} |f(l) - f(l)| = 0$$

mais pour tout $n \in \mathbb{N}$, $|f(x_{\varphi \circ \psi(n)}) - f(y_{\varphi \circ \psi(n)})| \geq \varepsilon > 0$, ce qui absurde, d'où l'uniforme continuité de f sur $[a, b]$.

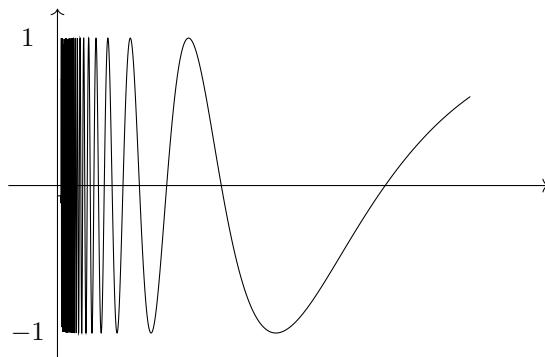
Exercice II.20.

Soit A une partie de X et $f : A \rightarrow \mathbb{R}$ une application uniformément continue. Montrer que f admet une limite en tout point de \overline{A} .

Exercice II.21.

Soit E un espace vectoriel normé et $f : B_f(0, 1) \rightarrow \mathbb{R}$ une application uniformément continue. Montrer que f est bornée.

Attention : une application continue bornée n'est pas nécessairement uniformément continue. En effet, considérons la fonction de $]0, 1]$ dans $[-1, 1]$, $f : x \mapsto \cos(\frac{1}{x})$.



Cette fonction est \mathcal{C}^∞ sur $]0, 1]$, mais elle n'est pas uniformément continue. Montrons le. Enonçons tout d'abord la négation de l'uniforme continuité.

$$\exists \varepsilon > 0, \forall \eta > 0, \exists (x, y) \in X^2, d(x, y) < \eta \text{ et } \delta(f(x), f(y)) \geq \varepsilon$$

i.e., en adaptant cette proposition à notre problème,

$$\exists \varepsilon > 0, \forall \eta > 0, \exists (x, y) \in]0, 1]^2, |x - y| < \eta \text{ et } |f(x) - f(y)| \geq \varepsilon$$

Considérons les suites $(x_n)_{n \in \mathbb{N}^*} = (\frac{1}{2n\pi})_{n \in \mathbb{N}^*}$ et $(y_n)_{n \in \mathbb{N}^*} = (\frac{1}{(2n+1)\pi})_{n \in \mathbb{N}^*}$. On a

$$|x_n - y_n| = \left| \frac{1}{2n\pi} - \frac{1}{(2n+1)\pi} \right| \xrightarrow{n \rightarrow +\infty} 0$$

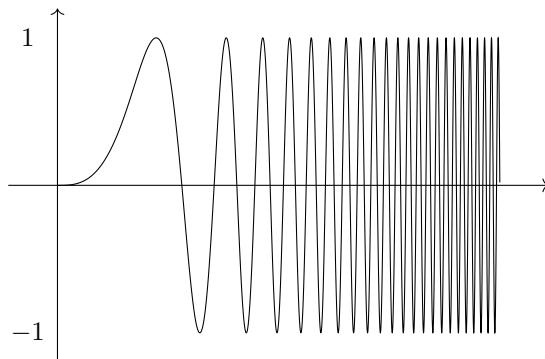
mais pour tout $n \in \mathbb{N}^*$

$$|f(x_n) - f(y_n)| = 1$$

donc en prenant $\varepsilon = \frac{1}{2}$, on a pour tout $\eta > 0$, on peut prendre n assez grand pour qu'on ait $|x_n - y_n| < \eta$ et $|f(x_n) - f(y_n)| = 1 \geq \varepsilon$ ce qui montre bien la négation de l'uniforme continuité.

L'intuition derrière ce contrexemple est que f oscille très rapidement au voisinage de 0 (voir figure ci-dessus), ce qui fait qu'on ne peut plus contrôler l'écart entre l'image de deux points assez proches.

Il existe une infinité d'autres contrexemples, on peut par exemple prendre la fonction de \mathbb{R} dans $[-1, 1]$ $x \mapsto \sin(x^2)$



on peut prouver de la même manière la non uniforme continuité en prenant les suites $(x_n)_{n \in \mathbb{N}} = (\sqrt{2n\pi})_{n \in \mathbb{N}}$ et $(y_n)_{n \in \mathbb{N}} = (\sqrt{(2n + \frac{1}{2})\pi})_{n \in \mathbb{N}}$. Ici encore, on voit que la fonction oscille très vite au voisinage de $+\infty$ ce qui empêche la fonction d'être uniformément continue.

6. Extensions du théorème de Heine

Exercice II.22.

Soit $T \in \mathbb{R}^+$ et $E = \mathcal{C}_T(\mathbb{R}, \mathbb{C})$ l'ensemble des fonctions continues T -périodiques de \mathbb{R} dans \mathbb{C} . Montrer que toute fonction de E est uniformément continue.

Exercice II.23.

Soit $E = \{f \in \mathcal{C}(\mathbb{R}, \mathbb{C}), f(x) \xrightarrow{x \rightarrow \pm\infty} 0\}$. Montrer que toute fonction de E est uniformément continue.

Correction de l'exercice I.5. :

Soit $\varepsilon > 0$, il existe $\eta > 0$ tel que pour tout $x \in B(0, \eta)$

$$\left| \frac{f(x) - f\left(\frac{x}{2}\right)}{x} - l \right| < \varepsilon$$

Or pour tout $k \in \mathbb{N}$, si $x \in B(0, \eta)$, alors $\frac{x}{2^k} \in B(0, \eta)$. On a alors pour tout $k \in \mathbb{N}$,

$$\left| \frac{f\left(\frac{x}{2^k}\right) - f\left(\frac{x}{2^{k+1}}\right)}{\frac{x}{2^k}} - l \right| < \varepsilon$$

i.e.

$$\left| \frac{f\left(\frac{x}{2^k}\right) - f\left(\frac{x}{2^{k+1}}\right)}{x} - \frac{l}{2^k} \right| < \frac{\varepsilon}{2^k}$$

En sommant toutes ces inégalités pour $k \in \llbracket 0; n-1 \rrbracket$ et utilisant l'inégalité triangulaire, on obtient que pour tout $n \in \mathbb{N}$ et $x \in B(0, \eta)$,

$$\left| \frac{f(x) - f\left(\frac{x}{2^n}\right)}{x} - l \sum_{k=0}^{n-1} \frac{1}{2^k} \right| \leq \sum_{k=0}^{n-1} \left| \frac{f\left(\frac{x}{2^{k+1}}\right) - f\left(\frac{x}{2^k}\right)}{x} - \frac{l}{2^k} \right| < \varepsilon \sum_{k=0}^{n-1} \frac{1}{2^k}$$

En faisant tendre n vers l'infini, par continuité de f , l'inégalité ci-dessus devient

$$\left| \frac{f(x) - f(0)}{x} - 2l \right| \leq 2\varepsilon$$

Ce qui montre que f est dérivable en 0 et que $f'(0) = 2l$.

Correction de l'exercice I.6. :

Soit $\varepsilon > 0$, $A > 1$ tel que pour tout $x \geq A-1$,

$$L - \varepsilon \leq f(x+1) - f(x) \leq L + \varepsilon$$

Posons pour tout x , $n(x)$ l'unique entier vérifiant $A \leq x - n(x) < A + 1$. On a alors

$$L - \varepsilon \leq f(x - (n(x) - 1) + 1) - f(x - (n(x) - 1)) \leq L + \varepsilon$$

$$L - \varepsilon \leq f(x - (n(x) - 2) + 1) - f(x - (n(x) - 2)) \leq L + \varepsilon$$

⋮

$$L - \varepsilon \leq f((x-1)+1) - f(x-1) \leq L + \varepsilon$$

En sommant toutes les inégalités ci-dessous, on obtient

$$n(x)(L - \varepsilon) \leq f(x) - f(x - n(x)) \leq n(x)(L + \varepsilon)$$

et on a $x - n(x)$ est toujours dans $[A, A+1]$ où f est bornée car continue, donc

$$\underbrace{\frac{n(x)}{x}}_{x \rightarrow +\infty} \underbrace{(L - \varepsilon) + \frac{f(x - n(x))}{x}}_{x \rightarrow +\infty \rightarrow 0} \leq \frac{f(x)}{x} \leq \underbrace{\frac{n(x)}{x}}_{x \rightarrow +\infty} \underbrace{(L + \varepsilon) + \frac{f(x - n(x))}{x}}_{x \rightarrow +\infty \rightarrow 0}$$

On peut donc choisir $B > A$ de sorte à ce que pour tout $x > B$,

$$\left| \frac{f(x - n(x))}{x} \right| \leq \varepsilon \text{ et } L - 2\varepsilon \leq \frac{n(x)}{x}(L + \varepsilon) \leq L + 2\varepsilon$$

et donc pour tout $x > B$

$$L - 3\varepsilon \leq \frac{f(x)}{x} \leq L + 3\varepsilon$$

On a donc bien montré que $x \mapsto \frac{f(x)}{x}$ admet une limite en $+\infty$ et que

$$\frac{f(x)}{x} \xrightarrow[x \rightarrow +\infty]{} L$$

Correction de l'exercice II.3. :

Posons pour tout $x \in [a, b]$ $f(x^+)$ et $f(x^-)$ respectivement la limite à droite et à gauche en x . Définissons les ensembles suivants.

- C est l'ensemble des points de discontinuité de f .
- $A = \{x \in [a, b], |f(x^+) - f(x^-)| > 0\}$
- Pour tout $p \in \mathbb{N}^*$, $A_p = \{x \in [a, b], |f(x^+) - f(x^-)| \geq \frac{1}{p}\}$
- $B = \{x \in [a, b], f(x^-) = f(x^+) \text{ et } f(x^+) \neq f(x)\}$
- Pour tout $p \in \mathbb{N}^*$ $B_p = \{x \in B, |f(x^+) - f(x)| \geq \frac{1}{p}\}$

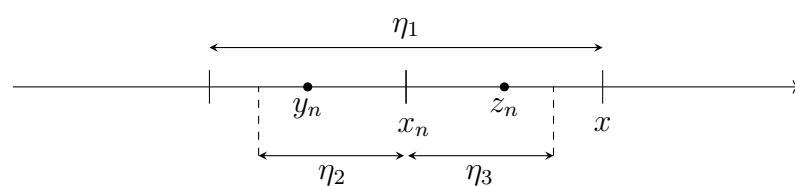
On a alors

$$C = B \cup A = \bigcup_{p \in \mathbb{N}^*} B_p \cup \bigcup_{p \in \mathbb{N}^*} A_p$$

On va montrer que pour tout $p \in \mathbb{N}^*$, A_p et B_p sont finis. Une fois cela fait, on peut facilement conclure car on aura montré que A et B sont union dénombrable d'ensembles finis et donc qu'ils sont dénombrables. Supposons par l'absurde qu'il existe $p \in \mathbb{N}^*$ tel que A_p est infini. A_p est infini borné en dimension finie, il possède donc un point d'accumulation qu'on note x . On dispose alors d'une suite $(x_n)_{n \in \mathbb{N}}$ injective à valeurs dans A qui converge vers x . Quitte à extraire de la suite (x_n) on suppose sans perte de généralité qu'elle est croissante.

- Soit $\eta_1 > 0$ tel que pour tout $\alpha \in]x - \eta_1, x[$, $|f(\alpha) - f(x^-)| < \frac{1}{4p}$
- Soit $n \in \mathbb{N}$ tel que $x_n \in]x - \eta_1, x[$. On suppose aussi sans perte de généralité que $x \neq a$.
- Soit $\eta_2 > 0$ tel que pour tout $\alpha \in]x_n - \eta_2, x_n[$, $|f(\alpha) - f(x_n^-)| < \frac{1}{4p}$
- Soit $\eta_3 > 0$ tel que pour tout $\alpha \in]x_n, x_n + \eta_3[$, $|f(x_n^+) - f(\alpha)| < \frac{1}{4p}$
- Quitte à remplacer η_2 par $\min(|x_n - x|, \eta_2)$ et η_3 par $\min(|x_n - x + \eta_1|, \eta_3)$, on suppose que $\eta_2 \leq |x_n - x + \eta_1|$ et que $\eta_3 \leq |x_n - x|$ pour qu'on ait $]x_n - \eta_2, x_n[\subset]x - \eta_1, x[$ et $]x_n, x_n + \eta_3[\subset]x - \eta_1, x[$.
- Soit $y_n, z_n \in [a, b]$ tels que $y_n \in]x_n - \eta_2, x_n[$ et $z_n \in]x_n, x_n + \eta_3[$.

Pour que tout cela soit plus clair, observons tous les paramètres qu'on vient de définir sur le dessin suivant :



On a

$$\begin{aligned} |f(y_n) - f(z_n)| &\geq |f(x_n^-) - f(x_n^+)| - |f(x_n^+) - f(z_n)| - |f(y_n) - f(x_n^-)| \\ &> \frac{1}{p} - \frac{1}{4p} - \frac{1}{4p} = \frac{1}{2p} \end{aligned}$$

et

$$|f(y_n) - f(z_n)| \leq |f(y_n) - f(x^-)| + |f(z_n) - f(x^-)| < \frac{1}{4p} + \frac{1}{4p} = \frac{1}{2p}$$

ce qui est absurde.

On va procéder de la même manière pour les ensembles B_p . Supposons par l'absurde qu'il existe $p \in \mathbb{N}^*$ tel que B_p est infini. B_p est infini borné en dimension finie, il admet donc un point d'accumulation qu'on note x . On dispose alors d'une suite $(x_n)_{n \in \mathbb{N}}$ injective à valeurs dans B_p qu'on suppose sans perte de généralité, quitte à extraire, croissante.

- Soit $\eta_1 > 0$ tel que pour tout $\alpha \in]x - \eta_1, x[$, $|f(\alpha) - f(x^-)| < \frac{1}{4p}$
- Soit $n \in \mathbb{N}$ tel que $x_n \in]x - \eta_1, x[$.
- Soit $\eta_2 > 0$ tel que pour tout $\alpha \in]x_n - \eta_2, x_n + \eta_2[$, $|f(\alpha) - f(x_n^-)| < \frac{1}{2p}$
Quitte à remplacer η_2 par $\min(|x_n - x|, |x_n - x + \eta_1|, \eta_2)$, on suppose que $]x_n - \eta_2, x_n + \eta_2[\subset]x - \eta_1, x[$.
- Soit $y_n \in]x_n - \eta_2, x_n + \eta_2[$.

On a alors

$$|f(x_n) - f(x^-)| < \frac{1}{4p}$$

et

$$\begin{aligned} |f(x_n) - f(x^-)| &\geq |f(x_n) - f(y_n)| - |f(y_n) - f(x^-)| \\ &\geq |f(x_n) - f(x_n^-)| - |f(x_n^-) - f(y_n)| - |f(y_n) - f(x^-)| \\ &> \frac{1}{p} - \frac{1}{2p} - \frac{1}{4p} = \frac{1}{4p} \end{aligned}$$

ce qui est absurde. On a donc bien obtenu le résultat voulu.

L'intuition derrière le fait que A_p et B_p soient finis est que lorsqu'on se rapproche par exemple par la gauche d'un point x où f admet une limite à gauche, on ne peut pas rencontrer un nombre infini de points de discontinuité de taille $\frac{1}{p}$ car sinon la fonction fera des pas trop grands pour tendre vers $f(x^-)$ à gauche de x .

Remarque : ici, x n'est pas nécessairement dans A . On a juste eu besoin du fait que f admet une limite à gauche de x .

Correction de l'exercice II.6. :

(1) ⇒ (2) Supposons que f est continue. Soit $x \in \overline{A}$. On dispose d'une suite $(x_n)_{n \in \mathbb{N}}$ à valeurs dans A qui converge vers x . On a alors par continuité de f , la suite $(f(x_n))_{n \in \mathbb{N}}$ est à valeurs dans $f(A)$ converge vers $f(x)$, i.e. $f(x) \in \overline{f(A)}$ et on a finalement $f(\overline{A}) \subset \overline{f(A)}$

(2) ⇒ (1) Supposons que pour tout $A \subset X$, $f(\overline{A}) \subset \overline{f(A)}$. Soit F un fermé de Y . Posons $A = f^{-1}(F)$ et montrons que A est fermé. Une fois cela fait, on peut aisément conclure que f est continue d'après une propriété du cours.

On a $f(\overline{A}) \subset \overline{f(A)} = \overline{f(f^{-1}(F))} \subset \overline{F} = F$, et donc $\overline{A} \subset f^{-1}(F) = A$ i.e. A est fermé.

Correction de l'exercice II.7. :

(1) ⇒ (2) On a pour tout $n \in \mathbb{Z}$ et $x \in \mathbb{R}$, $f(nx) = nf(x)$. Lorsque $n \neq 0$, en remplaçant x par $\frac{x}{n}$, $f(x) = nf\left(\frac{x}{n}\right)$, i.e. $f\left(\frac{x}{n}\right) = \frac{1}{n}f(x)$.

On a alors pour tout $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, $f\left(\frac{p}{q}x\right) = \frac{p}{q}f(x)$, et alors pour tout $\alpha \in \mathbb{Q}$, $f(\alpha x) = \alpha f(x)$.

Par densité de \mathbb{Q} dans \mathbb{R} , on dispose d'une suite $(x_n)_{n \in \mathbb{N}}$ à valeurs dans \mathbb{Q} qui converge vers x . On utilise alors cette suite pour avoir le résultat suivant : $f(x_n) = x_n f(1) \xrightarrow[n \rightarrow +\infty]{} xf(1)$ et f continue donc $f(x_n) \xrightarrow[n \rightarrow +\infty]{} f(x)$. En posant $\lambda = f(1)$, on obtient que pour tout $x \in \mathbb{R}$, $f(x) = \lambda x$.

(2) \Rightarrow (3) Le résultat est évident car toutes les homothéties de \mathbb{R} sont continues.

(3) \Rightarrow (4) idem.

(4) \Rightarrow (5) Il suffit d'appliquer la définition de la continuité en 0 avec $\varepsilon = 1$.

(5) \Rightarrow (1) Soit $\alpha > 0$ tel que f est bornée sur $[-\alpha, \alpha]$ et posons $M = \sup_{x \in [-\alpha, \alpha]} |f(x)|$. Soit $\varepsilon > 0$. On considère $n \in \mathbb{N}^*$ tel que $\frac{M}{n} < \varepsilon$. On a alors

$$f\left(\left[-\frac{\alpha}{n}, \frac{\alpha}{n}\right]\right) = \frac{1}{n}f([-n\alpha, n\alpha]) \subset \left[-\frac{M}{n}, \frac{M}{n}\right] \subset [-\varepsilon, \varepsilon]$$

ce qui nous donne la continuité de f en 0. La continuité de f en tout point $x \in \mathbb{R}$ vient du fait que

$$f(y) = \underbrace{f(y-x)}_{y \rightarrow x} + f(x) \xrightarrow[y \rightarrow x]{} f(x)$$

par continuité de f en 0.

Correction de l'exercice II.8. :

D'après l'exercice précédent, on dispose de $\lambda \in \mathbb{R}$, tel que $f = x \mapsto \lambda x$. Or, f étant un morphisme de corps, on a $f(1) = 1$, i.e. $\lambda = 1$ et alors $f = Id$

Correction de l'exercice II.9. :

En utilisant une méthode analogue à celle utilisée pour les deux exercices précédents, on peut montrer que pour tout nombre complexe $a + ib$, $f(a + ib) = a + f(i)b$. Il reste donc à déterminer la valeur de $f(i)$ pour déterminer f . On a $f(i)^2 = f(i^2) = f(-1) = -1$ et alors $f(i) \in \{i, -i\}$. On peut donc immédiatement en déduire que $f = Id$ ou $f = (z \mapsto \bar{z})$.

Correction de l'exercice II.14. :

(1) \Rightarrow (2) Posons $k \geq 0$ le rapport de lipschitziannité de f . On alors pour tout $a \in I$,

$$k \geq \left| \frac{f(x) - f(a)}{x - a} \right| \xrightarrow{x \rightarrow a} |f'(a)|$$

i.e. f' est bornée par k .

(2) \Rightarrow (1) Supposons que f' est bornée par k . Utilisons le théorème des accroissements finis. On a pour tout $x, y \in I$ différents, il existe $c \in I$ tel que

$$|f(x) - f(y)| = |f'(c)| |x - y| \leq k |x - y|$$

Correction de l'exercice II.15. :

1. On a

$$d(x, A) = 0 \iff \exists (a_n) \in A^{\mathbb{N}}, d(x, a_n) \xrightarrow[n \rightarrow +\infty]{} 0 \iff x \in \overline{A}$$

2. Il s'agit de l'inégalité triangulaire. Soit $x, y \in X$.

On a pour tout $a \in A$, $d(y, A) \leq d(y, a) \leq d(x, a) + d(x, y)$ et alors en passant à la borne inférieure sur a des deux côtés, on obtient

$$d(y, A) \leq d(x, A) + d(x, y) \quad (1)$$

de même, on a pour tout $a \in A$, $d(x, A) \leq d(x, a) \leq d(y, a) + d(x, y)$ et alors en passant à la borne

inférieure des deux côtés on obtient

$$d(x, A) \leq d(y, A) + d(x, y) \quad (2)$$

en combinant les inégalités (1) et (2), on obtient

$$-d(x, y) \leq d(x, A) - d(y, A) \leq d(x, y)$$

i.e.

$$|d(x, A) - d(y, A)| \leq d(x, y)$$

3. Considérons l'application $f : \begin{cases} X & \longrightarrow \mathbb{R} \\ x & \longmapsto d(x, B) - d(x, A) \end{cases}$
- Si $x \in A$, on a $x \notin B = \overline{B}$, et alors $f(x) = d(x, B) > 0$. On alors $A \subset \{x \in X, f(x) > 0\} = f^{-1}(\mathbb{R}_+^*) = U$
 - Si $x \in B$, on a $x \notin A = \overline{A}$, et alors $f(x) = -d(x, A) < 0$. On alors $B \subset \{x \in X, f(x) < 0\} = f^{-1}(\mathbb{R}_-^*) = V$

U et V sont les images réciproques des ouverts \mathbb{R}_+^* et \mathbb{R}_-^* par une fonction continue (car lipschitzienne) et donc sont ouverts. De plus on a $U \cap V = \emptyset$, on a alors bien obtenu le résultat voulu.

Correction de l'exercice II.16. :

Montrons tout d'abord que f est bien définie, i.e. pour tout $i \in I$ et $x \in \mathbb{R}$, la famille $(f_i(x))_{i \in I}$ est majorée. Soit M un majorant de $(f_i(a))_{i \in I}$, on a pour tout $x \in \mathbb{R}$ et $i \in I$,

$$f_i(x) - f_i(a) \leq k |x - a|$$

et alors

$$f_i(x) \leq k |x - a| + M$$

ce qui montre bien que f est définie.

Montrons ensuite que f est k -lipschitzienne. On a pour $i \in I$ et $x, y \in \mathbb{R}$,

$$|f_i(x) - f_i(y)| \leq k |x - y|$$

i.e.

$$f_i(y) - k |x - y| \leq f_i(x) \leq f_i(y) + k |x - y|$$

On peut donc passer à la borne supérieure en i de chaque côté de l'inégalité pour obtenir que

$$f(y) - k |x - y| \leq f(x) \leq f(y) + k |x - y|$$

i.e.

$$|f(x) - f(y)| \leq k |x - y|$$

Correction de l'exercice II.17. :

→ Montrons que g est bien définie et est k -lipschitzienne.

Posons pour tout $y \in X$, $\varphi_y : x \mapsto f(y) + kd(x, y)$. Toutes les fonctions $-\varphi_y$ sont k -lipschitziennes et par lipschitzianité de $-\varphi_y$ pour tout $y \in X$,

$$-\varphi_y(0) = -(f(y) + kd(0, y)) \leq -f(0)$$

donc la famille $(\varphi_y(0))_{y \in X}$ est majorée, et alors d'après l'exercice précédent, $h = \sup_{y \in X} (-\varphi_y)$ est bien définie et est k -lipschitzienne et donc de même pour $g = -h$.

→ Montrons que $g|_A = f$.

On a pour tout $x, y \in A$, $f(y) + kd(x, y) \geq f(x)$ (car f est k -lipschitzienne). Ce minorant est atteint pour $y = x$, donc $\inf_{y \in X} f(y) + kd(x, y) = f(x)$.

Correction de l'exercice II.20. :

Soit $a \in \overline{A}$ et $(x_n)_{n \in \mathbb{N}} \in A^{\mathbb{N}}$ telle que $x_n \xrightarrow{n \rightarrow +\infty} a$. On va montrer que la suite $(f(x_n))_{n \in \mathbb{N}}$ est de Cauchy.

Soit $\varepsilon > 0$. Par uniforme continuité de f , on peut considérer $\eta > 0$ tel que pour tout $x, y \in A$,

$$d(x, y) < \eta \implies |f(x) - f(y)| < \varepsilon$$

$(x_n)_{n \in \mathbb{N}}$ étant convergente et donc de Cauchy, on peut considérer $N \in \mathbb{N}$ tel que pour tout $n, m \geq N$, $d(x_n, x_m) < \eta$.

On alors pour tout $n, m > N$, $|f(x_n) - f(x_m)| < \varepsilon$. $(f(x_n))_{n \in \mathbb{N}}$ est donc de Cauchy, i.e. convergente. f admet donc bien une limite en tout point de \overline{A} .

Correction de l'exercice II.21. :

Supposons sans perte de généralité que $f(0) = 0$. Par uniforme continuité de f , on peut considérer $\eta > 0$ tel que pour tout $x, y \in B_f(0, 1)$, $\|x - y\| < \eta \implies |f(x) - f(y)| < 1$.

Soit $p \in \mathbb{N}^*$ tel que $\frac{1}{p} \leq \eta$. On a pour tout $x \in B_f(0, 1)$,

$$|f(x)| = |f(x) - f(0)| \leq \sum_{k=0}^{p-1} \left| f\left((k+1)\frac{x}{p}\right) - f\left(k\frac{x}{p}\right) \right|$$

Or on a pour tout $k \in \llbracket 0; p-1 \rrbracket$, $\left\| (k+1)\frac{x}{p} - k\frac{x}{p} \right\| = \frac{\|x\|}{p} < \frac{1}{p} < \eta$ et alors

$$|f(x)| \leq \sum_{k=0}^{p-1} \left| f\left((k+1)\frac{x}{p}\right) - f\left(k\frac{x}{p}\right) \right| \leq p$$

donc f est bornée sur $B_f(0, 1)$.

Correction de l'exercice II.22. :

f est une fonction continue sur le segment $[-T, 2T]$ et y est donc uniformément continue. Montrons maintenant que f est uniformément continue sur \mathbb{R} .

Soit $\varepsilon > 0$. Soit $\eta > 0$ tel que pour tout $x, y \in [-T, 2T]$,

$$|x - y| < \eta \implies |f(x) - f(y)| < \varepsilon$$

Soit $x, y \in \mathbb{R}$ tel que $|x - y| < \eta$. Quitte à remplacer η par $\min(\eta, T)$, on suppose que $\eta \leq T$. On dispose alors de $n \in \mathbb{Z}$ tel que $x - nT \in [-T, 2T]$ et $y - nT \in [-T, 2T]$. On a alors $|(x - nT) - (y - nT)| < \eta$ et donc

$$|f(x) - f(y)| = |f(x - nT) - f(y - nT)| < \varepsilon$$

d'où l'uniforme continuité de f .

Remarque : on a choisi de regarder l'uniforme continuité de f dans l'intervalle $[-T, 2T]$ et non pas $[0, T]$ pour éviter le cas pathologique où x se retrouve sur les bords de l'intervalle $[0, T]$ et y en dehors de cet intervalle, ce qui nous empêcherait de conclure car on pourra pas utiliser l'uniforme continuité de f sur $[0, T]$.

Correction de l'exercice II.23. :

Soit $\varepsilon > 0$ et $A > 0$ tel que pour tout $x \in \mathbb{R}$, $|x| \geq A \implies |f(x)| < \varepsilon$.

f est uniformément continue sur $[-A, A]$ car continue, donc il existe $\eta > 0$ tel que $\eta < A$ et pour tout $x, y \in [-A, A]$, $|x - y| < \eta \implies |f(x) - f(y)| < \varepsilon$.

Soit $x, y \in \mathbb{R}$, supposons que $|x - y| < \eta$, trois cas de présentent :

→ $x, y \in [-A, A]$, alors on a directement que $|f(x) - f(y)| < \varepsilon$.

→ $x, y \in]A, +\infty[$ ou $x, y \in]-\infty, A[$, alors on a $|f(x) - f(y)| \leq |f(x)| + |f(y)| < 2\varepsilon$

→ $x \in [-A, A]$ et $y \notin [-A, A]$. On suppose sans perte de généralité que $x < A < y$. On a alors $|f(x) - f(y)| \leq |f(x) - f(A)| + |f(y) - f(A)| \leq 3\varepsilon$

d'où l'uniforme continuité de f sur \mathbb{R} .



CHAPITRE 11.4

Comparaison de normes et espaces produits

Dans tout ce chapitre, \mathbb{K} est un corps égal à \mathbb{R} ou \mathbb{C} , E est un \mathbb{K} -espace vectoriel et n est un entier naturel strictement positif.

I Comparaison de normes

Définition I.1.

Soient N_1 et N_2 deux normes sur E . On dit que N_1 est plus fine que N_2 (ou domine N_2) s'il existe $C > 0$ tel que pour tout $x \in E$, $N_2(x) \leq CN_1(x)$.

Proposition I.2.

Si N_1 est plus fine que N_2 , alors

1. Pour tout $(x_n) \in E^{\mathbb{N}}$, $x_n \xrightarrow[n \rightarrow +\infty]{} l$ pour $N_1 \implies x_n \xrightarrow[n \rightarrow +\infty]{} l$ pour N_2 .
2. Si F est une partie fermée de E pour N_2 , alors elle l'est pour N_1 .
3. Si O est une partie ouverte de E pour N_2 , alors elle l'est pour N_1 .

Preuve

Supposons que N_1 est plus fine que N_2 . soit $C > 0$ tel que pour tout $x \in E$, $N_2(x) \leq CN_1(x)$

1. Soit (x_n) une suite à valeurs dans E qui converge vers l pour N_1 . On a alors

$$N_2(x_n - l) \leq CN_1(x_n - l) \xrightarrow[n \rightarrow +\infty]{} 0$$

d'où le résultat voulu.

2. Soit F une partie fermée de E pour N_2 . Soit (x_n) une suite à valeurs dans F convergente pour N_1 vers $x \in E$. (x_n) converge alors pour N_2 vers x . F étant fermé pour N_2 , on a $x \in F$ et alors F est fermé pour N_1 .
3. Si O est ouvert pour N_2 , alors $E \setminus O$ est fermé pour N_1 donc pour N_2 et finalement O est ouvert pour N_1 .

Définition I.3.

On dit que deux normes N_1 et N_2 sont équivalentes lorsque N_1 est plus fine que N_2 et N_2 est plus fine que N_1 . Dans ce cas, on note $N_1 \sim N_2$.

Proposition I.4.

Soit N_1 et N_2 deux normes équivalentes.

1. Les suites convergentes pour N_1 sont exactement les suites convergentes pour N_2 .
2. Les ouverts (resp. fermés) pour N_1 sont exactement les ouverts (resp. fermés) pour N_2 .
3. Les fonctions continues pour N_1 sont exactement les fonctions continues pour N_2 .
4. Les applications lipschitziennes pour N_1 sont exactement les applications lipschitziennes pour N_2 , mais le rapport de lipschitzianité ne reste plus le même quand on passe d'une norme à l'autre.

Exemple : dans le cas où $E = \mathbb{K}^n$, les normes $\|\cdot\|_\infty$, $\|\cdot\|_1$ et $\|\cdot\|_2$ sont équivalentes. En effet, on a pour tout $x \in E$

- $\frac{1}{n} \|x\|_1 \leq \|x\|_\infty \leq \|x\|_1$, donc $\|\cdot\|_1 \sim \|\cdot\|_\infty$.
- $\|x\|_2 \leq \|x\|_1 \leq \sqrt{n} \|x\|_2$, donc $\|\cdot\|_2 \sim \|\cdot\|_1$.
- Par transitivité, ces trois normes sont deux à deux équivalentes.

Proposition I.5.

Lorsque E est de dimension finie, alors toutes les normes sur E sont équivalentes.

Preuve : la preuve de ce résultat sera faite dans une partie ultérieure de ce cours, car nous n'avons pas encore exposé les outils nécessaires pour le montrer.

Exemple 1 : Dans le cas où $E = C([a, b], \mathbb{R})$ avec $a < b$, alors $\|\cdot\|_2$ est plus fine que $\|\cdot\|_1$ et $\|\cdot\|_\infty$ est plus fine que $\|\cdot\|_2$, mais parmi ces trois normes, il n'y en a aucune qui est équivalente à une autre.

- On a pour tout $f \in C([a, b], \mathbb{R})$, $\|f\|_1 \leq \sqrt{b-a} \|f\|_2 \leq (b-a) \|f\|_\infty$.
- Les inégalités dans le sens contraire sont toutes fausses en général. En effet, si on considère la suite de fonctions $(f_n)_{n \in \mathbb{N}} = (x \mapsto x^n)_{n \in \mathbb{N}}$ de $[0, 1]$ dans \mathbb{R} , alors on a $f_n \xrightarrow[n \rightarrow +\infty]{} 0$ pour $\|\cdot\|_1$ et $\|\cdot\|_2$, mais $\|f_n\|_\infty = 1$ pour tout n , donc (f_n) ne tend pas vers 0 pour $\|\cdot\|_\infty$.

Exemple 2 : On se place dans le cas où $E = C^1([0, 1], \mathbb{R})$ et on considère la norme $\|\cdot\|$ telle que pour tout $f \in E$, $\|f\| = |f(0)| + \int_0^1 |f'(x)| dx$.

- $\|\cdot\|$ est plus fine que $\|\cdot\|_\infty$.
En effet, on a pour tout $f \in E$ et $x \in [a, b]$,

$$|f(x)| = \left| f(0) + \int_0^x f'(t) dt \right| \leq |f(0)| + \int_0^x |f'(t)| dt \leq |f(0)| + \int_0^1 |f'(t)| dt = \|f\|$$

Ce qui entraîne $\|f\|_\infty \leq \|f\|$.

- $\|\cdot\|_\infty$ n'est pas plus fine que $\|\cdot\|$.
En effet, si on considère la suite de fonctions $(f_n)_{n \in \mathbb{N}} = (x \mapsto \frac{1}{n} \sin(n\pi x))$, on trouve

- $\|f_n\|_\infty = \frac{1}{n} \xrightarrow[n \rightarrow +\infty]{} 0$
- Pour tout n , $\|f_n\| = \int_0^1 |\sin(n\pi t)| dt \geq \int_0^1 \sin(n\pi t)^2 dt \geq \frac{1}{2}$ et donc $\|f_n\|$ ne tend pas vers 0.

Exercice I.6.

On reprend les notations de l'exemple précédent. Soit $f \in E$. Montrer que

$$\int_0^1 f(t) |\sin(nt)| dt \xrightarrow[n \rightarrow +\infty]{} \frac{2}{\pi} \int_0^1 f(t) dt$$

Exercice I.7.

On pose $E = \mathbb{R}_n[X]$. Comparer les normes suivantes sur E , telles que pour tout $P = \sum_{k=0}^n a_k X^k \in E$

$$\rightarrow \|P\|_0 = \max(|a_0|, \dots, |a_n|)$$

$$\rightarrow \|P\|_1 = \sum_{k=0}^n |a_k|$$

$$\rightarrow \|P\|_\infty = \sup_{x \in [0,1]} |P(x)|$$

II Espaces produits

Soit $p \in \mathbb{N}^*$. On considère p espaces métriques E_1, \dots, E_p munis respectivement des distances d_1, \dots, d_p et on pose $E = E_1 \times \dots \times E_p$. On définit pour tout $i \in \llbracket 1; p \rrbracket$ la i -ème projection canonique

$$\pi_i : \begin{cases} E_1 \times \dots \times E_p & \longrightarrow E_i \\ (x_1, \dots, x_p) & \longmapsto x_i \end{cases}$$

Remarque préliminaire : pour tout $i \in \llbracket 1; p \rrbracket$, si A_i est une partie de E_i , alors

$$\pi_i^{-1}(A_i) = E_1 \times \dots \times E_{i-1} \times A_i \times E_{i+1} \times \dots \times E_p$$

1. Métrique produit

On munit E de la distance d définie par

$$\forall (x_1, \dots, x_p), (y_1, \dots, y_p) \in E, \quad \max_{i \in \llbracket 1; p \rrbracket} d_i(x_i, y_i)$$

Remarque : pour tout $x = (x_1, \dots, x_p) \in E$ et $\varepsilon > 0$

$$B_d(x, \varepsilon) = \{(y_1, \dots, y_p) \in E, \quad \forall i \in \llbracket 1; p \rrbracket, d_i(x_i, y_i) < \varepsilon\} = B_{d_1}(x_1, \varepsilon) \times \dots \times B_{d_p}(x_p, \varepsilon)$$

Vocabulaire : on appelle pavé ouvert tout produit de la forme $\omega_1 \times \dots \times \omega_p$ avec pour tout $i \in \llbracket 1; p \rrbracket$, ω_i un ouvert de E_i .

Proposition II.1.

1. Tout pavé ouvert est ouvert dans E .
2. Tout ouvert de E est réunion de pavés ouverts.

Preuve

1. Soit $\Omega = \omega_1 \times \cdots \times \omega_p$ un pavé ouvert. soit $x = (x_1, \dots, x_p) \in \Omega$. On a pour tout $i \in \llbracket 1; p \rrbracket$, il existe $\varepsilon_i > 0$ tel que $B_{d_i}(x_i, \varepsilon_i) \subset \omega_i$. On pose alors $\varepsilon = \min_{i \in \llbracket 1; p \rrbracket} \varepsilon_i > 0$. Le choix de ε nous permet d'affirmer que $B(x, \varepsilon) \subset B_{d_1}(x_1, \varepsilon_1) \times \cdots \times B_{d_p}(x_p, \varepsilon_p) \subset \Omega$ donc Ω est ouvert.
2. Soit Ω un ouvert de E . Pour tout $a \in \Omega$, il existe $\varepsilon_a > 0$ tel que $B(a, \varepsilon_a) \subset \Omega$. On peut alors écrire $\Omega = \bigcup_{a \in \Omega} B(a, \varepsilon_a)$. Une boule ouverte de E est par définition un pavé ouvert, donc Ω est bien une union de pavés ouverts.

Proposition II.2.

Soit F_1, \dots, F_p des parties de E_1, \dots, E_p . Si pour tout $i \in \llbracket 1; p \rrbracket$, F_i est fermé dans E_i , alors $F = F_1 \times \cdots \times F_p$ est fermé dans E .

Preuve : Commeons par remarquer que $F = F_1 \times \cdots \times F_p = \bigcap_{i=1}^p G_i$ avec pour tout $i \in \llbracket 1; p \rrbracket$,

$$G_i = E_1 \times \cdots \times E_{i-1} \times F_i \times E_{i+1} \times \cdots \times E_p$$

Or on a pour tout $i \in \llbracket 1; p \rrbracket$,

$$E \setminus G_i = E_1 \times \cdots \times E_{i-1} \times (E_i \setminus F_i) \times E_{i+1} \times \cdots \times E_p$$

$E \setminus G_i$ est un produit de d'ouverts, il est donc ouvert et alors G_i est fermé. Finalement, on en déduit que F est intersection de fermés, il est donc fermé.

Exemple : placons nous dans le cas où $E = \mathbb{R}^p$.

- La distance associée à \mathbb{R}^p est la distance induite par $\|\cdot\|_\infty$.
- Pour tout $x = (x_1, \dots, x_p) \in \mathbb{R}^p$ et $\varepsilon > 0$, $B(x, \varepsilon) =]x_1 - \varepsilon, x_1 + \varepsilon[\times \cdots \times]x_p - \varepsilon, x_p + \varepsilon[$.
- Les pavés ouverts s'écrivent sous forme de $\omega_1 \times \cdots \times \omega_p$ avec pour tout $i \in \llbracket 1; p \rrbracket$, ω_i un ouvert de \mathbb{R} .
- Tout ouvert de \mathbb{R}^p est réunion d'ensembles de la forme $]x_1 - \varepsilon, x_1 + \varepsilon[\times \cdots \times]x_p - \varepsilon, x_p + \varepsilon[$.

Proposition II.3.

1. Pour tout $k \in \llbracket 1; p \rrbracket$, π_k est 1-lipschitzienne.
2. Pour tout $k \in \llbracket 1; p \rrbracket$, si Ω est un ouvert de E , $\pi_k(\Omega)$ est ouvert.

Preuve : soit $k \in \llbracket 1; p \rrbracket$.

1. Il suffit d'écrire la définition de la 1-lipschitzianité de π_k . En effet, on a pour tous $x, y \in E$, $d_k(\pi_k(x), \pi_k(y)) = d_k(x_k, y_k) \leq d(x, y)$.
2. Soit Ω un ouvert de E . Soit $a = (a_1, \dots, a_p) \in \Omega$ et $\varepsilon > 0$ tel que $B(a, \varepsilon) \subset \Omega$. On a alors $B_{d_k}(a_k, \varepsilon) = \pi_k(B(a, \varepsilon)) \subset \pi_k(\Omega)$, donc $\pi_k(\Omega)$ est ouvert.

Attention : si F est un fermé de E , sa projection $\pi_k(F)$ avec $k \in \llbracket 1; p \rrbracket$ n'est pas forcément un fermé. En effet, dans le cas où $E = \mathbb{R}^2$, on peut considérer $F = \{(x, y) \in \mathbb{R}^2, xy = 1\}$ qui est fermé car l'image réciproque du fermé $\{1\}$ par l'application continue $(x, y) \mapsto xy$, mais $\pi_1(F) = \mathbb{R}^*$ n'est pas fermé.

2. Fonctions à valeurs dans un espace produit

Proposition II.4.

Soit $(x_n)_{n \in \mathbb{N}} = (x_{n,1}, \dots, x_{n,p}) \in E^{\mathbb{N}}$ et $x = (x_1, \dots, x_p) \in E$. Les propositions suivantes sont équivalentes.

1. $x_n \xrightarrow[n \rightarrow +\infty]{} x$
2. $\forall i \in \llbracket 1; p \rrbracket, x_{n,i} \xrightarrow[n \rightarrow +\infty]{} x_i$

Preuve

(1) \Rightarrow (2) Si $x_n \xrightarrow[n \rightarrow +\infty]{} x$, alors pour tout $i \in \llbracket 1; p \rrbracket$, par continuité de π_i (π_i est 1-lipschitzienne donc continue)

$$x_{n,i} = \pi_i(x_n) \xrightarrow[n \rightarrow +\infty]{} \pi_i(x) = x_i$$

(2) \Rightarrow (1) Il suffit d'écrire la définition de la distance

$$d(x_n, x) = \max_{i \in \llbracket 1; p \rrbracket} d_i(x_{n,i}, x_i) \xrightarrow[n \rightarrow +\infty]{} 0$$

Proposition II.5.

Soit A un ensemble, f une fonction de A dans E et $a \in \overline{A}$. On pose pour tout $x \in A$, $f(x) = (f_1(x), \dots, f_p(x))$ avec pour tout $i \in \llbracket 1; p \rrbracket$, f_i une fonction de A dans E_i . On a alors équivalence entre les points suivants

1. f admet une limite $l = (l_1, \dots, l_p)$ en a .
2. Pour tout $i \in \llbracket 1; p \rrbracket$, f_i admet la limite l_i en a .

Preuve : la preuve se fait d'une manière identique à celle pour les suites et est donc laissée comme exercice au lecteur.

Proposition II.6.

On reprend les notations précédentes et on considère cette fois-ci que $a \in A$. la propriété précédente implique l'équivalence entre les deux points suivants

1. f est continue en a .
2. Pour tout $i \in \llbracket 1; p \rrbracket$, f_i est continue en a_i .

3. Fonctions d'un espace produit

Dans cette partie, on considère Y un ensemble et pour tout $f \in Y^E$, $i \in \llbracket 1; p \rrbracket$ et $a \in E$, on désigne par i -ème application partielle de f en a l'application

$$f_{a,i} : \begin{cases} E_i & \longrightarrow Y \\ x & \longmapsto f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_p) \end{cases}$$

Proposition II.7.

Soit $f : E \longrightarrow Y$ et $a \in E$ une application. Si f est continue, alors ses toutes se sapplications partielles en a sont continues.

Preuve : considérons pour tout $i \in \llbracket 1; p \rrbracket$, l'application

$$j_{a,i} : \begin{cases} E_i & \longrightarrow E \\ x & \longmapsto (a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_p) \end{cases}$$

Cette application est une isométrie, elle est donc continue. Or on a pour tout $i \in \llbracket 1; p \rrbracket$, $f_{a,i} = f \circ j_{a,i}$. $f_{a,i}$ est composition de fonctions continues, elle est donc continue.

Définition II.8.

On considère le cas particulier où pour tout $i \in \llbracket 1; p \rrbracket$, E_i est un intervalle ouvert de \mathbb{R} et Y est un espace vectoriel normé. Pour tout $i \in \llbracket 1; p \rrbracket$, on appelle i -ème dérivée partielle partielle de f lorsqu'elle existe, l'application suivante

$$\frac{\partial f}{\partial x_i} : \begin{cases} E & \longrightarrow Y \\ x & \longmapsto \lim_{t_i \rightarrow x_i} \frac{f_{x,i}(t_i) - f_{x,i}(x_i)}{t_i - x_i} \end{cases}$$

Cette dernière associe un réel x à la dérivée de la i -ème application partielle de f en x au point x_i .

Vocabulaire : une fonction de E vers Y continue, qui admet des dérivées partielles continues est dite dans \mathcal{C}^1 .

Attention : la continuité des applications partielles de f n'implique pas la continuité de f . En effet, il suffit de considérer l'application suivante

$$f : \begin{cases} \mathbb{R}^2 & \longrightarrow \mathbb{R} \\ (x, y) & \longmapsto \begin{cases} \frac{xy}{x^2+y^2} & \text{si } (x, y) \neq (0, 0) \\ 0 & \text{sinon} \end{cases} \end{cases}$$

Les applications partielles de f en tout point de \mathbb{R}^2 sont continues sur \mathbb{R} , mais f n'est pas continue en $(0, 0)$, car en considérant la suite qui tends vers 0 , $((\frac{1}{n}, \frac{1}{n}))_{n \in \mathbb{N}^*}$ on voit que pour tout $n \in \mathbb{N}^*$ $f(\frac{1}{n}, \frac{1}{n}) = \frac{1}{2}$ et ne tend donc pas vers 0 , ce qui fait que f n'est pas continue en $(0, 0)$.

Exercice II.9.

Soit f une application de \mathbb{R}^2 dans \mathbb{R} qui admet des applications partielles continues en tout point de \mathbb{R}^2 . Montrer que f est limite simple d'une suite de fonctions continues.

4. Polynômes à plusieurs indéterminées

Dans cette partie, pour tout $\alpha \in \mathbb{N}^n$, on note $\alpha_1, \dots, \alpha_n$ ses coordonnées. On appellera tout élément $\alpha \in \mathbb{N}^n$ un multi-indice.

Définition II.10.

Soit \mathbb{K} un corps. On pose $\mathbb{K}[X_1, \dots, X_n]$ l'ensemble des sommes de la forme

$$P(X_1, \dots, X_n) = \sum_{(\alpha_1, \dots, \alpha_n) \in A} a_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

Avec A une partie finie de \mathbb{N}^n . Dans toute la suite de cette partie, on fixe $P \in \mathbb{K}[X_1, \dots, X_n]$.

Remarque : en première année, les polynômes ont été vus comme des suites stationnaires en 0. De la même manière, on peut voir les polynômes de $\mathbb{K}[X_1, \dots, X_n]$ comme des suites à valeurs dans \mathbb{K} indexées par \mathbb{N}^n et dont le nombre de termes non nuls est fini. Ici par exemple, on se limite dans la somme aux indices $(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ tels que $a_{\alpha_1, \dots, \alpha_n} \neq 0$, mais sachant qu'il y a un nombre fini de coefficients non nuls, on aurait pu écrire

$$P(X_1, \dots, X_n) = \sum_{(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n} a_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

Vocabulaire : Soit $(\alpha_1, \dots, \alpha_n) \in A$.

- $a_{\alpha_1, \dots, \alpha_n}$ est un coefficient de P .
- $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ est un monôme.
- Le degré total du monôme $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ est $\alpha_1 + \dots + \alpha_n$.
- Pour tout $i \in \llbracket 1; n \rrbracket$, le degré partiel du monôme $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ en X_i est α_i .
- Le degré de P est défini par $\deg P = \max_{\alpha \in A'} (\alpha_1 + \dots + \alpha_n)$ avec A' l'ensemble des multi-indices α tels que $a_\alpha \neq 0$.

Définition II.11.

Soit $d \in \mathbb{N}$. On dit que P est homogène de degré d si

$$\forall (\alpha_1, \dots, \alpha_n) \in A, a_{\alpha_1, \dots, \alpha_n} \neq 0 \implies \alpha_1 + \dots + \alpha_n = d$$

L'ensemble des polynômes homogènes de degré d est noté $H_d(X_1, \dots, X_n)$.

Proposition II.12.

Soit $P = \sum_{(\alpha_1, \dots, \alpha_n) \in A} a_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n}$ et $Q = \sum_{(\alpha_1, \dots, \alpha_n) \in B} b_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n}$ deux éléments de $\mathbb{K}[X_1, \dots, X_n]$. On pose $C = A \cup B$.

$$1. P + Q = \sum_{(\alpha_1, \dots, \alpha_n) \in C} (a_{\alpha_1, \dots, \alpha_n} + b_{\alpha_1, \dots, \alpha_n}) X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

$$2. P \cdot Q = \sum_{(\alpha, \beta) \in A \times B} a_\alpha b_\beta X_1^{\alpha_1 + \beta_1} \dots X_n^{\alpha_n + \beta_n}$$

Proposition II.13.

Soit d et d' deux éléments de \mathbb{N} .

1. Si $P \in H_d(X_1, \dots, X_n)$ et $Q \in H_{d'}(X_1, \dots, X_n)$, alors $PQ \in H_{d+d'}(X_1, \dots, X_n)$.
2. $\mathbb{K}[X_1, \dots, X_n] = \bigoplus_{k \in \mathbb{N}} H_k(X_1, \dots, X_n)$
3. $\mathbb{K}[X_1, \dots, X_n]$ est une \mathbb{K} -algèbre commutative unitaire intègre.

Preuve

1. Soit P et Q deux éléments appartenant respectivement à $H_d(X_1, \dots, X_n)$ et $H_{d'}(X_1, \dots, X_n)$. Soit A (resp. B) l'ensemble des multi-indices α (resp. β) tels que $a_\alpha \neq 0$ (resp. $b_\beta \neq 0$). On a alors

$$P = \sum_{(\alpha_1, \dots, \alpha_n) \in A} a_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n} \text{ et } Q = \sum_{(\alpha_1, \dots, \alpha_n) \in B} b_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

On a

$$PQ = \sum_{(\alpha, \beta) \in A \times B} a_\alpha b_\beta X_1^{\alpha_1 + \beta_1} \dots X_n^{\alpha_n + \beta_n}$$

et pour tout $(\alpha, \beta) \in A \times B$, $\alpha_1 + \beta_1 + \dots + \alpha_n + \beta_n = d + d'$, donc $PQ \in H_{d+d'}(X_1, \dots, X_n)$.

2. Soit $P \in \mathbb{K}[X_1, \dots, X_n]$. Il suffit de diviser la somme de P selon le degré de chaque monome. En effet, on a

$$P = \sum_{(\alpha_1, \dots, \alpha_n) \in A} a_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n} = \underbrace{\sum_{d=0}^{\deg P} \sum_{\substack{(\alpha_1, \dots, \alpha_n) \in A \\ \alpha_1 + \dots + \alpha_n = d}} a_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n}}_{\in H_d(X_1, \dots, X_n)}$$

L'unicité de cette écriture découle du fait qu'un polynôme nul est nécessairement à coefficients nuls, on a donc bien $P \in \bigoplus_{k \in \mathbb{N}} H_k(X_1, \dots, X_n)$, d'où le résultat voulu.

3. Le fait que $\mathbb{K}[X_1, \dots, X_n]$ soit une algèbre commutative ne présente pas de difficulté majeure, nous allons donc uniquement montrer que cette algèbre est intègre.

Soit $P, Q \in \mathbb{K}[X_1, \dots, X_n] \setminus \{0\}$. On pose

$$P = \sum_{(\alpha_1, \dots, \alpha_n) \in A} a_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n} \text{ et } Q = \sum_{(\alpha_1, \dots, \alpha_n) \in B} b_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

Posons aussi

$$PQ = \sum_{(\alpha_1, \dots, \alpha_n) \in C} c_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

Considérons $\alpha, \beta \in \mathbb{N}^n$ maximaux pour l'ordre lexicographique tels que $a_\alpha \neq 0$ et $b_\beta \neq 0$.

Le coefficient devant $X^{\alpha_1 + \beta_1} \dots X^{\alpha_n + \beta_n}$ est $a_\alpha b_\beta = c_{\alpha+\beta}$ et $\alpha + \beta$ est le multi-indice maximal pour l'ordre lexicographique vérifiant $c_{\alpha+\beta} \neq 0$. PQ admet donc un coefficient non nul ce qui nous permet de déduire qu'il est non nul, d'où l'intégrité de $\mathbb{K}[X_1, \dots, X_n]$.

Définition II.14.

Soit $P = \sum_{(\alpha_1, \dots, \alpha_n) \in A} a_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n}$ un élément de $\mathbb{K}[X_1, \dots, X_n]$.

On appelle fonction polynôme associée à P la fonction

$$\tilde{P} : \begin{cases} \mathbb{K}^n & \longrightarrow \mathbb{K} \\ (x_1, \dots, x_p) & \longmapsto \sum_{(\alpha_1, \dots, \alpha_n) \in A} a_{\alpha_1, \dots, \alpha_n} x_1^{\alpha_1} \dots x_n^{\alpha_n} \end{cases}$$

Proposition II.15.

Lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$, pour tout $P \in \mathbb{K}[X_1, \dots, X_n]$, \tilde{P} est continue.

Preuve : pour tout $i \in \llbracket 1; p \rrbracket$, $\tilde{X}_i = \pi_i$, donc \tilde{X}_i est continue. Pour tout $P \in \mathbb{K}[X_1, \dots, X_n]$, la fonction \tilde{P} est produit et combinaison linéaire des fonctions continues \tilde{X}_i avec $i \in \llbracket 1; n \rrbracket$, elle est donc continue.

Proposition II.16.

Soient A_1, \dots, A_n des parties infinies de \mathbb{K} . Soit $P \in \mathbb{K}[X_1, \dots, X_n]$. Si \tilde{P} s'annule sur $A_1 \times \dots \times A_n$, alors P est nul.

Preuve : montrons ce résultat par récurrence sur n .

Lorsque $n = 1$, P est un polynôme à une seule indéterminée qui s'annule en un nombre infini de points, il est donc nul.

Soit $n \geq 2$. Soit $P = \sum_{(\alpha_1, \dots, \alpha_n) \in A} a_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n} \in \mathbb{K}[X_1, \dots, X_n]$. Réécrivons P de la manière suivante

$$P = \sum_{k=0}^N Q_k(X_1, \dots, X_{n-1}) X_n^k$$

avec $N \in \mathbb{N}$ et pour tout $k \in \llbracket 1; N \rrbracket$, $Q_k \in \mathbb{K}[X_1, \dots, X_{n-1}]$.

Soit $(a_1, \dots, a_{n-1}) \in A_1 \times \dots \times A_{n-1}$. Pour tout $a_n \in A_n$,

$$\tilde{P}(a_1, \dots, a_{n-1}, a_n) = \sum_{k=0}^N Q_k(a_1, \dots, a_{n-1}) a_n^k = 0$$

le polynôme $R(Y) = \sum_{k=0}^N Q_k(a_1, \dots, a_{n-1}) Y^k$ est nul sur A_n et possède donc une infinité de racines. Ce

polynôme est donc nul. On peut alors affirmer que pour tout $k \in \llbracket 1; N \rrbracket$ et $(a_1, \dots, a_{n-1}) \in A_1 \times \dots \times A_{n-1}$, $Q_k(a_1, \dots, a_{n-1}) = 0$. Q_k s'annule donc sur $A_1 \times \dots \times A_{n-1}$ et alors par hypothèse de récurrence, pour tout $k \in \llbracket 1; N \rrbracket$, $Q_k = 0$ et finalement $P = 0$.

Exercice II.17.

Montrer que $GL_n(\mathbb{C}) = \{M \in \mathcal{M}_n(\mathbb{C}), \det M \neq 0\}$ est ouvert.

Exercice II.18.

Soit $P \in \mathbb{C}[X_1, \dots, X_n] \setminus \{0\}$. Montrer que $Z(P) = \{(x_1, \dots, x_n) \in \mathbb{C}^n, \tilde{P}(x_1, \dots, x_n) = 0\}$ est fermé d'intérieur vide.

Exercice II.19.

Soit $P \in \mathbb{C}[X, Y]$ non consant. Montrer que $Z(P)$ est infini.

Correction de l'exercice I.6 :

Commençons démontrer le lemme suivant.

Lemme II.20.

Soit f une fonction continue et g une fonction de signe constant sur $[a, b]$ non identiquement nulle. Il existe $c \in [a, b]$ tel que

$$\int_a^b f(t)g(t)dt = f(c) \int_a^b g(t)dt$$

Preuve : on suppose sans perte de généralité que g est positive. On a alors $\int_a^b g(t)dt > 0$. Soit $\alpha, \beta \in [a, b]$ telle que $f(\alpha) = \inf_{t \in [a, b]} f(t)$ et $f(\beta) = \sup_{t \in [a, b]} f(t)$. On a

$$\int_a^b f(\alpha)g(t)dt \leq \int_a^b f(t)g(t)dt \leq \int_a^b f(\beta)g(t)dt$$

et alors

$$f(\alpha) \leq \frac{\int_a^b f(t)g(t)dt}{\int_a^b g(t)dt} \leq f(\beta) \quad (*)$$

f étant continue, le théorème des valeurs intermédiaires nous permet d'affirmer l'existence d'un réel $c \in [a, b]$ tel que

$$\frac{\int_a^b f(t)g(t)dt}{\int_a^b g(t)dt} = f(c)$$

d'où le résultat voulu.

Remarque : l'inégalité $(*)$ est en général fausse lorsque g n'est pas de signe constant.

Montrons à présent que l'intégrale de l'exercice converge vers la quantité voulue.

Soit $n \in \mathbb{N}^*$, on a

$$\int_0^1 f(t) |\sin(nt)| dt = \sum_{k=0}^{\lfloor \frac{n}{2\pi} \rfloor - 1} \int_{\frac{2k\pi}{n}}^{\frac{(2k+1)\pi}{n}} f(t) \sin(nt) dt - \int_{\frac{(2k+1)\pi}{n}}^{\frac{(2k+2)\pi}{n}} f(t) \sin(nt) dt + \int_{\lfloor \frac{n}{2\pi} \rfloor \frac{2\pi}{n}}^1 f(t) |\sin(nt)| dt$$

En appliquant le lemme précédent sur les deux premières intégrales ci-dessus, on peut affirmer, pour tout $k \in \llbracket 0; \lfloor \frac{n}{2\pi} \rfloor - 1 \rrbracket$ l'existence de $c_{k,n} \in [\frac{2k\pi}{n}, \frac{(2k+1)\pi}{n}]$ et $c'_{k,n} \in [\frac{(2k+1)\pi}{n}, \frac{(2k+2)\pi}{n}]$ tels que

$$\int_{\frac{2k\pi}{n}}^{\frac{(2k+1)\pi}{n}} f(t) \sin(nt) dt = f(c_{k,n}) \int_{\frac{2k\pi}{n}}^{\frac{(2k+1)\pi}{n}} \sin(nt) dt = \frac{2}{n} f(c_{k,n})$$

et

$$\int_{\frac{(2k+1)\pi}{n}}^{\frac{(2k+2)\pi}{n}} f(t) \sin(nt) dt = f(c'_{k,n}) \int_{\frac{(2k+1)\pi}{n}}^{\frac{(2k+2)\pi}{n}} \sin(nt) dt = -\frac{2}{n} f(c'_{k,n})$$

On a alors, en posant $\tilde{c}_{k,n} = c_{\frac{k}{2},n}$ si k pair et $\tilde{c}_{k,n} = c'_{\frac{k-1}{2},n}$ sinon, on obtient

$$\begin{aligned} \int_0^1 f(t) |\sin(nt)| dt &= \frac{2}{n} \sum_{k=0}^{\lfloor \frac{n}{2\pi} \rfloor - 1} f(c_{k,n}) + \frac{2}{n} \sum_{k=0}^{\lfloor \frac{n}{2\pi} \rfloor - 1} f(c'_{k,n}) + \int_{\lfloor \frac{n}{2\pi} \rfloor \frac{2\pi}{n}}^1 f(t) |\sin(nt)| dt \\ &= \frac{2}{\pi} \left(\sum_{k=0}^{2\lfloor \frac{n}{2\pi} \rfloor - 1} \frac{\pi}{n} f(\tilde{c}_{k,n}) \right) + \int_{\lfloor \frac{n}{2\pi} \rfloor \frac{2\pi}{n}}^1 f(t) |\sin(nt)| dt \end{aligned}$$

La somme dans la ligne ci-dessus est une somme de Riemann sur $[0, 1]$, donc elle converge vers $\int_0^1 f(t) dt$. De plus $t \mapsto f(t) |\sin(nt)|$ est bornée uniformément (sa borne supérieure ne dépend pas de n) sur $[0, 1]$ et $\lfloor \frac{n}{2\pi} \rfloor \frac{2\pi}{n} \xrightarrow[n \rightarrow +\infty]{} 1$, donc

$$\int_{\lfloor \frac{n}{2\pi} \rfloor \frac{2\pi}{n}}^1 f(t) |\sin(nt)| dt \xrightarrow[n \rightarrow +\infty]{} 0$$

On en déduit donc directement que

$$\int_0^1 f(t) |\sin(nt)| dt \xrightarrow[n \rightarrow +\infty]{} \frac{2}{\pi} \int_0^1 f(t) dt$$

Correction de l'exercice 2 :

On a pour tout $P = \sum_{k=0}^n a_k X^k \in E$,

$$\|P\|_0 = \max(|a_0|, \dots, |a_n|) \geq \frac{1}{n} \sum_{k=0}^n |a_k| \geq \frac{1}{n} \max(|a_0|, \dots, |a_n|) = \frac{1}{n} \|P\|_0$$

donc

$$\|P\|_0 \geq \frac{1}{n} \|P\|_1 \geq \frac{1}{n} \|P\|_0$$

et alors $\|\cdot\|_0 \sim \|\cdot\|_1$.

On a aussi

$$\|P\|_\infty \leq \sum_{k=0}^n |a_k| = \|P\|_1$$

donc $\|\cdot\|_1$ est plus fine que $\|\cdot\|_\infty$, mais $\|\cdot\|_\infty$ n'est pas toujours plus fine que $\|\cdot\|_1$.

En effet, si on considère la suite le polynôme $P_n = \sum_{k=1}^n (-1)^k k X^{k-1}$, on a pour tout $x \in [0, 1]$,

$$\begin{aligned} \tilde{P}_n(x) &= \left(\sum_{k=0}^n -x^k \right)' = \left(x \frac{1 - (-x)^n}{1+x} \right)' \\ &= -x \frac{1 - (-x)^n}{(1+x)^2} + \frac{1 - (-x)^n}{1+x} - \frac{n(-x)^n}{1+x} \end{aligned}$$

on a alors pour tout $x \in [0, 1]$

$$|\tilde{P}_n(x)| \leq \left| x \frac{1 - (-x)^n}{(1+x)^2} \right| + \left| \frac{1 - (-x)^n}{1+x} \right| + \left| \frac{n(-x)^n}{1+x} \right| \leq 2 + 2 + n = n + 4$$

et donc $\|P_n\|_\infty \leq n + 4$.

On a aussi $\|P_n\|_1 = \sum_{k=1}^n k = \frac{n(n+1)}{2}$, donc s'il existe $C > 0$ tel que pour tout $n \in \mathbb{N}$,

$\|P_n\|_1 \leq C \|P_n\|_\infty$, alors on aura $\frac{n(n+1)}{2} \leq C(n+4)$ ce qui est faux pour n assez grand, d'où le résultat voulu.

Correction de l'exercice 3 :

On va approcher f par une suite de fonctions de première application partielle affine par morceaux. Soit $n \in \mathbb{N}^*$. On subdivise \mathbb{R} en la famille d'intervalles $([\frac{k}{n}, \frac{k+1}{n}[)_{k \in \mathbb{Z}}$. Pour tout $n \in \mathbb{N}^*$, on définit f_n de la manière suivante : pour tout $(x, y) \in \mathbb{R}^2$ et $k \in \mathbb{Z}$, si $x \in [\frac{k}{n}, \frac{k+1}{n}[$, on pose $x = \frac{k+\varepsilon_{n,x}}{n}$ avec $\varepsilon_{n,x} = nx - \lfloor nx \rfloor \in [0, 1[$. On a alors

$$f_n(x, y) = f\left(\frac{k}{n}, y\right) + \varepsilon_{n,x} \left(f\left(\frac{k+1}{n}, y\right) - f\left(\frac{k}{n}, y\right) \right)$$

Montrons que pour tout $n \in \mathbb{N}^*$, f_n est continue. Soit $n \in \mathbb{N}$ et $x \in \mathbb{R}$, soit $k \in \mathbb{Z}$ tel que $x \in [\frac{k}{n}, \frac{k+1}{n}[$.

→ Cas $x \in]\frac{k}{n}, \frac{k+1}{n}[$

$]\frac{k}{n}, \frac{k+1}{n}[$ étant ouvert, on peut supposer que tous les couples considérés sont dans $]\frac{k}{n}, \frac{k+1}{n}[\times \mathbb{R}$. On pose alors pour tout $u \in]\frac{k}{n}, \frac{k+1}{n}[$, $u = \frac{k+\varepsilon_{n,u}}{n}$ avec $\varepsilon_{n,u} \in [0, 1[$. On a alors, lorsque $(u, v) \rightarrow (x, y)$, $\varepsilon_{n,u} \rightarrow \varepsilon_{n,x}$ et par continuité de la seconde application partielle de f

$$\begin{aligned} f_n(u, v) &= f\left(\frac{k}{n}, v\right) + \varepsilon_{n,u} \left(f\left(\frac{k+1}{n}, v\right) - f\left(\frac{k}{n}, v\right) \right) \\ &\xrightarrow{(u,v) \rightarrow (x,y)} f\left(\frac{k}{n}, y\right) + \varepsilon_{n,x} \left(f\left(\frac{k+1}{n}, y\right) - f\left(\frac{k}{n}, y\right) \right) = f(x, y) \end{aligned}$$

donc f_n est continue en (x, y)

→ Cas $x = \frac{k}{n}$

Étudions séparément la continuité à droite et à gauche.

- Continuité pour u à droite de $\frac{k}{n}$

Lorsque $(u, v) \in [\frac{k}{n}, \frac{k+1}{n}[\times \mathbb{R}$, si $(u, v) \rightarrow (\frac{k}{n}, y)$, alors $\varepsilon_{n,u} \rightarrow 0$ et $f\left(\frac{k+1}{n}, v\right) - f\left(\frac{k}{n}, v\right)$ reste bornée. On peut donc affirmer que

$$f_n(u, v) = f\left(\frac{k}{n}, v\right) + \varepsilon_{n,u} \left(f\left(\frac{k+1}{n}, v\right) - f\left(\frac{k}{n}, v\right) \right) \xrightarrow{(u,v) \rightarrow (x,y)} f\left(\frac{k}{n}, y\right)$$

d'où la continuité de f_n à gauche de x .

- Continuité pour u à gauche de $\frac{k}{n}$

Lorsque $(u, v) \in]\frac{k-1}{n}, \frac{k}{n}] \times \mathbb{R}$, si $(u, v) \rightarrow (\frac{k}{n}, y)$, alors $\varepsilon_{n,u} \rightarrow 1$ et

$$f_n(u, v) = f\left(\frac{k-1}{n}, v\right) + \varepsilon_{n,u} \left(f\left(\frac{k}{n}, v\right) - f\left(\frac{k-1}{n}, v\right) \right) \xrightarrow{(u,v) \rightarrow (x,y)} f\left(\frac{k}{n}, y\right)$$

d'où la continuité à gauche en $\frac{k}{n}$

On en déduit donc que pour tout n , f_n est continue sur \mathbb{R}^2 . Il reste maintenant à montrer que f_n converge simplement vers f .

Soit $(x, y) \in \mathbb{R}^2$. On a $\varepsilon_{n,x} \in [0, 1[$ et le terme $f\left(\frac{k+1}{n}, y\right) - f\left(\frac{k}{n}, y\right) \xrightarrow{n \rightarrow +\infty} 0$, car la première application de f est continue. On a alors

$$f_n(x, y) = f\left(\frac{k}{n}, y\right) + \varepsilon_{n,x} \left(f\left(\frac{k+1}{n}, y\right) - f\left(\frac{k}{n}, y\right) \right) \xrightarrow{n \rightarrow +\infty} f(x, y)$$

D'où la résultat voulu.

Correction de l'exercice 4 :

On a pour tout $M = (m_{i,j})_{i,j \in \llbracket 1; n \rrbracket} \in \mathcal{M}_n(\mathbb{C})$

$$\det M = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n m_{i,\sigma(i)}$$

L'application \det est alors polynômiale et donc continue. Or $GL_n(\mathbb{C}) = \det^{-1}(\mathbb{R}^*)$, il s'agit de l'image réciproque d'un ouvert par une application continue, c'est donc un ouvert.

Correction de l'exercice 5 :

On a $Z(P) = \tilde{P}^{-1}(\{0\})$, il s'agit de l'image réciproque d'un fermé par une application continue (car polynômiale), c'est donc un fermé.

Supposons que $Z(P)$ n'est pas d'intérieur vide. Il existe alors $\varepsilon > 0$ et $x = (x_1, \dots, x_n) \in Z(P)$ tel que $B(x, \varepsilon) \subset Z(P)$. P s'annule alors sur $B(x, \varepsilon) = B_{d_1}(x_1, \varepsilon) \times \dots \times B_{d_n}(x_n, \varepsilon)$. Pour tout $i \in \llbracket 1; n \rrbracket$, $B_{d_i}(x_i, \varepsilon)$ est infini. P s'annule sur le produit d'ensembles infinis, il est donc nul ce qui est absurde. On en déduit donc que $Z(P)$ est bien fermé d'intérieur vide.

Correction de l'exercice 6 :

On peut écrire P de la manière suivante

$$P(X, Y) = \sum_{k=0}^N Q_k(Y) X^k$$

avec $Q_N \neq 0$.

→ Cas $N = 0$

Lorsque $N = 0$, alors Q_0 est nécessairement non nul et admet au moins une racine qu'on note a .

On a alors pour tout $x \in \mathbb{C}$, $\tilde{P}(x, a) = 0$ ce qui implique que $\mathbb{C} \times \{a\} \subset Z(P)$. $Z(P)$ est donc infini.

→ Cas $N \geq 1$

$A = \{a \in \mathbb{C}, Q_N(a) \neq 0\}$ est infini. soit $a \in A$. $x \mapsto \tilde{P}(x, a)$ est une fonction polynômiale de degré N , elle admet donc au moins une racine b et donc $(a, b) \in Z(P)$. A étant infini, on peut construire une infinité de couples d'éléments distincts de $Z(P)$, $Z(P)$ est alors bien infini.



Compacité

CHAPITRE 11.5

Dans ce chapitre, on considère X un espace métrique muni d'une distance d . Tous les ensembles considérés sont, lorsque cela est nécessaire, non vides.

I Valeurs d'adhérence

Proposition I.1.

Soit $(x_n)_{n \in \mathbb{N}}$ une suite à valeurs dans X et $a \in X$. Les propriétés suivantes sont équivalentes.

1. $\forall \varepsilon > 0, \forall N \in \mathbb{N}, \exists n \geq N, x_n \in B(a, \varepsilon)$
2. Pour tout $\varepsilon > 0$, l'ensemble des indices n tels que $d(x_n, a) < \varepsilon$ est infini.
3. Il existe une extractrice φ telle que $x_{\varphi(n)} \xrightarrow[n \rightarrow +\infty]{} a$.

Lorsque ces propriétés sont vérifiées, on dit que a est une valeur d'adhérence de $(x_n)_{n \in \mathbb{N}}$.

Preuve

$$\rightarrow (1) \Rightarrow (2)$$

La proposition (1) implique que pour tout $\varepsilon > 0$, l'ensemble des indices $n \in \mathbb{N}$ telle que $d(a, x_n) < \varepsilon$ est non borné. Il est donc infini.

$$\rightarrow (2) \Rightarrow (3)$$

Construisons par récurrence une extractrice φ qui vérifie pour tout $n \in \mathbb{N}$, $d(a, x_{\varphi(n)}) < \frac{1}{n+1}$. Pour $n = 0$, l'ensemble $A_0 = \{n \in \mathbb{N}, d(a, x_n) < 1\}$ est infini donc non vide. On pose alors $\varphi(0) = m$ avec $m \in A$.

Soit $n \in \mathbb{N}$, supposons que $\varphi(0), \varphi(1), \dots, \varphi(n)$ sont correctement définis.

L'ensemble $A_n = \{k \in \mathbb{N}, d(a, x_k) < \frac{1}{n+2}\}$ est infini. On dispose donc de $r \in A_n$ tel que pour tout $i \in [1; n]$, $r > \varphi(i)$. On pose alors $\varphi(n+1) = r$, ce qui donne bien $d(a, x_{\varphi(n+1)}) < \frac{1}{n+2}$.

$$\rightarrow (3) \Rightarrow (1)$$

Soit $\varepsilon > 0$ et $N \in \mathbb{N}$. $x_{\varphi(n)} \xrightarrow[n \rightarrow +\infty]{} a$, donc il existe $n' \geq N$ tel que $x_{\varphi(n')} \in B(a, \varepsilon)$, il suffit alors de voir que $n = \varphi(n')$ vérifie la propriété voulue.

Notation : pour toute suite $(x_n) \in X^{\mathbb{N}}$, on note $Adh((x_n)_{n \in \mathbb{N}})$ l'ensemble des valeurs d'adhérence de (x_n) . Pour simplifier, et lorsqu'il n'y a pas ambiguïté, on notera $Adh((x_n)_{n \in \mathbb{N}})$ comme $Adh(x_n)$.

Proposition I.2.

Pour toute suite $(x_n) \in X^{\mathbb{N}}$, on a $Adh(x_n) = \bigcap_{p \in \mathbb{N}} \overline{\{x_n, n \geq p\}}$.

Preuve Posons pour tout $p \in \mathbb{N}$, $A_p = \{x_n, n \geq p\}$

$\rightarrow (\subset)$ Soit $a \in Adh(x_n)$. On a alors pour tout $p \in \mathbb{N}$, pour tout $\varepsilon > 0$ il existe $n \geq p$ tel que $x_n \in B(a, \varepsilon)$, i.e. $A_p \cap B(a, \varepsilon) \neq \emptyset$.

On peut alors affirmer que pour tout $p \in \mathbb{N}$, $a \in \overline{A_p}$, i.e. $a \in \bigcap_{p \in \mathbb{N}} \overline{A_p}$.

→ (⊇) Soit $a \in \bigcap_{p \in \mathbb{N}} \overline{A_p}$. Soit $\varepsilon > 0$ et $N \in \mathbb{N}$. $a \in \overline{A_N}$, donc pour tout $\varepsilon > 0$, il existe $n \geq N$ tel que $x_n \in B(a, \varepsilon)$, i.e. $a \in Adh(x_n)$.

II Définitions et propriétés structurelles

Définition II.1.

L'espace métrique (X, d) est dit compact lorsque toute suite à aleurs dans X admet une valeur d'adhérence dans A .

Une partie A de X est dite compacte si elle l'est pour la distance induite.

Exemples

- Pour tout $a, b \in \mathbb{R}$ tel que $a \leq b$, $[a, b]$ est une partie compacte de \mathbb{R} .
- \mathbb{R} n'est pas compact pour la distance induite par la valeur absolue. En effet, si on considère la suite $(u_n)_{n \in \mathbb{N}}$ définie par $\forall n \in \mathbb{N}, u_n = n$, on peut voir que toute extractrice de u_n tend vers l'infini et donc (u_n) n'admet pas de valeur d'adhérence.
- $\overline{\mathbb{R}}$ est compact pour la distance $d : (x, y) \mapsto |\arctan(x) - \arctan(y)|$ (avec $\arctan(+\infty) = \frac{\pi}{2}$ et $\arctan(-\infty) = -\frac{\pi}{2}$).

Proposition II.2.

1. Si A est une partie compacte de X , alors A est fermée et bornée.
2. Soit Y une partie de X et A une partie de Y . Si Y est compact, alors

$$A \text{ est compact} \iff A \text{ est fermé}$$

Preuve

1. Soit A une partie compacte de X .

→ Montrons que A est fermé.

Soit $a \in \overline{A}$. Par définition, il existe une suite $(a_n) \in A^{\mathbb{N}}$ qui converge vers a . A est compact, il existe donc une extractrice φ telle que $(a_{\varphi(n)})$ converge vers $b \in A$. Par unicité de la limite, on a $a = b \in A$ et finalement $A = \overline{A}$, i.e. A est fermé.

→ Montrons que A est borné.

Si A est non borné, alors par définition il existe une suite $(a_n) \in A^{\mathbb{N}}$ et $a \in A$ tel que $d(a, a_n) \xrightarrow{n \rightarrow +\infty} +\infty$. Aucune suite extraite ne peut alors converger car pour toute extractrice φ et $x \in A$, $d(x, a_{\varphi(n)}) \geq d(a, a_{\varphi(n)}) - d(x, a) \xrightarrow{n \rightarrow +\infty} +\infty$.

2. (\Rightarrow) Le sens de gauche à droite est une simple conséquence de la propriété précédente.

(\Leftarrow) Supposons que A est fermé. Soit $(a_n) \in A^{\mathbb{N}}$. Y est compact, il existe donc une extractrice φ et un élément x de Y tel que $a_{\varphi(n)} \xrightarrow{n \rightarrow +\infty} x$. A étant fermé, on a nécessairement $x \in A$ et donc A est compact.

III Produit d'espaces compacts

Proposition III.1.

Soit $p \in \mathbb{N}^*$ et X_1, \dots, X_p des compacts munis des distances d_1, \dots, d_p . L'espace produit $X_1 \times \dots \times X_p$ est compact.

Preuve : Procédons par récurrence.

- Le cas $p = 1$ est évident.
- Soit $p \in \mathbb{N}^*$. Supposons que p vérifie la propriété voulue. Soit X_1, \dots, X_{p+1} $p + 1$ compacts et soit $(x_n)_{n \in \mathbb{N}} = ((x_{1,n}, \dots, x_{p+1,n}))_{n \in \mathbb{N}}$. L'espace produit $X_1 \times \dots \times X_p$ étant compact par hypothèse, il existe une extractrice φ telle que $(y_{\varphi(n)}) = (x_{1,\varphi(n)}, \dots, x_{p,\varphi(n)})_{n \in \mathbb{N}}$ converge vers $(a_1, \dots, a_p) \in X_1 \times \dots \times X_p$. X_{p+1} est compact, il existe donc une extractrice ψ telle que la suite $(x_{p+1,\varphi \circ \psi(n)})_{n \in \mathbb{N}}$ converge vers $a_{p+1} \in X_{p+1}$. On a alors

$$\begin{aligned} d(x_{\varphi \circ \psi(n)}, (a_1, \dots, a_{p+1})) &= \max_{i \in [1; p+1]} d_i(x_{i,\varphi \circ \psi(n)}, a_i) \\ &\leq d(y_{\varphi \circ \psi(n)}, (a_1, \dots, a_p)) + d_{p+1}(x_{p+1,\varphi \circ \psi(n)}, a_{p+1}) \xrightarrow{n \rightarrow +\infty} 0 \end{aligned}$$

La suite $(x_{\varphi \circ \psi(n)})_{n \in \mathbb{N}}$ converge donc bien vers $(a_1, \dots, a_{p+1}) \in X_1 \times \dots \times X_{p+1}$. L'espace $X_1 \times \dots \times X_{p+1}$ est donc bien compact.

Proposition III.2.

Soit $n \in \mathbb{N}^*$ et A une partie de \mathbb{R}^n munie de $\|\cdot\|_\infty$. A est compact si et seulement si il est fermé et borné.

Preuve

(⇒) Cette implication a déjà été montrée auparavant.

(⇐) Supposons que A est fermée et bornée. A étant borné, il existe $M \geq 0$ tel que pour tout $a \in A$, $\|a\|_\infty \leq M$. On a alors $A \subset [-M, M]^n$. $[-M, M]$ étant compact, $[-M, M]^n$ est un produit de compacts de \mathbb{R} , c'est donc un compact. A est fermé borné et est inclus dans un compact, il est donc compact d'après ce qui précéde.

Conséquence : par équivalence des normes en dimension finie, si on munit \mathbb{R}^n d'une norme quelconque $\|\cdot\|$, l'équivalence ci-dessus reste vraie.

Attention : cette équivalence est fausse en dimension infinie en général. En effet, pour le voir, il suffit de considérer l'exemple suivant.

On considère l'espace vectoriel normé $E = \mathcal{C}([0, 2\pi], \mathbb{R})$ muni de la norme $\|\cdot\|_2$ définie par

$$\forall f \in E \quad \|f\|_2 = \left(\int_0^{2\pi} f(t)^2 dt \right)^{\frac{1}{2}}$$

On considère la suite à la valeurs dans E $(f_n)_{n \in \mathbb{N}} = (x \mapsto \sin(nx))_{n \in \mathbb{N}}$.

On a pour tout $n \in \mathbb{N}$,

$$\|f_n\|_2^2 = \int_0^{2\pi} \sin(nt)^2 dt = \int_0^{2\pi} \frac{1 - \cos(2nt)}{2} = \pi$$

Donc (f_n) est une suite à valeurs dans $B_f(0, \pi)$ qui est une partie fermée bornée de E . et pour tout

$n, m \in \mathbb{N}$ tels que $m \neq n$,

$$\|f_n - f_m\|_2^2 = \int_0^{2\pi} (\sin(nt) - \sin(mt))^2 dt = \int_0^{2\pi} \sin(nt)^2 + \sin(mt)^2 - 2 \sin(nt) \sin(mt) dt = 2\pi$$

on en déduit que pour toute extractrice φ et tout $n \in \mathbb{N}$, $\|f_{\varphi(n)} - f_{\varphi(n+1)}\|_2 = \sqrt{2\pi}$ et donc $(f_{\varphi(n)})$ ne peut pas converger.

En résumé, on a trouvé une suite (f_n) à valeurs dans un fermé borné dont aucune suite extraite ne converge, donc $B_f(0, \pi)$ est fermé borné mais n'est pas compact.

Définition III.3.

Soit $(u_n)_{n \in \mathbb{N}}$ une suite à valeurs dans X . On dit que (u_n) est de Cauchy si

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, \forall m \geq N, d(u_n, u_m) < \varepsilon$$

Remarque : toute suite convergente est de Cauchy. Montrons ce résultat. Soit $\varepsilon > 0$ si $(u_n) \in X^{\mathbb{N}}$ est convergente vers une limite $u \in X$, il suffit de prendre $N \in \mathbb{N}$ assez grand pour qu'on ait pour tout $n \geq N$, $d(u_n, u) < \frac{\varepsilon}{2}$. On a alors pour tout $n, m \geq N$, $d(u_n, u_m) \leq d(u_n, u) + d(u_m, u) < \varepsilon$.

Attention : la réciproque est fausse. En effet, si on considère l'espace vectoriel normé $\mathbb{R}[X]$ muni de $\|\cdot\|_1$, et la suite $(P_n) \in \mathbb{R}[X]^{\mathbb{N}}$ définie par

$$\forall n \in \mathbb{N}, P_n(X) = \sum_{k=0}^n \frac{1}{2^k} X^k$$

Montrons que cette suite de Cauchy. Soit $\varepsilon > 0$, on a pour tout $m, n \in \mathbb{N}$, si $n > m$, alors

$$\|P_n - P_m\|_1 = \sum_{k=m+1}^n \frac{1}{2^k} \leq \sum_{k=m+1}^{+\infty} \frac{1}{2^k} = \frac{1}{2^m}$$

Il existe donc $N \in \mathbb{N}$ assez grand tel que pour tout $n, m > N$, $\frac{1}{2^m} < \varepsilon$ et alors $\|P_n - P_m\|_1 < \varepsilon$, donc (P_n) est de Cauchy.

En revanche, cette suite n'est pas convergente. En effet, pour tout polynôme Q de degré m , pour tout $n > m$,

$$\|P_n - Q\| \geq \sum_{k=m+1}^n \frac{1}{2^k} \xrightarrow{n \rightarrow +\infty} \frac{1}{2^m} \neq 0$$

(P_n) ne peut donc pas converger vers Q et alors (P_n) n'est pas convergente.

Définition III.4.

On dit que X est complet lorsque toute suite à valeurs dans X de Cauchy converge.

IV Suites dans un compact

Proposition IV.1.

Si X est compact, alors il est complet.

Preuve : supposons que X est compact. Soit $(u_n) \in X^{\mathbb{N}}$ une suite de Cauchy. Soit φ une extractrice et

$u \in X$ tels que $u_{\varphi(n)} \xrightarrow{n \rightarrow +\infty} u$. Soit $\varepsilon > 0$ et $N \in \mathbb{N}$ tel que pour tout $m, n \geq N$ $d(u_n, u_m) < \frac{\varepsilon}{2}$. Soit $N' \in \mathbb{N}$ tel pour tout $n \geq N'$ $d(u_{\varphi(n)}, u) < \frac{\varepsilon}{2}$. On a alors

$$\forall n \geq \max(N, N'), d(u_n, u) \leq d(u_n, u_{\varphi(n)}) + d(u_{\varphi(n)}, u) < \varepsilon$$

(u_n) est bien convergente et donc X est complet.

Remarque : la preuve ci-dessus nous dévoile un résultat utile : peu importe l'espace X , une suite $(u_n) \in X^{\mathbb{N}}$ de Cauchy qui admet une valeur d'adhérence est convergente. Plus généralement, une suite de Cauchy admet au plus une seule valeur d'adhérence.

Attention : la réciproque de ce résultat est fausse. En effet, \mathbb{R} est complet mais n'est pas compact. Montrons ce résultat. Si $(u_n) \in \mathbb{R}^{\mathbb{N}}$ est de Cauchy, alors il existe $N \in \mathbb{N}$ tel que pour tous $m, n \geq N$, $|u_n - u_m| < \varepsilon$. En prenant $\varepsilon = 1$, on voit que pour tout $n \geq N$, $|u_n - u_N| < 1$. On en déduit donc immédiatement que (u_n) est bornée par $\max(|u_0|, |u_1|, \dots, |u_{N-1}|, |u_N|) + 1$. On peut donc appliquer Bolzano-Weierstrass pour affirmer que (u_n) admet une valeur d'adhérence. (u_n) est une suite de Cauchy qui admet une valeur d'adhérence, elle est donc convergente et donc \mathbb{R} est complet.

Proposition IV.2.

On suppose que X est compact. Soit $(u_n) \in X^{\mathbb{N}}$. On a alors

$$(u_n) \text{ converge} \iff (u_n) \text{ admet au plus une valeur d'adhérence}$$

Preuve

(\Rightarrow) Cette implication ne présente pas de difficulté et est laissée comme exercice au lecteur.

(\Leftarrow) Par compacité de X , (u_n) admet au moins une valeur d'adhérence, donc (u_n) admet exactement une valeur d'adhérence qu'on note u . Supposons que (u_n) ne converge pas vers u . Il existe donc $\varepsilon > 0$ tel que $A_\varepsilon = \{n \in \mathbb{N}, d(u_n, u) \geq \varepsilon\}$ est infini. On considère alors φ une extractrice telle que $\varphi(\mathbb{N}) \subset A_\varepsilon$. Par construction, on a pour tout $n \in \mathbb{N}$, $d(u_{\varphi(n)}, u) \geq \varepsilon$. Mais $(u_{\varphi(n)})$ est à valeurs dans le compact X , donc il existe $x \in X$ et ψ une extractrice telle que $u_{\varphi \circ \psi(n)} \xrightarrow{n \rightarrow +\infty} x$, mais $\varepsilon \leq d(u_{\varphi \circ \psi(n)}, u) \xrightarrow{n \rightarrow +\infty} d(x, u)$, donc $x \neq u$. On a trouvé une valeur d'adhérence de (u_n) différente de u ce qui est absurde.

Exercice IV.3.

Soit $d \in \mathbb{N}^*$ et $(u_n) \in (\mathbb{R}^d)^{\mathbb{N}}$ vérifiant les propriétés suivantes.

1. (u_n) est bornée.
2. (u_n) possède un nombre fini de valeurs d'adhérences.
3. $u_{n+1} - u_n \xrightarrow{n \rightarrow +\infty} 0$

Montrer que (u_n) est convergente.

Exercice IV.4.

Supposons que X est compact. Soit (u_n) une suite à valeurs dans X . Montrer que

$$d(u_p, \text{Adh}(u_n)) \xrightarrow{p \rightarrow +\infty} 0$$

Exercice IV.5.

Supposons que X est compact. Soit $f \in \mathcal{C}(X, X)$ et (u_n) une suite définie par

$$\begin{cases} u_0 \in X \\ \forall n \in \mathbb{N}, \quad u_{n+1} = f(u_n) \end{cases}$$

On pose $A = Adh(u_n)$. Montrer que $f(A) = A$.

Exercice IV.6.

Soit Y un espace métrique muni d'une distance δ . On pose pour tout $f \in Y^X$,

$$\Gamma_f = \{(x, f(x)), x \in X\} \subset X \times Y$$

1. Montrer que pour tout $f \in \mathcal{C}(X, Y)$, Γ_f est fermé dans $X \times Y$.
2. Donner un exemple de X, Y et f vérifiant f discontinue et Γ_f fermé.
3. On suppose que Y est compact. Montrer que si Γ_f est fermé, alors f est continue.

V Uniforme continuité

Théorème (Théorème de Heine) V.1.

Soit Y un espace métrique muni d'une distance δ et $f \in \mathcal{C}(X, Y)$. Si X est compact, alors f est uniformément continue.

Preuve : commençons par écrire la définition de l'uniforme continuité de f

$$\forall \varepsilon > 0, \exists \eta > 0 \quad \forall x, y \in X, \quad d(x, y) < \eta \implies \delta(f(x), f(y)) < \varepsilon$$

Supposons que la négation de cette proposition est vraie, i.e.

$$\exists \varepsilon > 0, \forall \eta > 0 \quad \exists x, y \in X, \quad d(x, y) < \eta \text{ et } \delta(f(x), f(y)) \geq \varepsilon$$

Il existe donc un certain $\varepsilon > 0$ pour lequel il existe deux suites (x_n) et (y_n) à valeurs dans X vérifiant

$$\forall n \in \mathbb{N}, \quad d(x_n, y_n) < \frac{1}{n+1} \text{ et } \delta(f(x_n), f(y_n)) \geq \varepsilon$$

X étant compact, il existe une extractrice φ telle que $(x_{\varphi(n)})$ est convergente. De même, il existe une extractrice ψ telle que $(y_{\varphi \circ \psi(n)})$ soit convergente. Or, on a pour tout $n \in \mathbb{N}$

$$d(x_{\varphi \circ \psi(n)}, y_{\varphi \circ \psi(n)}) < \frac{1}{\varphi \circ \psi(n) + 1} \xrightarrow[n \rightarrow +\infty]{} 0$$

$(x_{\varphi \circ \psi(n)})$ et $(y_{\varphi \circ \psi(n)})$ ont donc la même limite. On a alors par continuité de f

$$\varepsilon \leq \delta(f(x_{\varphi \circ \psi(n)}), f(y_{\varphi \circ \psi(n)})) \xrightarrow[n \rightarrow +\infty]{} 0$$

ce qui est absurde. On en déduit donc que f est uniformément continue.

Exercice V.2.

Soit $f \in \mathcal{C}([0, 1]^2, \mathbb{R})$, montrer que $\varphi : \begin{cases} [0, 1] & \longrightarrow \mathbb{R} \\ x & \longmapsto \sup_{y \in [0, 1]} f(x, y) \end{cases}$ est continue.

VI Optimisation sur un compact

Proposition VI.1.

Soit Y un espace métrique muni d'une distance δ et $f \in \mathcal{C}(X, Y)$.

1. Si X est compact, alors $f(X)$ est compact.
2. Si $X \neq \emptyset$ et $Y = \mathbb{R}$, alors f est bornée et atteint ses bornes.

Preuve

1. Soit $(y_n)_{n \in \mathbb{N}}$ une suite à valeurs dans $f(X)$. Il existe une suite $(x_n) \in X^{\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$, $f(x_n) = y_n$. Comme X est compact, il existe une extractrice φ telle que $(x_{\varphi(n)})$ converge vers un élément x de X . Par continuité de f , on a

$$y_{\varphi(n)} = f(x_{\varphi(n)}) \xrightarrow[n \rightarrow +\infty]{} f(x) \in f(X)$$

on en déduit donc que $f(X)$ est compact.

2. D'après le point précédent, $f(X)$ est compact donc c'est un fermé borné, cet ensemble contient alors sa borne supérieure et sa borne inférieure car c'est les limites de suites à valeurs dans $f(X)$. On en déduit qu'il existe $a, b \in X$ tel que $f(a) = \sup f(X)$ et $f(b) = \inf f(X)$. f est donc bornée et atteint ses bornes.

Corollaire VI.2.

Si X est compact, F fermé dans X et $f \in \mathcal{C}(X, Y)$, alors $f(F)$ est fermé dans Y .

Preuve : F est un fermé dans un compact, c'est donc un compact et alors $f(F)$ est compact et finalement c'est un fermé dans Y .

Exercice VI.3.

On suppose que X est compact. Soit $f \in \mathcal{C}(X, Y)$ bijective. Montrer que f^{-1} est continue.

Exercice VI.4.

Soit $f, g \in \mathcal{C}([0, 1], [0, 1])$ tels que $f \circ g = g \circ f$. Montrer qu'il existe $a \in [0, 1]$ tel que $f(a) = g(a)$.

Exercice VI.5.

Soit E un espace vectoriel normé muni d'une norme $\|\cdot\|$. Soit A et B deux parties de E . On pose

$$A + B = \{a + b, (a, b) \in A \times B\}$$

dire lesquelles des propositions suivantes sont vraies.

1. Si A ou B est ouvert, alors $A + B$ est ouvert.
2. Si A et B sont compacts, alors $A + B$ est compact.
3. Si A est compact et B est fermé, alors $A + B$ est fermé.
4. Si A et B sont fermés alors $A + B$ est fermé.

Exercice VI.6.

On suppose que X est compact non vide. Soit $f \in X^X$. telle que

$$\forall (x, y) \in X^2, x \neq y \implies d(f(x), f(y)) < d(x, y)$$

1. Montrer que f admet un unique point fixe l .
2. Considérons la suite $(u_n) \in X^{\mathbb{N}}$ définie par $\begin{cases} u_0 \in X \\ \forall n \in \mathbb{N}, u_{n+1} = f(u_n) \end{cases}$.
Montrer que $u_n \xrightarrow[n \rightarrow +\infty]{} l$.

VII Compléments

1. Recouvrement fini d'un compact

Proposition VII.1.

On suppose que X est compact. Pour tout $\varepsilon > 0$, il existe $p \in \mathbb{N}^*$ et a_1, \dots, a_p tels que

$$X = \bigcup_{k=1}^p B(a_k, \varepsilon)$$

Preuve : Supposons que

$$\exists \varepsilon > 0, \forall p \in \mathbb{N}^*, \forall (a_1, \dots, a_p) \in X^p, \bigcup_{k=1}^p B(a_k, \varepsilon) \subsetneq X$$

Soit $\varepsilon > 0$ vérifiant la propriété ci-dessus. Construisons la suite $(a_n)_{n \in \mathbb{N}} \in X^{\mathbb{N}}$ de la manière suivante :

On prend tout d'abord $a_0 \in X$ au hasard. Soit $n \in \mathbb{N}$ tel que a_n est bien défini. $A_n = X \setminus \bigcup_{k=0}^n B(a_k, \varepsilon)$ est non vide, on peut donc prendre a_{n+1} dans A_n . Par construction, on a pour tout $n \neq m$, $d(a_n, a_m) \geq \varepsilon$ et donc pour toute extractrice φ , pour tout $n \in \mathbb{N}$, $d(a_{\varphi(n)}, a_{\varphi(n+1)}) \geq \varepsilon$. $(a_{\varphi(n)})$ ne peut donc pas converger et alors X n'est pas compact ce qui est absurde.

Exercice VII.2.

On suppose que X est compact.

- Soit $\varepsilon > 0$. Montrer qu'il existe $N \in \mathbb{N}^*$ tel que

$$\exists (x_1, \dots, x_N) \in X^N, \forall i \neq j, d(x_i, x_j) \geq \varepsilon \quad (*)$$

et tel que toute famille de points y_1, \dots, y_n vérifiant la propriété $(*)$ est de cardinal inférieur à N (i.e. $n \leq N$).

- Soit $f : X \rightarrow X$ une isométrie. Montrer que f est surjective.

2. Fermés emboités**Proposition VII.3.**

On suppose que X est compact. Pour toute suite de fermés non vides décroissante pour l'inclusion $(F_n)_{n \in \mathbb{N}} \in \mathcal{P}(X)^{\mathbb{N}}$, $\bigcap_{n \in \mathbb{N}} F_n \neq \emptyset$.

Preuve : Soit (x_n) une suite à valeurs dans X telle que pour tout $n \in \mathbb{N}$, $x_n \in F_n$ (cette suite existe car tous les F_n sont non vides). La suite (F_n) étant décroissante, on a pour tout $n \in \mathbb{N}$ et tout $i \leq n$, $x_n \in F_i$. X étant compact, il existe une extractrice φ telle que $(x_{\varphi(n)})$ converge vers un élément x de X . On a alors pour tout $p \in \mathbb{N}$, la suite $(x_{\varphi(n)})$ est à valeurs dans F_p à partir d'un certain rang donc x est limite d'une suite à valeurs dans F_p , i.e. $x \in \overline{F_p} = F_p$. On a donc pour tout $p \in \mathbb{N}$, $x \in F_p$ et alors $x \in \bigcap_{n \in \mathbb{N}} F_n$ et

finalement $\bigcap_{n \in \mathbb{N}} F_n \neq \emptyset$.

Corollaire VII.4.

On suppose que X est compact. Soit (f_n) une suite de fonctions à valeurs dans $C(X, \mathbb{R})$ et $f \in C(X, \mathbb{R})$. Si pour tout $x \in X$, la suite $(f_n(x))_{n \in \mathbb{N}}$ est croissante et converge vers $f(x)$, alors (f_n) converge uniformément vers f .

Preuve : Soit $\varepsilon > 0$. Posons pour tout $n \in \mathbb{N}$, $F_n = \{x \in X, |f_n(x) - f(x)| \geq \varepsilon\}$. Remarquons tout d'abord que pour tout $n \in \mathbb{N}$, F_n est l'image réciproque d'un fermé par une fonction continue, c'est donc un fermé dans X . De plus, pour tout $n \in \mathbb{N}$, si $x \in F_{n+1}$, alors $|f_{n+1}(x) - f(x)| \geq \varepsilon$, i.e. $f(x) - \varepsilon \geq f_{n+1}(x)$ mais $f_{n+1}(x) \geq f_n(x)$, donc $f(x) - \varepsilon \geq f_n(x)$ et finalement $x \in F_n$. La suite (F_n) est donc décroissante.

→ S'il existe $n_\varepsilon \in \mathbb{N}$ tel que $F_{n_\varepsilon} = \emptyset$, alors pour tout $n \geq n_\varepsilon$, $F_n = \emptyset$ et alors

$$\forall n \geq n_\varepsilon, \forall x \in X, |f_n(x) - f(x)| < \varepsilon.$$

→ Sinon, toutes les hypothèses de la propriété précédente sont vérifiées, on peut donc affirmer que $\bigcap_{n \in \mathbb{N}} F_n \neq \emptyset$. Soit $x \in \bigcap_{n \in \mathbb{N}} F_n$. On a pour tout $n \in \mathbb{N}$, $|f_n(x) - f(x)| \geq \varepsilon$, donc $(f_n(x))$ ne converge pas vers $f(x)$ ce qui est absurde.

On peut donc affirmer l'existence de $n_\varepsilon \in \mathbb{N}$ tel que pour tout $n \geq n_\varepsilon$ et pour tout $x \in X$, $|f_n(x) - f(x)| < \varepsilon$, i.e. (f_n) converge uniformément vers f .

Exercice VII.5.

Montrer que $[0, 1]^{\mathbb{N}}$ muni de la distance $d : ((x_n), (y_n)) \mapsto \sum_{k=0}^{+\infty} \frac{|x_k - y_k|}{2^k}$ est compact.

Exercice VII.6.

Soit $\sum z_n$ une série complexe absolument convergente. On note

$$K = \left\{ z \in \mathbb{C}, \exists A \in \mathcal{P}(\mathbb{N}), z = \sum_{n \in A} z_n \right\}$$

En utilisant l'exercice précédent, montrer que K est compact.

Correction de l'exercice IV.3. :

Nous allons montrer que (u_n) est à valeurs dans un compact et admet au plus une valeur d'adhérence. Une fois cela fait, on peut directement appliquer la propriété précédente pour affirmer que (u_n) converge. Posons $A = \{a_1, \dots, a_p\}$ l'ensemble des valeurs d'adhérence de (u_n) avec $p \in \mathbb{N}^*$ (on peut dire que $p \geq 1$ car (u_n) est à valeurs dans un compact non vide)

Supposons que $|A| > 1$. Posons $\varepsilon = \frac{1}{3} \min_{i,j \in [1;p], i < j} \|a_i - a_j\| > 0$. Pour tout $i \in [1;p]$, l'ensemble

$$C = \left\{ n \in \mathbb{N}, u_n \in X \setminus \bigcup_{i=1}^p B(a_i, \varepsilon) \right\}$$

est fini et donc borné.

Soit $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $n \notin C$ et $\|u_{n+1} - u_n\| < \varepsilon$. Soit $n_1 \geq N$ tel que $u_{n_1} \in B(a_1, \varepsilon)$, $n_2 \geq n_1$ tel que $u_{n_2} \notin B(a_1, \varepsilon)$ et $k = \max \{l \in [n_1; n_2], u_l \in B(a_1, \varepsilon)\}$.

On a par construction $u_k \in B(a_1, \varepsilon)$ et $\exists i \neq 1$ $u_{k+1} \in B(a_i, \varepsilon)$. On a donc

$$\begin{aligned} \|u_k - u_{k+1}\| &= \|u_k - a_1 + a_1 - a_i + a_i - u_{k+1}\| \\ &\geq \|a_1 - a_i\| - \|u_k - a_1\| - \|u_{k+1} - a_i\| \\ &\geq 3\varepsilon - \varepsilon - \varepsilon = \varepsilon \end{aligned}$$

ce qui est absurde car $k \geq N$, donc $|A| \leq 1$.

Considérons M un majorant de $(\|u_n\|)$. (u_n) est à valeurs dans $B_f(0, M+1)$ qui est un fermé borné dans un \mathbb{R} -espace vectoriel de dimension finie. C'est donc un compact, ce qui nous permet de conclure.

Correction de l'exercice IV.4. :

Posons pour tout $p \in \mathbb{N}$, $\varepsilon_p = d(u_p, Adh(u_n))$. Supposons que (ε_p) ne tend pas vers 0. Soit $\delta > 0$ tel que l'ensemble $A = \{p \in \mathbb{N}, \varepsilon_p > \delta\}$ est infini et (u_n) est à valeurs dans un compact, on peut donc considérer une extractrice φ à valeurs dans A telle que $(u_{\varphi(p)})$ converge vers un certain $b \in Adh(u_n)$. Pour tout $p \in \mathbb{N}$, $d(u_{\varphi(p)}, Adh(u_n)) > \delta$ et alors $\delta < d(u_{\varphi(p)}, b) \xrightarrow[p \rightarrow +\infty]{} 0$ ce qui est absurde.

Correction de l'exercice IV.5. :

Montrons successivement les inclusions dans les deux sens.

$$\rightarrow f(A) \subset A$$

Soit $a \in A$. Il existe une extractrice φ telle que $u_{\varphi(n)} \xrightarrow[n \rightarrow +\infty]{} a$. On a alors

$u_{\varphi(n)+1} = f(u_{\varphi(n)}) \xrightarrow[n \rightarrow +\infty]{} f(a)$. $f(a)$ est donc une valeur d'adhérence de (u_n) , i.e. $f(a) \in A$. On conclut donc que $f(A) \subset A$.

$$\rightarrow A \subset f(A)$$

On reprend les notations du point précédent.

On considère l'extractrice $\varphi' : n \mapsto \varphi(n) - 1$. Soit ψ une extractrice telle que $(u_{\varphi' \circ \psi(n)})_{n \geq 1}$ converge vers un certain $b \in A$. On a alors $f(u_{\varphi' \circ \psi(n)}) = f(u_{\varphi \circ \psi(n)-1}) = u_{\varphi \circ \psi(n)}$. De plus, on a $f(u_{\varphi' \circ \psi(n)}) \xrightarrow[n \rightarrow +\infty]{} f(b)$ et $u_{\varphi \circ \psi(n)} \xrightarrow[n \rightarrow +\infty]{} a$. On a donc finalement $a = f(b) \in f(A)$ et alors $A \subset f(A)$.

Correction de l'exercice IV.6. :

- Soit $(w_n) = ((x_n, f(x_n)))_{n \in \mathbb{N}}$ une suite convergente à valeurs dans Γ_f . On pose (x, y) la limite de cette suite. On a $x_n \xrightarrow[n \rightarrow +\infty]{} x$, donc $f(x_n) \xrightarrow[n \rightarrow +\infty]{} f(x)$. Mais on a aussi $f(x_n) \xrightarrow[n \rightarrow +\infty]{} y$, donc $(x, y) = (x, f(x)) \in \Gamma_f$. La limite de (w_n) est dans Γ_f ce qui nous permet d'affirmer que Γ_f est fermé.

2. Considérons la fonction f définie par

$$f : \begin{cases} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto \begin{cases} \frac{1}{x} & \text{si } x \neq 0 \\ 0 & \text{sinon} \end{cases} \end{cases}$$

Posons $g : (x, y) \longmapsto xy - 1$. On a alors

$$\Gamma_f = g^{-1}(\{0\}) \cup \{(0, 0)\}$$

$g^{-1}(\{0\})$ est l'image réciproque d'un fermé par une fonction continue, c'est donc un fermé. $\{(0, 0)\}$ étant aussi un fermé, on en déduit que Γ_f est fermé dans $X \times Y$.

3. Soit $x \in X$. Soit $(x_n)_{n \in \mathbb{N}}$ une suite à valeurs dans X qui converge vers x . Considérons la suite $(w_n)_{n \in \mathbb{N}}$ à valeurs dans Γ_f définie par $(w_n) = (x_n, f(x_n))_{n \in \mathbb{N}}$. Par hypothèse, Y est compact, il existe donc une extractrice φ tel que $(f(x_{\varphi(n)}))$ converge dans Y et donc $(w_{\varphi(n)})_{n \in \mathbb{N}}$ converge dans Γ_f car c'est un fermé, i.e. il existe $y \in X$ tel que $w_{\varphi(n)} \xrightarrow{n \rightarrow +\infty} (y, f(y))$. On a alors $x_n \xrightarrow{n \rightarrow +\infty} y$ et $f(x_{\varphi(n)}) \xrightarrow{n \rightarrow +\infty} f(y)$. Or $x_{\varphi(n)} \xrightarrow{n \rightarrow +\infty} x$, donc $y = x$ et $f(x_{\varphi(n)}) \xrightarrow{n \rightarrow +\infty} f(x)$. On a donc montré que $(f(x_n))$ admet une unique valeur d'adhérence $f(x)$ et est à valeurs dans le compact Y , et par conséquence converge vers $f(x)$. D'où la continuité de f .

Correction de l'exercice V.2. :

Soit $x \in [0, 1]$ et $\varepsilon > 0$. f est continue sur le compact $[0, 1]^2$, donc d'après le théorème de Heine, f est uniformément continue. On dispose donc de $\eta > 0$ tel que

$$\forall (x, y), (x', y') \in [0, 1]^2, \quad \|(x, y) - (x', y')\| < \eta \implies |f(x, y) - f(x', y')| < \varepsilon$$

Soit x' tel que $|x - x'| < \eta$, on a alors pour tout $y \in [0, 1]$, $\|(x, y) - (x', y)\| = |x - x'| < \eta$ et donc

$$|f(x, y) - f(x', y)| < \varepsilon$$

i.e.

$$f(x', y) - \varepsilon < f(x, y) < f(x', y) + \varepsilon$$

En passant à la borne supérieure de chaque côté de l'inégalité, on obtient

$$\varphi(x') - \varepsilon \leq \varphi(x) \leq \varphi(x') + \varepsilon$$

i.e.

$$|\varphi(x) - \varphi(x')| \leq \varepsilon$$

d'où la continuité de φ .

Correction de l'exercice VI.3. :

→ **Méthode 1** : Soit F un fermé de X . X étant compact, on peut affirmer que F est compact. f est continue, donc $f(F)$ est compact donc fermé. Or on a $(f^{-1})^{-1}(F) = f(F)$, donc $(f^{-1})^{-1}(F)$ est fermé. La caractérisation des fonctions continues par image réciproque des fermés nous permet de conclure.

→ **Méthode 2** : On va utiliser l'exercice IV.6. f est continue, donc Γ_f est fermé dans $X \times Y$. On considère l'application

$$i : \begin{cases} X \times Y & \longrightarrow Y \times X \\ (x, y) & \longmapsto (y, x) \end{cases}$$

On a $\Gamma_{f^{-1}} = i(\Gamma_f)$ et i envoie les fermés su des fermés (preuve laissée en exercice), donc $\Gamma_{f^{-1}}$ est fermé dans $Y \times X$. X étant compact, l'exercice IV.6. nous donne que f^{-1} est continue.

→ **Méthode 3 :** Considérons (y_n) une suite à valeurs dans Y qui converge vers b . On pose $a = f^{-1}(b)$ et $(x_n) = (f^{-1}(y_n))_{n \in \mathbb{N}}$. Pour montrer que f^{-1} est continue, il faut montrer que $x_n \xrightarrow[n \rightarrow +\infty]{} a$.

(x_n) est à valeurs dans le compact X , on peut donc considérer a' une valeur d'adhérence de (x_n) . Il existe une extractrice φ telle que $x_{\varphi(n)} \xrightarrow[n \rightarrow +\infty]{} a'$. On a par continuité de f , $f(x_{\varphi(n)}) \xrightarrow[n \rightarrow +\infty]{} f(a')$.

Mais on a aussi $f(x_{\varphi(n)}) = y_n \xrightarrow[n \rightarrow +\infty]{} b$, donc $f(a') = b$, i.e. $a' = f^{-1}(b) = a$. On a alors montré que (x_n) admet une unique valeur d'adhérence qui est a . (x_n) étant à valeurs dans un compact, on peut déduire que $x_n \xrightarrow[n \rightarrow +\infty]{} a$, d'où le résultat voulu.

Correction de l'exercice VI.4. :

Posons $A = \{x \in [0, 1], g(x) = x\}$.

→ A est non vide.

En effet, en considérant $h = g - Id$, on a $h(0) = g(0) \geq 0$ et $h(1) = g(1) - 1 \leq 0$. h étant continue, le théorème des valeurs intermédiaires nous permet d'affirmer qu'il existe $a \in [0, 1]$ tel que $h(a) = 0$, i.e. $g(a) = a$. A est donc non vide

→ A est fermé, car il est égal à $h^{-1}(\{0\})$, qui est l'image réciproque d'un fermé par une fonction continue. A est une ferme inclus dans le compact $[0, 1]$, il est donc compact et admet alors un minimum $\alpha = \min A$ et un maximum $\beta = \max A$ tel que $g(\alpha) = \alpha$ et $g(\beta) = \beta$. Or, $f(g(\alpha)) = f(\alpha) = g(f(\alpha))$. $f(\alpha)$ est donc un point fixe de g , i.e. $f(\alpha) \in A$. De même, on a $f(\beta) \in A$.

Posons $w = f - g$. On a $w(\alpha) = f(\alpha) - g(\alpha) = f(\alpha) - \alpha \geq 0$ et $w(\beta) = f(\beta) - g(\beta) = f(\beta) - \beta \leq 0$. w étant continue, le théorème des valeurs intermédiaires nous permet donc d'affirmer qu'il existe $a \in [\alpha, \beta]$ tel que $w(a) = 0$, i.e. $f(a) = g(a)$.

Correction de l'exercice VI.5. :

1. Cette proposition est vraie.

Soit $a \in A$, $b \in B$, et $\varepsilon > 0$ tel que $B(a, \varepsilon) \subset A$ ou $B(b, \varepsilon) \subset B$. Soit $x \in B(a+b, \varepsilon)$. On peut écrire x comme $x = a + b + u$ tel que $\|u\| \leq \varepsilon$. On a alors $a + u \in B(a, \varepsilon) \subset A$ ou $b + u \in B(b, \varepsilon)$, donc $x \in A + B$ et finalement $B(a+b, \varepsilon) \subset A + B$. On en déduit donc que $A + B$ est ouvert.

2. Cette proposition est vraie.

Soit $(w_n)_{n \in \mathbb{N}}$ une suite à valeurs dans $A + B$. On peut écrire $(w_n) = (a_n + b_n)_{n \in \mathbb{N}}$ avec (a_n) et (b_n) deux suites à valeurs respectivement dans A et B . A est compact, il existe donc une extractrice φ et $a \in A$ tel que $a_{\varphi(n)} \xrightarrow[n \rightarrow +\infty]{} a$. De même B étant compact et $(b_{\varphi(n)})$ étant à valeurs dans B , il existe une extractrice ψ et $b \in B$ tel que $b_{\psi(n)} \xrightarrow[n \rightarrow +\infty]{} b$. On a alors $a_{\psi(n)} + b_{\psi(n)} \xrightarrow[n \rightarrow +\infty]{} a + b$, d'où la compacité de $A + B$.

3. Cette proposition est vraie.

Soit $(c_n)_{n \in \mathbb{N}} = (a_n + b_n)$ une suite à valeurs dans $A + B$ qui converge vers c . A étant compact, on peut considérer une extractrice φ telle que $a_{\varphi(n)} \xrightarrow[n \rightarrow +\infty]{} a \in A$. On a alors $b_{\varphi(n)} = c_{\varphi(n)} - a_{\varphi(n)} \xrightarrow[n \rightarrow +\infty]{} c - a$. B est fermé et $b_{\varphi(n)}$ est à valeurs dans B , ce qui nous permet de dire que $c - a \in B$. On en déduit que $c = \underbrace{a}_{\in A} + \underbrace{c - a}_{\in B} \in A + B$, donc $A + B$ est fermé.

4. Cette proposition est fausse.

En effet, il suffit de considérer le cas $A = \mathbb{Z}$ et $B = \sqrt{2}\mathbb{Z}$. $A + B = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ est un sous groupe de \mathbb{R} , donc d'après l'exercice VI.4. du chapitre 11.2, il est soit égal à $a\mathbb{Z}$ avec $a \in \mathbb{R}$ ou alors il est dense dans \mathbb{R} . Le premier cas n'est pas possible (il est facile de montrer que cela implique que $\sqrt{2}$ est rationnel), donc $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ est dense dans \mathbb{R} . Pour résumer, on a

→ $A = \mathbb{Z}$ fermé dans \mathbb{R} .

→ $B = \sqrt{2}\mathbb{Z}$ fermé dans \mathbb{R} .

→ $\overline{A+B} = \overline{Z + \sqrt{2}\mathbb{Z}} = \mathbb{R} \neq A+B$, donc $A+B$ n'est pas fermé dans \mathbb{R} .

Correction de l'exercice VI.6. :

- Existence et unicité du point fixe.

→ Existence

On considère la fonction $\varphi : x \mapsto d(x, f(x))$.

- Montrons que φ est continue.

Soit $x, y \in X$. On a

$$\begin{aligned} |\varphi(x) - \varphi(y)| &\leq |d(x, f(x)) - d(y, f(x))| + |d(y, f(x)) - d(y, f(y))| \\ &\leq d(x, y) + d(f(x), f(y)) \\ &\leq 2d(x, y) \end{aligned}$$

φ est lipschitzienne et donc continue.

- Montrons que φ atteint 0.

X est compact donc φ y atteint son minimum, i.e. il existe $a \in X$ tel que $\varphi(a) = \inf_{x \in X} \varphi(x)$.

Supposons que $a \neq f(a)$, i.e. $\varphi(a) \neq 0$.

On a alors

$$\varphi(f(a)) = d(f(a), f(f(a))) < d(a, f(a)) = \varphi(a)$$

ce qui est absurde par construction. On en déduit donc que $\varphi(a) = 0$, i.e. $f(a) = a$ et donc que f admet un point fixe.

→ Unicité

Soit a et a' deux points fixes de f qu'on suppose distincts. On a $d(a, a') = d(f(a), f(a')) < d(a, a')$ ce qui est absurde, d'où l'unicité du point fixe.

- Considérons la suite $(\varepsilon_n) = (d(u_n, a))_{n \in \mathbb{N}}$. On a pour tout $n \in \mathbb{N}$,

$$\varepsilon_{n+1} = d(u_{n+1}, a) = d(f(u_n), f(a)) \leq d(u_n, a) = \varepsilon_n$$

(ε_n) est donc décroissante minorée par 0, elle est alors convergente. Notons α sa limite.

→ Si $\alpha = 0$, alors $u_n \xrightarrow[n \rightarrow +\infty]{} a$ ce qui est bien le résultat voulu.

→ Supposons que $\alpha > 0$.

X étant compact, on peut considérer a une valeur d'adhérence de u_n . Soit φ une extractrice telle que $u_{\varphi(n)} \xrightarrow[n \rightarrow +\infty]{} a$. Par continuité de $u \mapsto d(a, u)$, $d(u_{\varphi(n)}, a) \xrightarrow[n \rightarrow +\infty]{} d(a, a)$, donc $d(a, a) = \alpha$.

Or, $u_{\varphi(n)+1} = f(u_{\varphi(n)}) \xrightarrow[n \rightarrow +\infty]{} f(a)$, donc $f(a)$ est aussi une valeur d'adhérence de (u_n) . Par un raisonnement similaire à ce qui précéde, $f(a)$ étant une valeur d'adhérence de (u_n) , on peut affirmer que $d(f(a), a) = \alpha$. On a alors

$$\alpha = d(f(a), a) = d(f(a), f(l)) < d(a, f(l)) = \alpha$$

ce qui est absurde, donc $\alpha = 0$, d'où le résultat voulu. La dernière inégalité provient du fait que $a \neq f(a)$ car $f(a) = f(l)$ entraînerait $\alpha = 0$ ce qui est faux par hypothèse.

Correction de l'exercice VII.2. :

- Posons $A = \{n \in \mathbb{N}, \exists (y_1, \dots, y_n) \in X^n \text{ vérifiant } (*)\}$. Il est facile de voir que $1 \in A$. En utilisant la caractérisation d'un compact par recouvrement fini d'ouverts, on dispose de $p \in \mathbb{N}^*$ tel que

$$X = \bigcup_{k=1}^p B\left(a_k, \frac{\varepsilon}{3}\right)$$

Soit $n > p$ et $y_1, \dots, y_n \in X^n$. Par principe des tiroirs, il existe $(k, i, j) \in \mathbb{N}^{\ast 3}$, tel que $i \neq j$, $y_i \in B\left(a_k, \frac{\varepsilon}{3}\right)$ et $y_j \in B\left(a_k, \frac{\varepsilon}{3}\right)$. On a alors

$$d(y_i, y_j) \leq d(y_i, a_k) + d(a_k, y_j) \leq \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \frac{2\varepsilon}{3} < \varepsilon$$

A est donc une partie de \mathbb{N} majorée par p , elle admet donc un maximum qu'on note N . N vérifie bien la propriété voulue.

2. **Rappel :** $f : X \rightarrow X$ est une isométrie si $\forall (x, y) \in X^2$, $d(f(x), f(y)) = d(x, y)$.

On pose $N = \max A$ et on considère x_1, \dots, x_N vérifiant (*). Posons pour tout $i \in \llbracket 1; N \rrbracket$, $f(x_i) = y_i$. f étant une isométrie, on a pour tout $i \neq j$, $d(y_i, y_j) \geq d(x_i, x_j) \geq \varepsilon$, i.e. y_1, \dots, y_N vérifie (*).

→ Montrons que $X = \bigcup_{k=1}^N B(y_k, \varepsilon)$.

Supposons que $X \setminus \bigcup_{k=1}^N B(y_k, \varepsilon) \neq \emptyset$. On dispose alors de $z \in X \setminus \bigcup_{k=1}^N B(y_k, \varepsilon)$. Par construction, (y_1, \dots, y_N, z) est une famille de cardinal $N+1$ qui vérifie (*) ce qui est absurde. On en déduit donc qu'on a bien $X = \bigcup_{k=1}^N B(y_k, \varepsilon)$.

→ Montrons finalement que f est surjective.

On a $\{y_1, \dots, y_N\} \subset f(X)$ et $X = \bigcup_{k=1}^N B(y_k, \varepsilon)$, donc pour tout $z \in X$,

$$d(z, f(X)) \leq d(z, \{y_1, \dots, y_N\}) \leq \varepsilon$$

Cette inégalité est valable pour tout ε , ce qui nous donne que pour tout $z \in X$, $d(z, f(X)) = 0$, i.e. $z \in \overline{f(X)}$. X est compact et f est continue car c'est une isométrie, on a donc que $f(X)$ est compact, donc $\overline{f(X)} = f(X)$.

En résumé, on a que $X \subset \overline{f(X)} = f(X)$ ce qui nous donne que $f(X) = X$, i.e. f est surjective.

Correction de l'exercice VII.5. :

Soit $((x_{k,n})_{n \in \mathbb{N}})_{k \in \mathbb{N}}$ une suite à valeurs dans $[0, 1]^{\mathbb{N}}$.

On va définir par récurrence une suite d'extractrices $(\varphi_n)_{n \in \mathbb{N}}$ et une suite $(x_n)_{n \in \mathbb{N}}$ de la manière suivante :

- φ_0 est une extractrice telle que $x_{\varphi_0(k), 0} \xrightarrow[k \rightarrow +\infty]{} x_0 \in [0, 1]$. Cette extractrice existe car la suite $(x_{k,0})_{k \in \mathbb{N}}$ est à valeurs dans le compact $[0, 1]$.
- Soit $n \in \mathbb{N}$, on suppose que φ_n est bien définie, on définit alors φ_{n+1} comme une extractrice telle que la suite $x_{\varphi_0 \circ \dots \circ \varphi_n \circ \varphi_{n+1}(k), n+1} \xrightarrow[n \rightarrow +\infty]{} x_{n+1} \in [0, 1]$. Encore une fois, cette extractrice existe car la suite $(x_{\varphi_0 \circ \dots \circ \varphi_n(k), n+1})_{k \in \mathbb{N}}$ est à valeurs dans le compact $[0, 1]$.

Considérons à présent l'application

$$\varphi : \begin{cases} \mathbb{N} & \longrightarrow \mathbb{N} \\ n & \longmapsto \varphi_0 \circ \dots \circ \varphi_n(n) \end{cases}$$

Montrons qu'il s'agit bien d'une extractrice. Pour cela, il faut montrer que φ est strictement croissante. Soit $l, k \in \mathbb{N}$ tel que $l < k$. On a

$$\varphi(k) = \varphi_0 \circ \dots \circ \varphi_l \circ \underbrace{\varphi_{l+1} \circ \dots \circ \varphi_k}_{\psi}(k)$$

ψ est une extractrice car c'est une composition d'extractrices, on a alors $\psi(k) \geq k > l$. De plus $\varphi_0 \circ \dots \circ \varphi_l$

est strictement croissante car c'est une composition de fonctions strictement croissantes, on a alors :

$$\varphi(k) = \varphi_0 \circ \cdots \circ \varphi_l \circ \psi(k) \geq \varphi_0 \circ \cdots \circ \varphi_l(k) > \varphi_0 \circ \cdots \circ \varphi_l(l) = \varphi(l)$$

donc φ est bien une extractrice.

Montrons à présent que pour la distance d , on a $(x_{\varphi(k),n})_{n \in \mathbb{N}} \xrightarrow[k \rightarrow +\infty]{} (x_n)_{n \in \mathbb{N}}$.

Soit $\varepsilon > 0$. On a pour tout $n \in \mathbb{N}$, $x_{\varphi(k),n} \xrightarrow[k \rightarrow +\infty]{} x_n$, i.e.

$$\forall n \in \mathbb{N}, \exists K_n \in \mathbb{N}, \forall k \geq K_n, |x_{\varphi(k),n} - x_n| \leq \varepsilon$$

Soit $N \in \mathbb{N}$ tel que $\frac{1}{2^N} \leq \varepsilon$ et soit $K = \max\{K_1, \dots, K_N\}$. On a pour tout $k \geq K$

$$\begin{aligned} d((x_{\varphi(k),n})_{n \in \mathbb{N}}, (x_n)_{n \in \mathbb{N}}) &= \sum_{n=0}^{\infty} \frac{|x_{\varphi(k),n} - x_n|}{2^n} \\ &= \sum_{n=0}^{N-1} \frac{|x_{\varphi(k),n} - x_n|}{2^n} + \sum_{n=N}^{\infty} \frac{|x_{\varphi(k),n} - x_n|}{2^n} \\ &\leq \sum_{n=0}^{N-1} \frac{\varepsilon}{2^n} + \sum_{n=N}^{\infty} \frac{2}{2^n} \\ &\leq 2\varepsilon + \frac{4}{2^N} \leq 6\varepsilon \end{aligned}$$

On a donc trouvé une suite extraite de $((x_{k,n})_{n \in \mathbb{N}})_{k \in \mathbb{N}}$ qui converge vers une suite $(x_n)_{n \in \mathbb{N}}$ dans $[0, 1]^{\mathbb{N}}$ pour la distance d , ce qui montre bien que $[0, 1]^{\mathbb{N}}$ est compact pour cette distance.

Correction de l'exercice VII.6. :

On pose $X_c = \{0, 1\}^{\mathbb{N}}$. Une preuve quasi-identique à celle de l'exercice précédent permet d'affirmer que X_c muni de la distance d vue dans cet exercice est compact.

Pour toute partie A de \mathbb{N} , on considère la fonction

$$1_A : x \mapsto \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{sinon} \end{cases}$$

On considère également l'application

$$f : \begin{cases} X_c & \longrightarrow K \\ (\varepsilon_n) & \longmapsto \sum_{n=0}^{\infty} \varepsilon_n z_n \end{cases}$$

Cette application est définie correctement et est surjective (pour la surjectivité, il suffit d'utiliser les suites de la forme $(\varepsilon_n) = (1_A(n))_{n \in \mathbb{N}}$).

Si on montre que f est continue, alors $f(X_c) = K$ est compact car il s'agit de l'image d'un compact par une application continue. Montrons donc que f est continue.

Soit $\varepsilon > 0$ et $(\varepsilon_n)_{n \in \mathbb{N}} \in X_c$. Pour tout $\eta > 0$ et $(\gamma_n) \in X_c$, on a

$$d((\varepsilon_n), (\gamma_n)) < \eta \implies \forall n \in \mathbb{N}, |\varepsilon_n - \gamma_n| < 2^n \eta$$

donc pour tout $N \in \mathbb{N}$, lorsque $\eta < \frac{1}{2^N}$, on a pour tout $n \in \llbracket 0; N \rrbracket$, $|\varepsilon_n - \gamma_n| < 2^n \eta < 1$, i.e. $\varepsilon_n = \gamma_n$.

On a alors pour tout $(\gamma_n)_{n \in \mathbb{N}}$ et $N \in \mathbb{N}$,

$$d((\varepsilon_n), (\gamma_n)) < \frac{1}{2^N} \implies |f((\varepsilon_n)) - f((\gamma_n))| \leq \left| \sum_{k=N+1}^{\infty} (\varepsilon_k - \gamma_k) z_k \right| \leq \sum_{k=N+1}^{\infty} |z_k|$$

En prenant $N \in \mathbb{N}$ tel que $\sum_{k=N+1}^{\infty} |z_k| < \varepsilon$, on obtient

$$d((\varepsilon_n), (\gamma_n)) < \frac{1}{2^N} \implies |f((\varepsilon_n)) - f((\gamma_n))| \leq \sum_{k=N+1}^{\infty} |z_k| \leq \varepsilon$$

ce qui montre la continuité de f et par conséquent la compacité de K .



Applications linéaires continues

I Quelques propriétés

Dans ce chapitre, on considère deux \mathbb{K} -espaces vectoriels de dimension quelconque E et F munis respectivement des normes $\|\cdot\|_E$ et $\|\cdot\|_F$, où \mathbb{K} est égal à \mathbb{R} ou \mathbb{C} .

Proposition I.1.

Soit $u \in \mathcal{L}(E, F)$. On a

$$u \text{ est continue} \iff \exists C > 0, \forall x \in E, \|u(x)\|_F \leq C \|x\|_E$$

Preuve

(\Leftarrow) On a pour tout $y \in E$,

$$\|u(x) - u(y)\| = \|u(x - y)\| \leq C \|x - y\| \xrightarrow{x \rightarrow y} 0$$

Donc u est bien continue.

(\Rightarrow) Pour cette implication, on va uniquement utiliser le fait que u est continue en 0.

Montrons que u est bornée sur $B_f(0, 1)$. u étant continue en 0, il existe $r > 0$ tel que

$$\forall x \in B_f(0, r), \|u(x)\|_F \leq 1$$

ici, on a utilisé la définition de la continuité en 0 en prenant $\varepsilon = 1$. Soit $x \in B_f(0, 1)$, on a $rx \in B_f(0, r)$ et alors $\|u(rx)\|_F \leq 1$. On en déduit donc que

$$\forall x \in B_f(0, 1), \|u(x)\|_F \leq \frac{1}{r}$$

On notant $C = \frac{1}{r}$, on a pour tout $x \in E \setminus \{0\}$, $\left\|u\left(\frac{x}{\|x\|_E}\right)\right\|_F \leq C$, i.e.

$$\forall x \in E, \|u(x)\|_F \leq C \|x\|_E$$

d'où le résultat voulu.

Proposition I.2.

Soit $u \in \mathcal{L}(E, F)$. les propositions suivantes sont équivalentes

1. u est continue.
2. u est continue en 0.
3. u est continue en un point de E .
4. u est lipschitzienne.
5. u est bornée sur $S(0, 1)$.
6. u est bornée sur $B_f(0, 1)$.
7. u est bornée sur une boule non réduite à un point.

Preuve

→ Les implications $(1) \Rightarrow (2) \Rightarrow (3)$ sont évidentes.

→ $(3) \Rightarrow (4)$ Si u est continue en un point $a \in E$, alors $u(x+a) \xrightarrow{x \rightarrow 0} u(a)$, donc

$$u(x) = u(x+a) - u(a) \xrightarrow{x \rightarrow 0} 0$$

u est donc continue en 0 et donc d'après la preuve de la proposition I.1., u est lipschitzienne.

→ $(4) \Rightarrow (5)$ si u est lipschitzienne de facteur de lipschitzianité $k \geq 0$, alors on a pour tout $x \in S(0, 1)$,

$$\|u(x)\|_F = \|u(x) - u(0)\|_F \leq k \|x\|_E = k$$

donc u est bornée sur $S(0, 1)$.

→ $(5) \Rightarrow (6)$ Soit M un majorant de $x \mapsto \|u(x)\|_F$ sur $S(0, 1)$. On a pour tout $x \in B_f(0, 1) \setminus \{0\}$,

$$\|u(x)\|_F = \|x\|_E \left\| u\left(\frac{x}{\|x\|_E}\right) \right\|_F \leq M \|x\|_E \leq M$$

donc u est bien bornée sur $B_f(0, 1)$.

→ $(6) \Rightarrow (7)$ Cette implication est évidente.

→ $(7) \Rightarrow (1)$ Soit $(a, r) \in E \times \mathbb{R}_+^*$ tel que u est bornée sur $B_f(a, r)$ et M un majorant de $x \mapsto \|u(x)\|_F$ sur $B_f(a, r)$. On a pour tout $x \in B_f(0, 1)$,

$$r \|u(x)\|_F - \|u(a)\|_F \leq \|u(a + rx)\|_F \leq M$$

et alors

$$\|u(x)\|_F \leq \frac{M + \|u(a)\|_F}{r} := C$$

On en déduit que pour tout $x \in E \setminus \{0\}$,

$$\|u(x)\|_F = \|x\|_E \left\| u\left(\frac{x}{\|x\|_E}\right) \right\|_F \leq C \|x\|_E$$

la proposition I.1. nous permet donc d'affirmer le fait que u est continue.

Proposition I.3.

Soit $u \in \mathcal{L}(E, F)$ continue. Les trois nombres suivants sont égaux.

1. $\sup_{x \in B_f(0, 1)} \|u(x)\|_F$
2. $\sup_{x \in S(0, 1)} \|u(x)\|_F$
3. $\inf \{C \geq 0, \forall x \in E, \|u(x)\|_F \leq C \|x\|_E\}$

De plus, lorsque E est de dimension finie, les bornes inférieures (2) et (1) sont atteinte alors que (3) est atteinte peu importe la dimension de E . On appelle ce nombre norme d'opérateur de u et on le note $\|u\|$.

Preuve

→ $(1) = (2)$

- On a $S(0, 1) \subset B_f(0, 1)$, donc $(1) \geq (2)$

- On a pour tout $x \in B_f(0, 1) \setminus \{0\}$,

$$\|u(x)\|_F = \|x\|_E \left\| u\left(\frac{x}{\|x\|_E}\right) \right\| \leq \|x\|_E \sup_{y \in S(0,1)} \|u(y)\|_F \leq \sup_{x \in S(0,1)} \|u(x)\|_F$$

On en déduit donc que (1) \leq (2) et que finalement (1) $=$ (2).

\rightarrow (2) $=$ (3) On a

$$\begin{aligned} (3) &= \inf \{C \geq 0, \forall x \in E, \|u(x)\|_F \leq C \|x\|_E\} \\ &= \inf \left\{C \geq 0, \forall x \in E \setminus \{0\}, \left\| u\left(\frac{x}{\|x\|_E}\right) \right\|_F \leq C \right\} \\ &= \inf \{C \geq 0, \forall x \in S(0,1), \|u(x)\|_F \leq C\} \\ &= \sup_{x \in S(0,1)} \|u(x)\|_F = (2) \end{aligned}$$

Or, (2) $\in \{C \geq 0, \forall x \in E, \|u(x)\|_F \leq C \|x\|_E\}$, donc la borne inférieure (3) est bien atteinte.

Notation : On note $\mathcal{L}_c(E, F)$ l'ensemble des application linéaires continues de E dans F .

Proposition I.4.

$|||\cdot|||$ est une norme sur $\mathcal{L}_c(E, F)$.

Preuve : La preuve est laissée comme exercice au lecteur.

Proposition I.5.

Soit G un espace vectoriel normé, $u \in \mathcal{L}_c(E, F)$ et $v \in \mathcal{L}_c(F, G)$. On a

$$|||v \circ u||| \leq |||v||| \times |||u|||$$

Preuve : on a pour tout $x \in E$,

$$\|v \circ u(x)\|_G \leq |||v||| \|u(x)\|_F \leq |||v||| \times |||u||| \|x\|_E$$

On peut alors dire par définition de la norme d'opérateur que $|||v \circ u||| \leq |||v||| \times |||u|||$.

Remarque : en pratique, pour une application linéaire $u \in \mathcal{L}_c(E, F)$ donnée, on peut calculer $|||u|||$ en utilisant l'égalité suivante :

$$|||u||| = \sup_{x \in E \setminus \{0\}} \frac{\|u(x)\|_F}{\|x\|_E}$$

Application : On peut utiliser cette nouvelle définition de la continuité d'une application linéaire pour énoncer une nouvelle formulation des résultats de comparaison de normes.

Soit N_1 et N_2 deux normes sur l'espace vectoriel normé E . On a

N_1 plus fine que $N_2 \iff \exists C > 0, \forall x \in E, N_2(x) \leq CN_1(x)$

\iff L'application linéaire $Id : \begin{cases} (E, N_1) & \longrightarrow (E, N_2) \\ x & \mapsto x \end{cases}$ est continue.

\iff Pour tout $\Omega \in \mathcal{P}(E)$, Ω est ouvert dans $(E, N_2) \implies Id^{-1}(\Omega)$ est ouvert dans (E, N_1)

II Exercices

Exercice II.1.

1. On pose $E = \mathcal{C}([0, 1], \mathbb{R})$, $a \in [0, 1]$ et $u \in \mathcal{L}(E, \mathbb{R})$ définie par $\forall f \in E$, $u(f) = f(a)$. Étudier la continuité de u pour les normes $\|\cdot\|_\infty$, $\|\cdot\|_1$ et $\|\cdot\|_2$.
2. On pose $F = \mathcal{C}^1([0, 1], \mathbb{R})$ muni de la norme $\|\cdot\|$ définie par $\forall f \in F$, $\|f\| = \|f\|_\infty + \|f'\|_\infty$. On considère $v \in \mathcal{L}(F, E)$ définie par $\forall f \in F$, $v(f) = f'$. Étudier la continuité de v pour $\|\cdot\|$ et $\|\cdot\|_\infty$ lorsque E est muni de $\|\cdot\|_\infty$.
3. Calculer $\|u\|$ pour $\|\cdot\|_\infty$.
4. Soit $u \in \mathcal{L}(E, \mathbb{R})$ définie par $\forall f \in E$, $u(f) = \sum_{n=0}^{\infty} \frac{(-1)^n}{2^n} f\left(\frac{1}{2^n}\right)$. Montrer que u est bien définie, linéaire et continue pour $\|\cdot\|_\infty$ mais que $\|u\|$ n'est pas atteinte.

Exercice II.2.

Soit $u \in \mathcal{L}(E, F)$. Montrer que les deux propositions suivantes sont équivalentes

1. u est continue
2. $\{x \in E, \|u(x)\|_F = 1\}$ est fermé dans E .

Exercice II.3.

On suppose que $\mathbb{K} = \mathbb{R}$. Soit u un morphisme additif de E dans F borné sur $B_f(0, 1)$. Montrer que u est une application linéaire continue.

Exercice II.4.

Soit $u \in \mathcal{L}(E, \mathbb{R})$. Montrer que les propositions suivantes sont équivalentes.

1. u est continue.
2. $\text{Ker } u$ est fermé.

Exercice II.5.

Soit X un espace métrique compact. On considère l'espace vectoriel $E = \mathcal{C}(X, \mathbb{R})$ muni de $\|\cdot\|_\infty$.

1. Soit u une forme linéaire de E dans \mathbb{R} . On suppose que

$$\forall f \in E, f \geq 0 \implies u(f) \geq 0$$

Montrer que u est continue et trouver $\|u\|$.

2. Soit $\chi : E \rightarrow \mathbb{R}$ un morphisme d'anneau unitaire et linéaire, montrer que χ est continu.
3. Montrer qu'il existe $x_0 \in X$ tel que pour tout $f \in E$, $\chi(f) = f(x_0)$.

Correction de l'exercice II.1. :

1. Étudions la continuité de u pour les 3 normes de l'énoncé.

→ Continuité pour $\|\cdot\|_\infty$

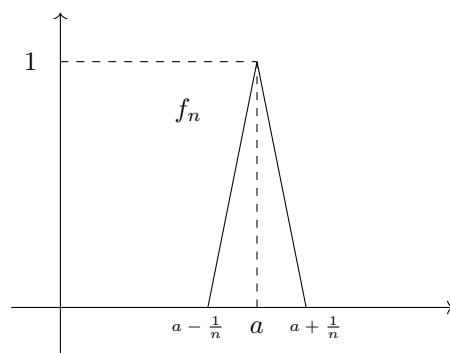
On a pour tout $f \in E$, $|u(f)| = |f(a)| \leq \|f\|_\infty$, donc u est continue pour $\|\cdot\|_\infty$.

→ Continuité pour $\|\cdot\|_1$

On considère la suite de fonctions (f_n) définie par

$$\forall n \in \mathbb{N}^*, \forall x \in [0, 1], f_n(x) = \begin{cases} n \left(x - a + \frac{1}{n} \right) & \text{si } x \in \left[a - \frac{1}{n}, a \right] \\ n \left(-x + a + \frac{1}{n} \right) & \text{si } x \in \left[a, a + \frac{1}{n} \right] \\ 0 & \text{sinon} \end{cases}$$

Pour comprendre l'intuition derrière cette construction, voici un dessin d'un terme de la suite (f_n) .



On a pour tout $n_0 \in \mathbb{N}^*$ assez grand pour qu'on ait $\left[a - \frac{1}{n}, a + \frac{1}{n} \right] \subset [0, 1]$ et soit $n \geq n_0$,

$$\frac{|u(f)|}{\|f\|_1} = \frac{|f(a)|}{1/n} = n \xrightarrow{n \rightarrow +\infty} +\infty$$

Donc $\begin{cases} E \setminus \{0\} & \longrightarrow \mathbb{R} \\ f & \longmapsto \frac{u(f)}{\|f\|_1} \end{cases}$ est non bornée, et alors u n'est pas continue pour $\|\cdot\|_1$.

→ Continuité pour $\|\cdot\|_2$

On pose $(g_n) = (\sqrt{f_n})_{n \in \mathbb{N}^*}$. On a pour tout $n \geq n_0$,

$$\frac{|u(f)|}{\|f\|_2} = \frac{1}{\sqrt{1/n}} = \sqrt{n} \xrightarrow{n \rightarrow +\infty} +\infty$$

ce qui nous permet comme avant de conclure que u n'est pas continue pour $\|\cdot\|_2$. La non continuité pour $\|\cdot\|_2$ aurait aussi pu être démontrée en utilisant le fait que $\|\cdot\|_2$ est plus fine que $\|\cdot\|_1$.

2. Etudions la continuité de v pour les deux normes de l'énoncé.

→ Continuité pour $\|\cdot\|$

On a pour tout $f \in C^1([0, 1], \mathbb{R})$, $\|v(f)\|_\infty = \|f'\|_\infty \leq \|f\|_\infty + \|f'\|_\infty = \|f\|$. On en déduit donc que u est continue pour $\|\cdot\|$.

→ Continuité pour $\|\cdot\|_\infty$

On considère la suite (f_n) de fonctions à valeurs dans $C([0, 1], \mathbb{R})$ définie par

$$\forall n \in \mathbb{N}, \forall x \in [0, 1], f_n(x) = e^{nx}$$

On a alors pour tout $n \in \mathbb{N}$,

$$\frac{\|v(f_n)\|_\infty}{\|f_n\|_\infty} = n \xrightarrow{n \rightarrow +\infty} +\infty$$

Ce qui permet de dire que u n'est pas continue pour $\|\cdot\|_\infty$.

3. On a pour tout $f \in E$, $|u(f)| \leq \|f\|_\infty$, donc $\|u\| \leq 1$. De plus, si on considère f la fonction constante égale à 1 sur $[0, 1]$, on a $|u(f)| = \|f\|_\infty = 1$, ce qui nous permet d'affirmer que $\|u\| = 1$.

4. → Montrons que u est bien définie et linéaire.

Soit $f \in E$. f est continue donc bornée sur le segment $[0, 1]$. Soit M un majorant de $|f|$. On a pour tout $n \in \mathbb{N}$,

$$\left| \frac{(-1)^n}{2^n} f\left(\frac{1}{2^n}\right) \right| \leq \frac{M}{2^n}$$

Le terme de gauche est le terme générale d'une série convergence, donc la série $\sum_{n=0}^{\infty} \frac{(-1)^n}{2^n} f\left(\frac{1}{2^n}\right)$

est absolument convergente ce qui nous permet d'affirmer que u est bien définie.

On a aussi pour tout $f, g \in E$,

$$\begin{aligned} u(f+g) &= \sum_{n=0}^{\infty} \frac{(-1)^n}{2^n} \left(f\left(\frac{1}{2^n}\right) + g\left(\frac{1}{2^n}\right) \right) \\ &= \sum_{n=0}^{\infty} \frac{(-1)^n}{2^n} f\left(\frac{1}{2^n}\right) + \sum_{n=0}^{\infty} \frac{(-1)^n}{2^n} g\left(\frac{1}{2^n}\right) \\ &= u(f) + u(g) \end{aligned}$$

Donc u est bien linéaire.

→ Montrons que u est continue

On a pour tout $f \in E$,

$$|u(f)| = \left| \sum_{n=0}^{\infty} \frac{(-1)^n}{2^n} f\left(\frac{1}{2^n}\right) \right| \leq \sum_{n=0}^{\infty} \frac{1}{2^n} \|f\|_\infty = 2 \|f\|_\infty$$

donc u est bien continue et $\|u\| \leq 2$.

→ Montrons que $\|u\| = 2$

Soit $(f_N)_{N \in \mathbb{N}}$ une suite à valeurs dans $B_f(0, 1)$ telle que pour tout $N \in \mathbb{N}$, $\forall n \leq N$, $f_N\left(\frac{1}{2^n}\right) = (-1)^n$ et $\|f_N\|_\infty \leq 1$. On alors pour tout $N \in \mathbb{N}$,

$$\begin{aligned} |u(f_N)| &= \left| \sum_{n=0}^{\infty} \frac{(-1)^n}{2^n} f_N\left(\frac{1}{2^n}\right) \right| = \left| \sum_{n=0}^N \frac{1}{2^n} + \sum_{n=N+1}^{\infty} \frac{(-1)^n}{2^n} f_N\left(\frac{1}{2^n}\right) \right| \\ &= \left| 2 - \frac{1}{2^N} + \sum_{n=N+1}^{\infty} \frac{(-1)^n}{2^n} f_N\left(\frac{1}{2^n}\right) \right| \\ &\geq 2 - \frac{1}{2^N} - \sum_{n=N+1}^{\infty} \frac{1}{2^n} \|f_N\|_\infty \\ &\geq 2 - \frac{1}{2^{N-1}} \xrightarrow{N \rightarrow \infty} 2 \end{aligned}$$

Par caractérisation séquentielle de la borne supérieure, on a $\sup_{f \in B_f(0,1)} |u(f)| = 2$ et alors $\|u\| = 2$.

→ Montrons finalement que $\|u\|$ n'est pas atteinte

Supposons le contraire. On dispose alors de $f \in E$ telle que $\|f\|_\infty = 1$ et $|u(f)| = 2$.

En supposant sans perte de généralité que $u(f) = 2$, on a que

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{2^n} f\left(\frac{1}{2^n}\right) = 2 = \sum_{n=0}^{\infty} \frac{1}{2^n}$$

et alors

$$\sum_{n=0}^{\infty} \frac{1}{2^n} \underbrace{\left(1 - (-1)^n f\left(\frac{1}{2^n}\right)\right)}_{\geq 0} = 0$$

Il s'agit d'une somme de nombres positifs qui est nulle, donc tous les termes de la somme sont nuls. On a alors pour tout $n \in \mathbb{N}$, $f\left(\frac{1}{2^n}\right) = (-1)^n$. f n'admet pas de limite en 0 et n'est donc pas continue en 0, ce qui nous permet d'affirmer que $f \notin E$, ce qui est absurde.

Correction de l'exercice II.2. :

Posons $K = \{x \in E, \|u(x)\|_F = 1\}$.

$\rightarrow (1) \Rightarrow (2)$ L'application $f : x \mapsto \|u(x)\|_F$ est continue, donc $\{x \in E, \|u(x)\|_F = 1\} = f^{-1}(\{1\})$ est fermé car c'est l'image réciproque d'un fermé par une application continue.

$\rightarrow (2) \Rightarrow (1)$ Procédons par contraposée. Supposons que u n'est pas continue, u n'est donc pas bornée sur $S(0, 1)$. On dispose alors d'une suite $(x_n) \in S(0, 1)^\mathbb{N}$ telle que $\|u(x_n)\| \xrightarrow{n \rightarrow +\infty} +\infty$. Soit n_0 assez grand pour qu'on ait pour tout $n \geq n_0$, $\|u(x_n)\| > 0$. On pose alors pour tout $n \geq n_0$, $y_n = \frac{x_n}{\|u(x_n)\|}$. Pour tout $n \geq n_0$, on a $y_n \in \{x \in E, \|u(x)\|_F = 1\}$ et

$$\|y_n\|_E = \frac{\|x_n\|_E}{\|u(x_n)\|_F} = \frac{1}{\|u(x_n)\|_F} \xrightarrow{n \rightarrow +\infty} 0$$

Mais $0 \notin K$. on a trouvé une suite à valeurs dans K qui converge vers un élément qui n'est pas dans cet ensemble. On en déduit que K n'est pas fermé.

Correction de l'exercice II.3. :

On a tout d'abord

$$\forall n \in \mathbb{Z}, \forall x \in E, f(nx) = nf(x)$$

A partir de cette propriété, on peut facilement en déduire que

$$\forall r \in \mathbb{Q}, \forall x \in E, f(rx) = rf(x)$$

Soit M un majorant de f sur $B_f(0, 1)$. Soit $\lambda \in \mathbb{R}$, et $(r_n) \in \mathbb{Q}^\mathbb{N}$ telle que $r_n \xrightarrow{n \rightarrow +\infty} \lambda$. Soit $x \in E$, pour tout $p \in \mathbb{N}^*$ il existe $N_p \in \mathbb{N}$ tel que pour tout $n \geq N_p$, $(r_n - \lambda)x \in B\left(0, \frac{1}{p}\right)$. On a alors pour tout $p \in \mathbb{N}$, il existe $N_p \in \mathbb{N}^*$ tel que pour tout $n \geq N_p$,

$$\|f((r_n - \lambda)x)\| = \frac{1}{p} \|\underbrace{f(p(r_n - \lambda)x)}_{\in B_f(0,1)}\| \leq \frac{M}{p}$$

i.e.

$$\|r_nf(x) - f(\lambda x)\| \leq \frac{M}{p}$$

On a alors

$$\|\lambda f(x) - f(\lambda x)\| \leq \frac{M}{p} + \|(r_n - \lambda)f(x)\| \xrightarrow{n \rightarrow +\infty} \frac{M}{p}$$

On en déduit donc que pour tout $p \in \mathbb{N}^*$, $\|\lambda f(x) - f(\lambda x)\| \leq \frac{M}{p}$ et que finalement $f(\lambda x) = \lambda f(x)$. On conclut que f est une application linéaire bornée sur $B_f(0, 1)$, donc continue.

Correction de l'exercice II.4. :

- (1) ⇒ (2) On a $\text{Ker } u = u^{-1}(\{0\})$. Il s'agit de l'image réciproque d'un fermé par une application continue, c'est donc un fermé.
- (2) ⇒ (1) Si $u = 0$, $\text{Ker } u = E$ est fermé. Supposons donc maintenant que $u \neq 0$. $H = \text{Ker } u$ est un hyperplan et u est surjective. Il existe donc $a \in E$ tel que $u(a) = 1$. On a alors

$$\forall x \in E, u(x) = 1 \iff u(x - a) = 0 \iff x \in a + H$$

de même, il est facile de voir que

$$\forall x \in E, u(x) = -1 \iff u(x + a) = 0 \iff x \in -a + H$$

Posons donc $F = (a + H) \cup (-a + H)$. $a + H$ et $-a + H$ sont fermés car ce sont les images directes du fermé H par respectivement $x \mapsto a + x$ et $x \mapsto -a + x$ qui sont deux applications linéaires bijectives d'inverse continu, donc F est fermé. Or $0 \notin F$ et F^c est ouvert, donc il existe $r > 0$ tel que $B_f(0, r) \subset F^c$.

Montrons que pour tout $x \in B_f(0, r)$, $|u(x)| \leq 1$. Soit $x \in B(0, r)$ non nul. On suppose par l'absurde que $|u(x)| > 1$. On a alors $y := \frac{x}{|u(x)|} \in B(0, r)$ et $u(y) \in \{1, -1\}$, i.e. $y \in F$ ce qui est absurde étant donné que $y \in B(0, r) \subset F^c$. On a donc trouvé une boule non réduite à un point où u est bornée, ce qui nous permet d'affirmer que u est continue.

Correction de l'exercice II.5. :

1. On a pour tout $f, g \in E$,

$$f \geq g \implies f - g \geq 0 \implies u(f - g) \geq 0 \implies u(f) \geq u(g)$$

Posons e la fonction constante égale à 1 sur X . On a pour tout $f \in E$,

$$-\|f\|_\infty e \leq f \leq \|f\|_\infty e$$

en posant $C = u(e)$ et en appliquant u de chaque côté de l'inégalité on obtient

$$-C \|f\|_\infty \leq u(f) \leq C \|f\|_\infty$$

et enfin

$$\forall f \in E, |u(f)| \leq C \|f\|_\infty$$

Donc u est continue et $\|u\| \leq C$, mais $u(e) = C$ et $e \in B_f(0, 1)$, donc $\|u\| \geq C$, i.e. $\|u\| = C$.

2. Soit $f \in E$ tel que $f \geq 0$, on pose $g = \sqrt{f}$. On a $g \in E$ et

$$\chi(f) = \chi(g^2) = \chi(g)^2 \geq 0$$

Il suffit alors d'appliquer la question 1.



CHAPITRE 11.7

Espaces vectoriels normés de dimension finie

Dans tout ce chapitre, \mathbb{K} est égal à \mathbb{R} ou \mathbb{C} . On considère E un \mathbb{K} -espace vectoriel normé de dimension finie $n \geq 1$ et on pose (e_1, \dots, e_n) une base de cet espace.

I Équivalence des normes

Proposition I.1.

Dans \mathbb{R}^n , toutes les normes sont équivalentes.

Preuve : Soit N une norme sur \mathbb{R}^n . En posant $(\varepsilon_1, \dots, \varepsilon_n)$ la base canonique de \mathbb{R}^n , on a pour tout $x = x_1\varepsilon_1 + \dots + x_n\varepsilon_n \in \mathbb{R}^n$,

$$N(x) = N(x_1\varepsilon_1 + \dots + x_n\varepsilon_n) \leq \sum_{k=1}^n |x_k| N(\varepsilon_k) \leq \left(\sum_{k=1}^n N(\varepsilon_k) \right) \|x\|_\infty$$

Et on a en posant $C = \sum_{k=1}^n N(\varepsilon_k)$ pour tout $x, y \in E$

$$|N(x) - N(y)| \leq N(x - y) \leq C \|x - y\|_\infty$$

N est donc lipschitzienne et alors continue pour $\|\cdot\|_\infty$.

Posons $S = \{x \in \mathbb{R}^n, \|x\|_\infty = 1\}$. S est fermé et borné dans un espace de dimension finie pour $\|\cdot\|_\infty$, c'est donc un compact d'après la proposition III.2 du chapitre 11.5. N étant continue, elle est bornée sur S et y atteint sa borne inférieure qu'on note α . Il existe alors $y \in S$ pour lequel pour tout $x \in E \setminus \{0\}$,

$$N\left(\frac{x}{\|x\|_\infty}\right) \geq N(y) = \alpha > 0$$

et alors

$$\alpha \|x\|_\infty \leq N(x) \leq C \|x\|_\infty$$

On en déduit donc que tout norme N sur \mathbb{R}^n est équivalent à $\|\cdot\|_\infty$ et que donc par transitivité, toutes les normes sur \mathbb{R}^n sont équivalentes.

Corollaire I.2.

E étant isomorphe à \mathbb{R}^n , toutes les normes sur E sont équivalentes.

Preuve : Soit $\varphi : \mathbb{R}^n \rightarrow E$ un isomorphisme et soit N_1 et N_2 deux normes sur E . Sur \mathbb{R}^n , les deux normes $N_1 \circ \varphi$ et $N_2 \circ \varphi$ sont équivalentes. Il existe donc $\beta, \gamma > 0$ tels que pour tout x

$$\gamma N_2(\varphi(x)) \leq N_1(\varphi(x)) \leq \beta N_2(\varphi(x))$$

Or φ étant surjective, pour tout $y \in E$, il existe $x \in \mathbb{R}^n$ tel que $\varphi(x) = y$, on a donc pour tout $y \in E$,

$$\gamma N_2(y) \leq N_1(y) \leq \beta N_2(y)$$

N_1 et N_2 sont alors équivalentes.

II Suites et composantes

Proposition II.1.

Soit $(u_p) \in E^{\mathbb{N}}$, on pose pour tout $p \in \mathbb{N}$, $u_p = \sum_{k=1}^n u_{p,k} e_k$ et soit $\|\cdot\|$ une norme sur E . Les propositions suivantes sont équivalentes.

1. (u_p) converge pour $\|\cdot\|$.
2. $\forall k \in \llbracket 1; n \rrbracket$, $\exists l_k \in \mathbb{K}$, $u_{n,k} \xrightarrow[n \rightarrow +\infty]{} l_k$.

Dans ce cas, on a $u_n \xrightarrow[n \rightarrow +\infty]{} \sum_{k=1}^n l_k e_k$.

Preuve : On pose pour tout $x = \sum_{k=1}^n x_k e_k$, $N(x) = \max_{k \in \llbracket 1; n \rrbracket} |x_k|$. N est une norme sur E équivalente à $\|\cdot\|$.

On a alors

$$\begin{aligned} (1) &\iff (u_n) \text{ converge vers un certain } l = \sum_{k=1}^n l_k e_k \text{ pour } \|\cdot\| \\ &\iff (u_n) \text{ converge vers un certain } l \text{ pour } N \\ &\iff \exists l = (l_1, \dots, l_n) \in \mathbb{K}^n, \max_{k \in \llbracket 1; n \rrbracket} |u_{n,k} - l_k| \xrightarrow[n \rightarrow +\infty]{} 0 \\ &\iff \exists l \in E, \forall k \in \llbracket 1; n \rrbracket, u_{n,k} \xrightarrow[n \rightarrow +\infty]{} l_k \iff (2) \end{aligned}$$

Application : Une suite de matrices de $\mathcal{M}_n(\mathbb{R})$ converge si et seulement les suites de ses coefficients convergent.

Proposition II.2.

Soit X un espace métrique et A une partie de X . Soit $a \in \overline{A}$ et l'application

$$f : \begin{cases} A &\longrightarrow E \\ x &\longmapsto \sum_{k=1}^n f_k(x) e_k \end{cases}$$

Avec pour tout k , f_k une application de A dans E .

Les propositions suivantes sont équivalentes.

1. f possède une limite finie en a selon A , notée l .
2. Chaque f_k possède une limite finie en a , notée l_k .

Preuve : La preuve est laissé comme exercice au lecteur.

III Compacité et complétude

Théorème (Bolzano Weierstraß) III.1.

Soit (u_p) une suite à valeurs dans E . Si (u_p) est bornée pour $\|\cdot\|$, alors elle admet au moins une valeur d'adhérence.

Preuve : Posons pour tout $x = \sum_{k=1}^n x_k e_k \in E$, $N(x) = \max_{k \in \llbracket 1; n \rrbracket} |x_k|$.

N étant équivalente à $\|\cdot\|$, donc (u_p) est aussi bornée pour N . Toutes les suites $(u_{p,k})_{p \in \mathbb{N}}$ sont alors bornées. Montrons par récurrence sur r la propriété suivante :

il existe une extractrice φ_r telle que pour tout $i \in \llbracket 1; r \rrbracket$, $(u_{\varphi_r(p), i})$ est convergence vers $l_i \in \mathbb{R}$

La propriété pour $r = 1$ est vraie car il s'agit du théorème de Bolzano Weierstraß pour les suites réelles et complexes. Supposons maintenant que la propriété est vraie pour $r \in \llbracket 1; n - 1 \rrbracket$. La suite $(u_{\varphi_r(p), r+1})$ est bornée, il existe alors une extractrice φ telle que $(u_{\varphi_r \circ \varphi(p), r+1})$ converge vers un certain l_{r+1} . On a alors pour tout $i \in \llbracket 1; r+1 \rrbracket$, $(u_{\varphi_r \circ \varphi(p), i})$ converge vers l_i . La propriété est alors vraie pour $r = n$ ce qui implique que, pour $\|\cdot\|_\infty$, $(u_{\varphi_n(p)})$ converge vers $l = \sum_{k=1}^n l_k e_k$ et donc par équivalence des normes N et $\|\cdot\|_\infty$, $(u_{\varphi_n(p)})$ converge vers l pour N , d'où le résultat voulu.

Corollaire III.2.

Les propositions suivantes sont vraies. Une partie A de E est compacte si elle est fermée et bornée.

Preuve : Soit $(u_p) \in A^\mathbb{N}$. (u_p) est bornée, le théorème précédent nous permet d'affirmer qu'il existe une extractrice φ telle que $u_{\varphi(p)} \xrightarrow[p \rightarrow +\infty]{} a \in E$. A étant fermé, on a $a \in A$, d'où la compacité de A .

Proposition III.3.

L'espace vectoriel normé de dimension finie $(E, \|\cdot\|)$ est complet.

Preuve : Soit $(u_p) \in E^\mathbb{N}$ une suite de Cauchy et $N \in \mathbb{N}$ tel que pour tout $m, n \geq N$,

$$\|u_m - u_n\| \leq 1$$

On a alors pour tout $n \in \mathbb{N}$,

$$\|u_n\| \leq \max\{\|u_0\|, \dots, \|u_{N-1}\|, \|u_N\| + 1\}$$

La suite (u_p) est bornée, donc d'après le théorème III.1, elle admet une suite extraite convergente. D'après la remarque à la fin de la page 4 du chapitre 11.5, toute suite de Cauchy admettant une valeur d'adhérence converge, d'où le résultat voulu.

Corollaire III.4.

Soit (u_p) une suite à valeurs dans E .

$$\sum \|u_p\| \text{ converge} \implies \sum u_p \text{ converge}$$

Preuve : Supposons que $\sum \|u_p\|$ converge et soit $\varepsilon > 0$. Il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$,

$$\sum_{k=n}^{\infty} \|u_p\| \leq \varepsilon$$

On a alors pour tout $m \geq n \geq N$,

$$\left\| \sum_{k=n}^m u_k \right\| \leq \sum_{k=n}^m \|u_k\| \leq \varepsilon$$

La suite $(U_n) = \left(\sum_{k=0}^n u_k \right)_{n \in \mathbb{N}}$ est de Cauchy et E est complet, donc elle converge, d'où la convergence de la série $\sum u_p$.

Remarque : La propriété ci-dessus est en particulier vraie pour tout espace vectoriel normé complet.

Proposition III.5.

Soit A une partie fermée de E et $f : A \rightarrow A$. Si f vérifie la propriété

$$\exists q \in]0, 1[, \forall x, y \in A, \|f(x) - f(y)\| \leq q \|x - y\|$$

Alors f possède un unique point fixe dans A .

Preuve

→ Unicité

Soit l et l' deux éléments de A tels que $f(l) = l$ et $f(l') = l'$. On alors

$$q \|l - l'\| \geq \|f(l) - f(l')\| = \|l - l'\|$$

On a alors nécessairement $l = l'$.

→ Existence

Soit $a \in A$. On considère la suite $(u_n)_{n \in \mathbb{N}}$ définie par

$$\begin{cases} u_0 = a \\ \forall n \in \mathbb{N}, u_{n+1} = f(u_n) \end{cases}$$

On a alors pour tout $n > 1$,

$$\|u_{n+1} - u_n\| = \|f(u_n) - f(u_{n-1})\| \leq q \|u_n - u_{n-1}\| \leq \cdots \leq q^n \|u_1 - u_0\|$$

On a $q \in]0, 1[$, $\sum_{n \in \mathbb{N}} q^n$ est alors convergente, et par conséquent $\sum_{n \in \mathbb{N}} \|u_{n+1} - u_n\|$ est convergente. E

étant complet, le corollaire III.4 nous permet donc d'affirmer que $\sum_{n \in \mathbb{N}} u_{n+1} - u_n$ est convergente, i.e. (u_n) est convergente vers une limite qu'on note l . A est fermé donc $l \in A$ et en passant à la limite dans la relation de récurrence $f(u_n) = u_{n+1}$, on obtient par continuité de f que $l = f(l)$, d'où le résultat voulu.

Remarque : Pour démontrer le résultat ci-dessus, on n'a pas eu besoin du fait que E est de dimension finie. Il suffit que A soit complet.

Proposition III.6.

Si E est un sous espace vectoriel de dimension finie d'un \mathbb{K} -espace vectoriel $(F, \|\cdot\|)$, alors E est fermé.

Preuve : Soit (u_p) une suite à valeurs dans E qui converge vers $a \in F$. E est de dimension finie et (u_p) est convergente donc bornée dans E , il existe donc une extractrice φ telle que $u_{\varphi(p)} \xrightarrow[p \rightarrow +\infty]{} b \in E$, or par unicité de la limite, $a = b \in E$, donc E est bien fermé.

Exemple : $\mathbb{R}_n[X]$ est fermé dans $\mathcal{C}([0, 1], \mathbb{R})$ muni de la norme $\|\cdot\|_\infty$.

Théorème (théorème de représentation de Riesz) III.7.

Soit $(F, \|\cdot\|)$ un espace vectoriel normé. $B_f(0, 1)$ est compacte si et seulement si F est de dimension finie.

Preuve : La preuve sera présentée sous forme d'exercice dans la suite du chapitre.

IV Fonctions polynômes sur \mathbb{K}^n

On rappelle ici que E est un espace vectoriel normé de **dimension finie** muni de la norme $\|\cdot\|_E$ et (e_1, \dots, e_n) une base de E .

Définition IV.1.

Soit f une application de E dans \mathbb{K} . Soit $\mathcal{E} = (\varepsilon_1, \dots, \varepsilon_n)$ une base de F . On dit que f est polynomiale dans la base \mathcal{E} , lorsqu'il existe une suite $(a_\alpha)_{\alpha \in \mathbb{N}^n} \in \mathbb{K}^{\mathbb{N}^n}$ avec un nombre fini de termes non nuls telle que pour tout $x = x_1\varepsilon_1 + \dots + x_n\varepsilon_n \in E$,

$$f(x) = \sum_{(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n} a_{\alpha_1, \dots, \alpha_n} x_1^{\alpha_1} \dots x_n^{\alpha_n}$$

Proposition IV.2.

Soit F un espace vectoriel normé quelconque.

1. Toute application u linéaire de E dans F est continue.
2. Toute application f polynomiale dans une base de E à valeurs dans \mathbb{K} est continue.

Preuve

1. soit N une norme sur E définie de la manière suivante

$$\forall x = x_1e_1 + \dots + x_ne_n \in E, N(x) = \sum_{k=1}^n |x_k|$$

On alors pour tout $x = x_1e_1 + \dots + x_ne_n \in E$,

$$\|u(x)\|_F = \|x_1u(e_1) + \dots + x_nu(e_n)\|_F \leq \sum_{k=1}^n |x_k| \|u(e_k)\|_F \leq CN(x)$$

Avec $C = \max_{k \in [1; n]} \|u(e_k)\|_F$. Mais E est de dimension finie, donc N est équivalente à $\|\cdot\|_E$, donc u est continue.

2. Posons pour tout $x = x_1e_1 + \dots + x_ne_n \in E$,

$$f(x) = \sum_{(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n} a_{\alpha_1, \dots, \alpha_n} x_1^{\alpha_1} \dots x_n^{\alpha_n}$$

Pour tout $k \in \llbracket 1; n \rrbracket$, l'application $x \mapsto x_k$ est continue, et f est somme et produit d'applications de cette forme qui sont toutes continues, donc f est continue.

Corollaire IV.3.

Toute application f multilinéaire de E^p dans un espace vectoriel normé F est continue.

Preuve : Considérons les p éléments de E suivants :

$$\begin{aligned} x_1 &= x_{1,1}e_1 + \dots + x_{1,n}e_n \\ x_2 &= x_{2,1}e_1 + \dots + x_{2,n}e_n \\ &\vdots \\ x_p &= x_{p,1}e_1 + \dots + x_{p,n}e_n \end{aligned}$$

On a alors

$$\begin{aligned} f(x_1, \dots, x_p) &= f\left(\sum_{i_1=1}^n x_{1,i_1} e_{i_1}, \sum_{i_2=1}^n x_{2,i_2} e_{i_2}, \dots, \sum_{i_p=1}^n x_{p,i_p} e_{i_p}\right) \\ &= \sum_{(i_1, \dots, i_p) \in \llbracket 1; n \rrbracket^p} x_{i_1} \dots x_{i_p} f(e_{i_1}, \dots, e_{i_p}) \end{aligned}$$

f est donc combinaison linéaire et produit d'applications de la forme $(x_1, \dots, x_p) \mapsto x_{k,l}$ avec $(k, l) \in \llbracket 1; p \rrbracket \times \llbracket 1; n \rrbracket$. Toutes ces applications sont continues, donc f est continue.

V Exercices

Exercice V.1.

Soit $f : \mathbb{R} \rightarrow \mathbb{R}^+$ de classe \mathcal{C}^n telle que f et $f^{(n)}$ sont bornées. Montrer que pour tout $k \in \llbracket 1; n-1 \rrbracket$, $f^{(k)}$ est bornée.

Exercice V.2.

Soit $n \in \mathbb{N}^*$. On note $\Omega = \{P \in \mathbb{R}_n[X], \deg P = n \text{ et } P \text{ est scindé à racines simples}\}$. Montrer que Ω est ouvert dans $\mathbb{R}_n[X]$.

Exercice V.3.

Soit $(P_k)_{k \in \mathbb{N}}$ une suite à valeurs dans $\mathbb{R}_n[X]$. On suppose que la suite (\tilde{P}_k) de fonctions polynômes associée à (P_k) converge simplement vers $f \in \mathcal{C}([0, 1], \mathbb{R})$ sur $[0, 1]$. Montrer que la convergence est uniforme.

Exercice V.4.

Soit F un fermé non vide de l'espace vectoriel normé de dimension finie $(E, \|\cdot\|)$ et soit $a \in E$. Montrer qu'il existe $b \in F$ tel que $\|a - b\| = d(a, F)$.

Exercice V.5.

Soit F un sous espace de dimension finie d'un espace vectoriel normé $(G, \|\cdot\|)$ de dimension quelconque. Soit $a \in G$. Montrer qu'il existe $b \in F$ tel que $\|a - b\| = d(a, F)$.

Exercice V.6.

Soit K un compact non vide de l'espace euclidien \mathbb{R}^n . Montrer qu'il existe une boule fermée de rayon minimum contenant K et que cette boule est unique.

Exercice V.7.

Soit f une fonction continue de l'espace vectoriel normé de dimension finie $(E, \|\cdot\|)$ dans \mathbb{R} . On suppose que $f(x) \xrightarrow[\|x\| \rightarrow +\infty]{} +\infty$. Montrer que f est minorée et qu'il existe $a \in E$ tel que $f(a) = \min_{x \in E} f(x)$.

Exercice V.8.

Ceci est un exercice visant à prouver le théorème III.7 (Théorème de Riesz).

Soit $(F, \|\cdot\|)$ un espace vectoriel normé de dimension infinie.

1. Soit G un sous-espace vectoriel de F de dimension finie. Montrer qu'il existe $a \in S(0, 1)$ tel que $d(a, F) \geq 1$.
2. Construire une suite $(a_n) \in S(0, 1)^{\mathbb{N}}$ telle que $\forall n \neq m, \|a_n - a_m\| \geq 1$.
3. Conclure.

Correction de l'exercice V.1. :

f est de classe \mathcal{C}^n , on peut alors appliquer l'égalité de Talor-Lagrange à l'ordre n pour f sur $[0, 1]$

$$\forall (x, h) \in \mathbb{R}^+ \times [0, 1], \exists c_{x,h} \in [0, 1], f(x+h) - f(x) - \frac{h^n}{n!} f^{(n)}(c_{x,h}) = \underbrace{\sum_{k=1}^{n-1} \frac{f^{(k)}(x)}{k!} h^k}_{P_x(h)}$$

D'après les hypothèses, $(x, h) \mapsto f(x+h) - f(x) - \frac{h^n}{n!} f^{(n)}(c_{x,h})$ est bornée par un certain $M > 0$. On alors en posant $g_x : h \mapsto f(x+h) - f(x) - \frac{h^n}{n!} f^{(n)}(c_{x,h})$, on a par construction, pour tout $x \in \mathbb{R}^+$, $\|g_x\|_\infty \leq M$, et alors $\|P_x\|_\infty \leq M$. Posons pour tout $P(X) = \sum_{k=0}^n a_k X^k \in \mathbb{R}_n[X]$, $N(P) = \max_{k \in \llbracket 0; n \rrbracket} |a_k|$. $\mathbb{R}_n[X]$ est de dimension finie, donc toutes les normes y sont équivalentes. En particulier, N et $\|\cdot\|_\infty$ sont équivalentes, ce qui nous permet d'affirmer qu'il existe $M' > 0$ tel que pour tout $x \in \mathbb{R}^+$, $N(P_x) < M'$. On a donc pour tout

$$x \in \mathbb{R}^+, \forall k \in \llbracket 1; n \rrbracket, \left| \frac{f^{(k)}(x)}{k!} \right| < M'$$

Ce qui nous permet d'affirmer que pour tout $k \in \llbracket 1; n \rrbracket$, $f^{(k)}$ est bornée.

Correction de l'exercice V.2. :

Soit $P \in \Omega$. P admet n racines distinctes et est scindé à racine simples, il change donc $n+1$ fois de signe sur \mathbb{R} . Soit $y_1, \dots, y_{n+1} \in \mathbb{R}$ tels que sans perte de généralité, pour tout $k \in \llbracket 1; n+1 \rrbracket$, $\text{signe}(P(y_k)) = (-1)^k$.

Posons pour tout $Q \in \mathbb{R}_n[X]$, $N(Q) = \sum_{k=1}^{n+1} |Q(y_k)|$. N est bien une norme sur $\mathbb{R}_n[X]$, car elle vérifie l'inégalité triangulaire, homogène, et pour tout polynôme Q de degré au plus n , $N(Q) = 0 \implies Q = 0$.

Posons $\varepsilon = \min_{k \in \llbracket 1; n+1 \rrbracket} |P(y_k)|$. Pour tout $Q \in \mathbb{R}_n[X]$, si $N(P - Q) < \frac{\varepsilon}{2}$, alors pour tout $k \in \llbracket 1; n+1 \rrbracket$

$$|Q(y_k) - P(y_k)| < \frac{\varepsilon}{2}$$

i.e.

$$P(y_k) - \frac{\varepsilon}{2} < Q(y_k) < P(y_k) + \frac{\varepsilon}{2}$$

Mais pour tout $k \in \llbracket 1; n+1 \rrbracket$, $|P(y_k)| \geq \varepsilon$, donc

$$\text{signe}\left(P(y_k) + \frac{\varepsilon}{2}\right) = \text{signe}\left(P(y_k) - \frac{\varepsilon}{2}\right) = \text{signe}(P(y_k))$$

Donc pour tout $k \in \llbracket 1; n+1 \rrbracket$, $Q(y_k)$ a le même signe que $P(y_k)$. En appliquant le théorème des valeurs intermédiaires sur $[y_k, y_{k+1}]$ pour tout $k \in \llbracket 1; n \rrbracket$, on trouve que Q , étant de degré n , admet n racines distinctes et donc est scindé à racines simples. On en déduit donc que $B(P, \varepsilon) \subset \Omega$ et finalement que Ω est ouvert.

Correction de l'exercice V.3. :

Soit x_0, x_1, \dots, x_n des éléments deux à deux distincts de $[0, 1]$. Posons pour tout $k \in \mathbb{N}$,

$$P_k(X) = \sum_{i=0}^n a_{k,i} X^i$$

On a alors pour tout $l \in \llbracket 0; n \rrbracket$,

$$\sum_{i=1}^n a_{k,i} x_l^i \xrightarrow{k \rightarrow +\infty} f(x_l)$$

i.e.

$$\begin{pmatrix} 1 & x_0 & \dots & x_0^n \\ 1 & x_1 & \dots & x_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \dots & x_n^n \end{pmatrix} \begin{pmatrix} a_{k,0} \\ a_{k,1} \\ \vdots \\ a_{k,n} \end{pmatrix} \xrightarrow[k \rightarrow +\infty]{} \begin{pmatrix} f(x_0) \\ f(x_1) \\ \vdots \\ f(x_n) \end{pmatrix}$$

En posant

$$V = V(x_0, x_1, \dots, x_n) = \begin{pmatrix} 1 & x_0 & \dots & x_0^n \\ 1 & x_1 & \dots & x_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \dots & x_n^n \end{pmatrix}$$

On remarque que V est une matrice de Vandermonde, elle est donc inversible. $X \mapsto V^{-1}X$ est une application linéaire en dimension finie, elle est donc continue d'après la proposition IV.2. On a alors, en multipliant par V^{-1} et en passant à la limite

$$\begin{pmatrix} a_{k,0} \\ a_{k,1} \\ \vdots \\ a_{k,n} \end{pmatrix} \xrightarrow[k \rightarrow +\infty]{} V^{-1} \begin{pmatrix} f(x_0) \\ f(x_1) \\ \vdots \\ f(x_n) \end{pmatrix} \quad (*)$$

En posant pour tout $Q(X) = \sum_{i=0}^n b_i X^i$, $N(Q) = \sum_{i=0}^n |b_i|$, on voit que N est une norme dans l'espace de dimension finie $\mathbb{R}_n[X]$, elle est donc équivalente à $\|\cdot\|_\infty : Q \mapsto \sup_{x \in [0,1]} Q(x)$. D'après $(*)$, $(P_k)_{k \in \mathbb{N}}$ converge

pour N (chaque coefficient converge) et donc par équivalence des normes, (P_k) converge aussi pour $\|\cdot\|_\infty$. (\tilde{P}_k) converge donc uniformément vers une certaine fonction continue dans $[0, 1]$ g . Il reste à montrer que $f = g$. La convergence uniforme implique la convergence simple, donc (\tilde{P}_k) converge simplement vers f et g , et donc par unicité de la limite, $f = g$.

Remarque : l'espace des fonctions polynômes de degré au plus n étant de dimension finie, il est fermé dans l'espace des fonctions continues sur $[0, 1]$. Cet argument nous permet d'affirmer que (P_k) converge uniformément vers un polynôme de degré au plus n .

Une démonstration plus directe de ce résultat peut être faite de la manière suivante. Soit a_0, \dots, a_n les limites respectives des suites de coefficients $(a_{k,0})_{k \in \mathbb{N}}, \dots, (a_{k,n})_{k \in \mathbb{N}}$. En posant $P(X) = \sum_{i=0}^n a_i X^i$, on a

$$\|\tilde{P}_k - P\|_\infty \leq \sum_{i=0}^n |a_{k,i} - a_i| \xrightarrow[k \rightarrow +\infty]{} 0$$

Correction de l'exercice V.4. :

Soit $R > d(a, F)$. On a $B_f(a, R) \cap F = K \neq \emptyset$. K est une intersection de deux fermés inclus dans l'ensemble bornée $B_f(a, R)$ en dimension finie, c'est donc une partie compacte de E . On considère la fonction

$$g : \begin{cases} K & \longrightarrow \mathbb{R} \\ x & \longmapsto \|a - x\| \end{cases}$$

g est continue sur le compact K , il y atteint donc son minimum en un élément de K qu'on note b .

Soit $y \in F$, $\begin{cases} \text{Si } y \notin K, \text{ alors } \|y - a\| > R \geq \|a - b\| \\ \text{Si } y \in K, \text{ alors } \|y - a\| \geq \|a - b\| \end{cases}$

On a donc bien $\|a - b\| = \min_{x \in F} \|a - x\| = d(a, F)$.

Correction de l'exercice V.5. :

Cet exercice se fait d'une manière identique au précédent. Soit $R > d(a, F)$ et $K = B_f(a, R) \cap F$. K est fermé borné inclus dans un espace de dimension finie F , c'est donc un compact. En reprenant les notations de l'exercice précédent, g est continue et donc atteint son minimum sur le compact K en un certain $b \in K$. Avec un raisonnement identique à l'exercice précédent, on peut affirmer que $\|a - b\| = d(a, F)$.

Correction de l'exercice V.6. :

Posons $S_K = \{\gamma \geq 0, \exists a \in \mathbb{R}^n, K \subset B_f(a, \gamma)\}$. K est borné, il existe donc une boule fermée contenant K . L'ensemble S_K est alors non vide, minoré par 0. Il admet donc une borne inférieure $r = \inf S_K$.

Soit $((a_n, r_n))_{n \in \mathbb{N}}$ une suite à valeurs dans $\mathbb{R}^n \times \mathbb{R}^+$ vérifiant les deux propriétés suivantes

$$\begin{cases} \forall n \in \mathbb{N}, K \subset B(a_n, r_n) \\ r_n \xrightarrow[n \rightarrow +\infty]{} r \end{cases}$$

D'après les hypothèses, il existe N assez grand tel que pour tout $n \geq N$ on ait $r_n \leq r + 1$. Soit $b \in K$. On a pour tout $n \geq N$,

$$\|a_n - b\| \leq r_n \leq r + 1$$

et alors

$$\|a_n\| \leq r + 1 + \|b\|$$

La suite (a_n) est bornée, ce qui nous permet en utilisant le théorème III.1 d'affirmer que (a_n) admet une suite extraite convergente. Quitte à extraire de la suite (a_n) , on suppose qu'elle est convergente vers un certain $a \in \mathbb{R}^n$.

→ Pour montrer l'existence de la boule, montrons que $K \subset B_f(a, r)$.

On a pour tout $x \in K$ et pour tout $n \in \mathbb{N}$, $\|a_n - x\| \leq r_n$. En passant à la limite, on obtient $\|a - x\| \leq r$, i.e. $x \in B_f(a, r)$. On a donc bien que $K \subset B_f(a, r)$.

→ Unicité de la boule

On sait que le rayon de la boule est unique car il est défini comme la borne inférieure de S_K , il suffit donc de montrer l'unicité du centre.

Soit $a' \in \mathbb{R}^n$ différent de a tel que $K \subset B_f(a', r)$. Soit $x \in B_f(a, r) \cap B_f(a', r)$, on a

$$\begin{aligned} 2r^2 &\geq \underbrace{\|x - a\|^2}_u + \underbrace{\|x - a'\|^2}_v = \frac{1}{2}(\|u + v\|^2 + \|u - v\|^2) \\ &= 2 \left(\left\| x - \frac{a + a'}{2} \right\|^2 + \underbrace{\left\| \frac{a - a'}{2} \right\|^2}_{\alpha} \right) \end{aligned}$$

En posant $b = \frac{a+a'}{2}$, on en déduit

$$\|x - b\| \leq \sqrt{r^2 - \underbrace{\alpha}_{>0}} < r$$

Donc $K \subset B_f(b, \sqrt{r^2 - \alpha})$ ce qui est absurde par définition de r , d'où le résultat voulu.

Correction de l'exercice V.7. :

Le fait que $f(x) \xrightarrow[\|x\| \rightarrow +\infty]{} +\infty$ se réécrit

$$\forall M > 0 \exists R > 0, \forall x \in E, \|x\| > R \implies \|f(x)\| > M$$

Appliquons cette proposition à $M = |f(0)| + 1$. f est continue sur $B_f(0, R)$ qui est fermé borné en dimension finie donc compact, elle y atteint donc son minimum en un certain $a \in B_f(0, R)$.

Or pour tout $y \in E$

- Si $\|y\| > R$, $f(y) > |f(0)| + 1 > f(a)$.
- Sinon, par construction, $f(y) \geq f(a)$

Donc f atteint bien son minimum sur E en a .

Correction de l'exercice V.8. : (Preuve du théorème de Riesz)

1. Soit $a_0 \in F \setminus G$. L'exercice V.4 nous permet d'affirmer qu'il existe $b \in G$ tel que

$$\|a_0 - b\| = \inf_{x \in G} \|x - a_0\| = d(a_0, F)$$

Posons alors $a = \frac{b-a_0}{\|b-a_0\|} \in S(0, 1)$, on a alors pour tout $x \in G$,

$$\begin{aligned} \|x - a\| &= \left\| x - \frac{a_0 - b}{\|a_0 - b\|} \right\| \\ &= \frac{1}{d(a_0, G)} \underbrace{\|b + x\|a_0 - b\|}_{=y \in G} - a_0 \| \\ &= \frac{1}{d(a_0, G)} \|y - a_0\| \geq 1 \end{aligned}$$

2. Construisons la suite a_n par récurrence. le premier terme a_0 peut être pris quelconque vérifiant $\|a_0\| = 1$.

Soit $n \in \mathbb{N}$. Supposons que les termes a_0, \dots, a_n sont bien définis. Posons $G_n = Vect(a_0, \dots, a_n)$. D'après la question précédente, il existe $a_{n+1} \in S(0, 1)$ tel que $d(a_{n+1}, G_n) \geq 1$. On a alors

$$\forall m \leq n, \|a_m - a_{n+1}\| \geq 1$$

Il est clair que la suite (a_n) telle qu'on l'a définie vérifie

$$\forall m, n \in \mathbb{N}, (n \neq m \implies \|a_n - a_m\| \geq 1) \text{ et } \forall n \in \mathbb{N}, \|a_n\| = 1$$

3. Reprenons le théorème III.7. L'énoncé du théorème est le suivant : Si H un espace vectoriel normé, alors on a l'équivalence

H est de dimension finie \iff La boule unité fermée de H est compacte

→ (\Leftarrow) nous allons faire cette implication par contraposée. Supposons que H soit de dimension infinie. La question précédente nous permet de considérer une suite $(a_n) \in S(0, 1)^{\mathbb{N}}$ telle que

$$\forall m, n \in \mathbb{N}, n \neq m \implies \|a_n - a_m\| \geq 1$$

Si la boule unité était compacte, on disposerait d'une extractrice φ telle que $(a_{\varphi(n)})$ soit convergente, et alors

$$1 \leq \|a_{\varphi(n+1)} - a_{\varphi(n)}\| \xrightarrow{n \rightarrow +\infty} 0$$

ce qui est absurde.

→ (\Rightarrow) Si H est de dimension finie, alors la boule unité fermée de H est fermé bornée en dimension finie, elle est alors compacte.



CHAPITRE 11.8

Connexité

I Généralités

Définition I.1.

Soit (X, d) un espace métrique. Les propositions suivantes sont équivalentes

1. Si O_1 et O_2 sont deux ouverts de X tels que $X = O_1 \cup O_2$ et $O_1 \cap O_2 = \emptyset$, alors $O_1 = \emptyset$ ou $O_2 = \emptyset$.
2. Si F_1 et F_2 sont deux fermés de X tels que $X = F_1 \cup F_2$ et $F_1 \cap F_2 = \emptyset$, alors $F_1 = \emptyset$ ou $F_2 = \emptyset$.
3. Si A est une partie à la fois fermée et ouverte de X , alors $A = X$ ou $A = \emptyset$.
4. Si f est une fonction continue de X dans $\{0, 1\}$, alors f est constante.

Lorsque l'une de ces propriétés est vérifiée, on dit que X est connexe.

Preuve

- (1) ⇒ (2) Soit F_1 et F_2 deux fermés vérifiant $F_1 \cup F_2 = X$ et $F_1 \cap F_2 = \emptyset$, et posons $O_1 = X \setminus F_1$ et $O_2 = X \setminus F_2$. O_1 et O_2 sont ouverts et $O_1 \cup O_2 = X$ et $O_1 \cap O_2 = \emptyset$, donc $O_1 = X$ et $O_2 = \emptyset$ ou $O_1 = \emptyset$ et $O_2 = X$, i.e. $F_1 = X$ et $F_2 = \emptyset$ ou $F_1 = \emptyset$ et $F_2 = X$.
- (2) ⇒ (3) Soit A une partie fermée et ouverte de X . $F_1 = A$ et $F_2 = A^c$ vérifient les hypothèses de (2). Donc on a $A = X$ et $A^c = \emptyset$ ou $A = \emptyset$ et $A^c = X$, d'où le résultat voulu.
- (3) ⇒ (4) Posons $F_1 = f^{-1}(\{0\})$ et $F_2 = f^{-1}(\{1\})$. F_1 et F_2 sont fermés car il s'agit d'images réciproques de deux fermés par une fonction continue. De plus, on a $F_1 \cup F_2 = X$ et $F_1 \cap F_2 = \emptyset$. On a alors $F_1 = X$ ou $F_2 = X$, i.e. $f^{-1}(\{0\}) = X$ ou $f^{-1}(\{1\}) = X$. f est alors toujours égale à 0 ou toujours égale à 1. On a donc bien le résultat voulu.
- (4) ⇒ (1) Soit O_1 et O_2 deux ouverts vérifiant $O_1 \cup O_2 = X$ et $O_1 \cap O_2 = \emptyset$. On considère l'application de X dans $\{0, 1\}$ suivante :

$$f : \begin{cases} X & \longrightarrow \{0, 1\} \\ x & \longmapsto \begin{cases} 0 & \text{si } x \in O_1 \\ 1 & \text{si } x \in O_2 \end{cases} \end{cases}$$

f est continue car O_1 et O_2 sont ouverts, elle est donc constante. On a alors $O_1 = f^{-1}(\{0\}) = \emptyset$ et $O_2 = f^{-1}(\{1\}) = X$ ou $O_1 = f^{-1}(\{0\}) = X$ et $O_2 = f^{-1}(\{1\}) = \emptyset$, ce qui est bien ce qu'on cherchait.

Proposition I.2.

Soit I un ensemble et $(\Omega_i)_{i \in I}$ une partition d'ouverts d'un espace métrique connexe X . Il existe alors au plus un indice i_0 tel que $\Omega_{i_0} \neq \emptyset$.

Preuve : Soit i_0 tel que $\Omega_{i_0} \neq \emptyset$. Posons $\Omega = \bigcup_{i \in I \setminus \{i_0\}} \Omega_i$. On a alors $\Omega_{i_0} \cup \Omega = X$ et $\Omega_{i_0} \cap \Omega = \emptyset$. De plus Ω_{i_0} et Ω sont ouverts (car c'est l'union d'ouverts), donc X étant connexe, on a nécessairement $\Omega = \emptyset$, i.e. $\forall i \neq i_0, \Omega_i = \emptyset$.

Proposition I.3.

Si A est une partie connexe de l'espace métrique X alors \overline{A} aussi.

Preuve : Soit $f : \overline{A} \rightarrow \{0, 1\}$ une application continue. f est continue sur A par restriction et A est connexe, donc f est constante sur A . \overline{A} est dense dans A donc f étant continue, elle est aussi constante sur \overline{A} , donc \overline{A} est bien connexe.

Remarque : Attention, si A est connexe, \overline{A} ne l'est pas forcément !

Proposition I.4.

Soit X et Y deux espaces métriques et $f \in \mathcal{C}(X, Y)$. Si A est une partie connexe de X , alors $f(A)$ est aussi une partie connexe de Y .

Preuve : Soit $g : f(A) \rightarrow \{0, 1\}$ une application continue. $g \circ f$ est une fonction continue de A dans $\{0, 1\}$ car il s'agit de la composition de deux applications continues, elle est alors constante. On en déduit donc directement que $\exists c \in \{0, 1\}$, $g \circ f(A) = \{c\}$, i.e. $g(f(A)) = \{c\}$. g est alors constante sur $f(A)$ ce qui nous permet d'affirmer que $f(A)$ est bien une partie connexe de Y .

II Parties connexes par arc

Dans cette partie, on considère (E, d) un espace métrique.

Proposition II.1.

$[0, 1]$ est une partie connexe.

Preuve : Soit $f \in \mathcal{C}([0, 1], \{0, 1\})$. Supposons sans perte de généralité que $f(0) = 0$. On considère l'ensemble

$$A = \{x \in [0, 1], \forall y \in [0, x], f(y) = 0\}$$

Posons $a = \sup A$. a est limite d'une suite à valeurs dans A , donc par continuité de f , on a $f(a) = 0$. Supposons que $a \neq 1$. On a pour tout $n \in \mathbb{N}$, $\exists x_n \in [a, a + \frac{1}{n}]$, $f(x_n) = 1$. La suite (x_n) converge vers a et donc

$$f(x_n) \xrightarrow{n \rightarrow +\infty} 1 \neq f(a)$$

ce qui est absurde car f est continue.

Définition II.2.

1. On appelle arc continu toute application continue d'un segment $[a, b]$ de \mathbb{R} dans E .
2. Une partie A de E est dite connexe par arcs si tous éléments x et y de A peuvent être reliés par un arc continu sur A , i.e.

$$\forall (x, y) \in A^2, \exists \gamma \in \mathcal{C}([0, 1], A), \gamma(0) = x \text{ et } \gamma(1) = y$$

Remarque : Dans la définition de la connexité par arc, on aurait pu remplacer 0 par $a \in \mathbb{R}$ et 1 par $b \in \mathbb{R}$ tel que $a < b$ quelconques.

Définition II.3.

Soit $x, y, z \in E$, γ un arc continu reliant x et y et δ un arc continu reliant y et z . L'arc $\gamma \bullet \delta$ est défini par

$$\gamma \bullet \delta : \begin{cases} [0, 1] & \longrightarrow E \\ y & \longmapsto \begin{cases} \gamma(2t) & \text{si } t \in [0, \frac{1}{2}] \\ \delta(2t - 1) & \text{si } t \in [\frac{1}{2}, 1] \end{cases} \end{cases}$$

Par construction $\gamma \bullet \delta$ est un arc continu reliant x à z . On dit que $\gamma \bullet \delta$ est la reliure des deux arcs γ et δ . • n'étant pas associative, pour trois arcs $\gamma_1, \gamma_2, \gamma_3$, on définit $\gamma_1 \bullet \gamma_2 \bullet \gamma_3$ comme $\gamma_1 \bullet (\gamma_2 \bullet \gamma_3)$.

Définition II.4.

Supposons que pour tout $t \in [0, 1]$, $(1-t)a + tb \in E$. Pour tout $x, y \in E$, on définit l'arc $\theta(x, y)$ comme

$$\theta(x, y) : \begin{cases} [0, 1] & \longrightarrow E \\ t & \longmapsto (1-t)x + ty \end{cases}$$

Par construction, $\theta(x, y)$ est bien un arc continu reliant x à y .

Remarque : Attention, ces deux dernières notations sont propres à ce cours en particulier et ne sont pas communes en classes préparatoires. Si vous souhaitez les utiliser, il faut les définir avant.

Proposition II.5.

Soit F un espace métrique et f une fonction continue de E dans F . L'image d'une partie de E connexe par arcs par f est connexe par arcs.

Preuve : Soit A une partie connexe par arcs de E . Soit $a, b \in f(A)$, et $x, y \in A$ tels que $a = f(x)$ et $b = f(y)$. A est connexe par arcs, il existe donc un arc $\gamma \in \mathcal{C}([0, 1], A)$ tel que $\gamma(0) = x$ et $\gamma(1) = y$. On a alors $f \circ \gamma$ est un arc continu reliant $a = f(x)$ et $b = f(y)$.

Proposition II.6.

Une partie A de E connexe par arcs est connexe.

Preuve : Soit $g : A \longrightarrow \{0, 1\}$ une fonction continue. Soient x et y dans A . A est connexe par arcs, il existe donc un arc continu $\gamma \in \mathcal{C}([0, 1], A)$ tel que $\gamma(0) = x$ et $\gamma(1) = y$.

L'application $g \circ \gamma : [0, 1] \longrightarrow \{0, 1\}$ est continue et $[0, 1]$ est connexe, donc elle est constante et alors $g(x) = g(y)$. On en déduit donc que g est constante et que par conséquent A est connexe.

Exemple : Pour tout $n \in \mathbb{N}^*$, $GL_n(\mathbb{R})$ n'est pas connexe par arcs. En effet, l'application $f = \det$ est continue, donc si $GL_n(\mathbb{R})$ était connexe par arcs, $f(GL_n(\mathbb{R}))$ le serait aussi. Mais $f(GL_n(\mathbb{R})) = \mathbb{R}^*$ qui n'est pas connexe par arcs.

Proposition II.7.

Soit A une partie de E .

1. La relation sur A^2 définie par

$$\forall x, y \in A, x \sim_A y \iff \exists \gamma \in \mathcal{C}([0, 1], A), \gamma(0) = x \text{ et } \gamma(1) = y$$

est une relation d'équivalence.

2. Les classes d'équivalence pour \sim_A sont connexes par arcs. On appelle ces classes composantes connexes par arcs.

Lorsqu'il n'y a pas d'ambiguïté sur l'ensemble A , on note \sim au lieu de \sim_A .

Preuve

1. \rightarrow Réflexivité

Soit $x, y \in A$. Si $x \sim y$, alors il existe un arc $\gamma \in \mathcal{C}([0, 1], A)$ reliant x et y . Il suffit alors de considérer $\tilde{\gamma} : a \mapsto \gamma(1 - a)$. L'arc $\tilde{\gamma}$ relie x et y et $\tilde{\gamma}(0) = y$ et $\tilde{\gamma}(1) = x$ et alors $y \sim x$.

- \rightarrow Symétrie

Soit $x \in A$. L'arc $\gamma : t \mapsto x$ constant sur $[0, 1]$ relie x à x , donc $x \sim x$.

- \rightarrow Transitivité

Soit $x, y, z \in A$ tels que $x \sim y$ et $y \sim z$. Soit $\gamma, \delta \in \mathcal{C}([0, 1], A)$ deux arcs reliant respectivement x à y et y à z . On considère l'arc suivant

$$\beta = \gamma \bullet \delta : \begin{cases} [0, 1] & \longrightarrow A \\ x & \longmapsto \begin{cases} \gamma(2t) & \text{si } x \in \left[0, \frac{1}{2}\right] \\ \delta(2t - 1) & \text{si } x \in \left[\frac{1}{2}, 1\right] \end{cases} \end{cases}$$

β est continu et $\beta(0) = x$ et $\beta(1) = z$, donc $x \sim z$.

Proposition II.8.

1. Une réunion de parties de E connexes par arcs ayant un point en commun est connexe par arcs.
2. Soit $n \in \mathbb{N}^*$ et E_1, \dots, E_n des espaces métriques. Si pour tout $k \in \llbracket 1; n \rrbracket$, A_k est une partie connexe par arcs de E_k , alors $A_1 \times \dots \times A_n$ est une partie connexe par arcs de l'espace métrique produit $E_1 \times \dots \times E_n$.

Preuve

1. Soit $n \in \mathbb{N}^*$ et $(A_n)_{n \in \mathbb{N}}$ une famille de parties connexes par arcs tels que pour tout $k \in \llbracket 1; n \rrbracket$, $a \in A_k$. Posons $A = \bigcup_{n \in \mathbb{N}} A_n$. soit x et y deux points de A . Soit $k, l \in \mathbb{N}$ tels que $x \in A_k$ et $y \in A_l$. On a a et x sont deux éléments de l'ensemble connexe par arcs A_k , donc $x \sim_{A_k} a$ donc $x \sim_A a$ et a et y sont deux éléments de l'ensemble connexe par arcs A_l , donc $a \sim_{A_l} y$ donc $a \sim_A y$. On en déduit donc par transitivité que $x \sim y$ et que finalement A est connexe par arcs.
2. Soit $a = (a_1, \dots, a_n)$ et $b = (b_1, \dots, b_n)$ deux éléments de $E_1 \times \dots \times E_n$. Pour tout $k \in \llbracket 1; n \rrbracket$, il existe un arc γ_k reliant a_k et b_k . Considérons l'arc sur $E_1 \times \dots \times E_n$, $\gamma : t \mapsto (\gamma_1(t), \dots, \gamma_n(t))$. L'arc γ est continu et relie a et b , donc $A_1 \times \dots \times A_n$ est bien connexe par arcs.

Exercice II.9.

Soit Ω une union d'ouverts disjoints de \mathbb{R} . On écrit

$$\Omega = \bigcup_{n \in \mathbb{N}}]a_n, b_n[$$

avec pour tout $n \in \mathbb{N}$, $a_n < b_n$. Montrer que Ω n'est pas connexe par arcs.

Exercice II.10.

Soit $p \in \mathbb{N}^*$ et $z_1, \dots, z_p \in \mathbb{C}$. Montrer que $\mathbb{C} \setminus \{z_1, \dots, z_p\}$ est connexe par arcs.

Exercice II.11.

Soit $n \in \mathbb{N}^*$ et H un hyperplan de \mathbb{C}^n . Montrer que $\mathbb{C}^n \setminus H$ est connexe par arcs.

Exercice II.12.

Soit $n \in \mathbb{N}^*$ et H un hyperplan de \mathbb{R}^n . Montrer que $\mathbb{R}^n \setminus H$ n'est pas connexe par arcs.

Exercice II.13.

Soit Ω un ouvert connexe de \mathbb{R}^n . Montrer que Ω est connexe par arcs polygonaux, i.e. pour tous points x, y de E , x et y peuvent être reliés par un arc affine par morceaux.

III Application aux fonctions à variables réelles

Proposition III.1.

Soit A une partie de \mathbb{R} . Les propositions suivantes sont équivalentes.

1. A est connexe par arcs.
2. A est un intervalle.

Preuve

$\rightarrow (2) \Rightarrow (1)$ Pour tout $a, b \in A$ tel que $a < b$, si on considère l'application continue $f_{a,b} : x \mapsto (b-a)x + a$, alors $f_{a,b}$ est un arc continu reliant a à b donc $a \sim b$. A est donc connexe par arcs.

$\rightarrow (1) \Rightarrow (2)$ soit $x, y \in A$ et $z \in]x, y[$. Soit γ un arc continu reliant x et y . Posons

$$S_z = \{t \in [0, 1], \gamma(t) \leq z\} = \gamma^{-1}([x, z])$$

S_z est fermé car il s'agit de l'image réciproque d'un fermé par la fonction continue γ et de plus, S_z est non vide car $1 \in S_z$, donc $c = \sup S_z \in S_z$, i.e. $\gamma(c) \leq z$ et $c < 1$ car $1 \notin S_z$. On a aussi pour tout $t \in]0, 1 - c]$, $\gamma(c + t) > z$. En faisant tendre t vers 0, on obtient par continuité de γ que $\gamma(c) \geq z$, et alors $\gamma(c) = z$. On en déduit donc que $z \in A$, donc $[x, y] \subset A$ et finalement que A est un intervalle.

Conséquence : Si I est un intervalle et f une fonction continue de I dans \mathbb{R} , alors I est continu par arcs donc $f(I)$ aussi, i.e. $f(I)$ est un intervalle.

Proposition III.2.

Soit I un intervalle de \mathbb{R} et $f \in \mathcal{C}(I, \mathbb{R})$. Les propositions suivantes sont équivalentes.

1. f est injective.
2. f est strictement monotone.

Preuve

$\rightarrow (2) \Rightarrow (1)$ Supposons que f soit injective et donc dans perte de généralité strictement croissante.

Pour tout $x, y \in I$, si $x \neq y$, on suppose sans perte de généralité que $x > y$. Par stricte monotonie de f , on a que $f(x) > f(y)$ et alors $f(x) \neq f(y)$. f est donc bien injective.,

$\rightarrow (1) \Rightarrow (2)$ Posons $\Delta = \{(x, y) \in I^2, x < y\}$ et considérons l'application

$$\varphi : \begin{cases} \Delta & \longrightarrow \mathbb{R} \\ (x, y) & \mapsto f(y) - f(x) \end{cases}$$

Le fait que f soit injective est équivalent au fait que φ ne s'annule pas sur Δ , donc φ est à valeurs dans \mathbb{R}^* . Δ est convexe donc connexe par arcs. En effet, si a et b sont deux points de Δ , l'arc continu

$$\gamma : \begin{cases} [0, 1] & \longrightarrow \Delta \\ t & \mapsto ta + (1 - t)b \end{cases}$$

lie a et b dans Δ . Or φ est continue, $\varphi(\Delta)$ est alors une partie connexe par arcs de \mathbb{R}^* et donc un intervalle. Deux cas de présentent alors

- $\varphi(\Delta) \subset]0, +\infty[$ donc f est strictement croissante.
- $\varphi(\Delta) \subset]-\infty, 0[$ donc f est strictement décroissante.

On a donc bien le résultat voulu.

Proposition III.3.

Soit I un intervalle de \mathbb{R} et f une application de I dans \mathbb{R} .

1. Si f est monotone, alors les propositions suivantes sont équivalentes.
 - (a) f est continue.
 - (b) $f(I)$ est un intervalle.
2. Si f est continue et injective, alors $f^{-1} : f(I) \longrightarrow I$ est continue.

Preuve

1. Supposons que f est monotone.

$\rightarrow (a) \Rightarrow (b)$ I est connexe par arcs et f est continue, donc $f(I)$ est aussi connexe par arcs i.e. c'est un intervalle.

$\rightarrow (b) \Rightarrow (a)$ Supposons sans perte de généralité que f soit croissante. Nous allons traiter uniquement le cas où f admet un point de discontinuité sur l'intérieur de I . Le lecteur pourra essayer de faire le cas d'une discontinuité aux bords de l'intervalle. Supposons que f admette un point de discontinuité x_0 sur l'intérieur de I . On note respectivement $f(x_0^+)$ et $f(x_0^-)$ les limites à droite et à gauche de x_0 des f . On a alors $f(x_0^-) \leq f(x_0) \leq f(x_0^+)$ et $f(x_0^-) < f(x_0^+)$. Soit $y_0 \in]f(x_0^-), f(x_0^+)[\setminus \{f(x_0)\} := A_0$. On a pour tout $t \in I$,

- Si $t < x_0$, alors $f(t) \leq f(x_0^-)$ et donc $f(t) \neq y_0$
- Si $t = x_0$, alors $f(t) = f(x_0) \neq y_0$

- Si $t > x_0$, alors $f(t) \geq f(x_0^+)$, donc $f(t) \neq y_0$.

On en déduit que $y_0 \notin f(I)$ et y_0 est compris entre deux éléments de $f(I)$. $f(I)$ n'est donc pas un intervalle.

- Il suffit d'appliquer la question précédente et la proposition III.2. f est une fonction continue sur l'intervalle I et injective, elle est donc strictement monotone d'après la proposition III.2. f^{-1} est alors aussi strictement monotone. De plus, on a $f^{-1}(f(I)) = I$ et I et $f(I)$ sont des intervalles, donc d'après (1), f^{-1} est continue.

Exercice III.4.

Soit f une fonction de $[0, 1]$ dans $[0, 1]$ telle qu'il existe $p \in \mathbb{N}^*$, $\underbrace{f \circ \cdots \circ f}_{p \text{ fois}} = Id$. Supposons que $f(0) = 0$. Montrer que $f = Id$.

Exercice III.5.

Soit $f \in \mathcal{C}^1([0, 1], \mathbb{R})$ telle que $f \times (1 - f') = 0$. Déterminer f .

Exercice III.6.

Montrer que \mathbb{R} et \mathbb{R}^2 ne sont pas homéomorphes.

Exercice III.7.

Posons $S(0, 1) = \{z \in \mathbb{C}, |z| = 1\}$. Montrer que $S(0, 1)$ n'est homéomorphe à aucune partie \mathbb{R} .

Exercice III.8.

Soit $f : S(0, 1) \rightarrow S(0, 1)$ une fonction injective et continue. Montrer que f est un homéomorphisme.

Correction de l'exercice II.9. :

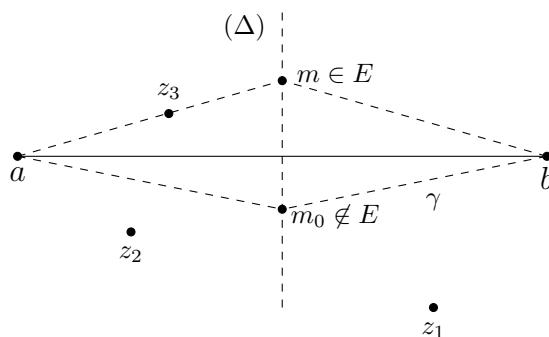
Méthode 1 : Soit $n, m \in \mathbb{N}$ deux entiers naturels différents, $x \in]a_n, b_n[$ et $y \in]a_m, b_m[$. Supposons par l'absurde que Ω soit connexe par arcs. Il existe un arc γ liant x et y . On suppose sans perte de généralité que $b_n \leq a_m$. On a $\gamma(0) = x < b_n < y = \gamma(1)$ et γ est continue. Par le théorème des valeurs intermédiaires, il existe $c \in]0, 1[$, $\gamma(c) = b_n$, mais $b_n \notin \Omega$ ce qui est absurde car γ est à valeurs dans Ω par hypothèse.

Méthode 2 (plus simple) : En posant pour tout $k \in \mathbb{N}$, $A_k =]a_k, b_k[$, on peut partitionner Ω en deux ouverts, par exemple $O_1 = A_0$ et $O_2 = \bigcup_{k \geq 1} A_k$. On a $O_1 \cup O_2 = \Omega$, $O_1 \cap O_2 = \emptyset$, $O_1 \neq \emptyset$ et $O_2 \neq \emptyset$. Ω n'est donc pas connexe et alors pas connexe par arcs.

Correction de l'exercice II.10. :

Soit $a, b \in S = \mathbb{C} \setminus \{z_1, \dots, z_p\}$. Considérons les deux ensembles suivants :

- $\Delta = \{x \in \mathbb{C}, |x - a| = |x - b|\}$ la médiatrice du segment $[a, b]$.
- $E = \{m \in \Delta, \exists k \in \llbracket 1; p \rrbracket, z_k \in [a, m] \cup [b, m]\}$.



$|E| \leq p$, donc E est fini. On peut donc considérer $m_0 \in \Delta \setminus E$ car cet ensemble est non vide. Il suffit alors de considérer l'arc

$$\gamma = \theta(a, m_0) \bullet \theta(m_0, b) : \begin{cases} [0, 1] & \longrightarrow S \\ t & \longmapsto \begin{cases} 2tm_0 + (1 - 2t)a & \text{si } t \in \left[0, \frac{1}{2}\right] \\ (2t - 1)b + 2(1 - t)m_0 & \text{si } t \in \left[\frac{1}{2}, 1\right] \end{cases} \end{cases}$$

γ est un arc continu à valeurs dans S qui lie a à b en passant par m_0 , donc S est bien connexe par arcs.

Correction de l'exercice II.11. :

Soit H un hyperplan de \mathbb{C}^n et φ une forme linéaire non nulle telle que $\text{Ker } \varphi = H$. Posons $S = \mathbb{C}^n \setminus H$ et montrons que S est connexe par arcs. Soit $a, b \in S$

- Si $\varphi(a) = \varphi(b)$, alors pour tout $\lambda \in [0, 1]$, $\varphi((1 - \lambda)a + \lambda b) = \varphi(a) \neq 0$. Il suffit alors de considérer l'arc $\gamma = \theta(a, b) : t \longmapsto (1 - t)a + tb$. Cet arc est bien à valeurs dans S et lie a et b .
- Si $\varphi(a) \neq \varphi(b)$, alors on considère $K_{a,b} = \{\lambda \in \mathbb{C}, \varphi((1 - \lambda)a + \lambda b) = 0\}$.
 $\varphi((1 - \lambda)a + \lambda b) = 0 \iff \lambda = \frac{\varphi(a)}{\varphi(b) - \varphi(a)} := \lambda_{a,b}$, donc on a $K_{a,b} = \{\lambda_{a,b}\}$.

D'après l'exercice précédent, on dispose d'un arc γ liant a et b dans $\mathbb{C} \setminus \{\lambda_{a,b}\}$. Considérons Γ l'arc défini par

$$\Gamma : \begin{cases} [0, 1] & \longrightarrow S \\ t & \longmapsto (1 - \gamma(t))a + \gamma(t)b \end{cases}$$

Γ est bien à valeurs dans S car pour tout t , $\Gamma(t) \in H$ impliquerait que $\gamma(t) = \lambda_{a,b}$ ce qui est impossible. Γ lie a à b dans S , S est donc bien connexe par arcs.

Correction de l'exercice II.12. :

Soit H un hyperplan de \mathbb{R}^n et φ une forme linéaire non nulle telle que $\text{Ker } \varphi = H$. Considérons les deux ensembles $A_+ = \{x \in \mathbb{R}^n, \varphi(x) > 0\}$ et $A_- = \{x \in \mathbb{R}^n, \varphi(x) < 0\}$. On a $\mathbb{R}^n \setminus H = A_+ \cup A_-$. Soit $x \in A_+$ et $y \in A_-$. Supposons par l'absurde qu'il existe un arc γ liant x et y . L'application $\varphi \circ \gamma$ est continue et $\varphi \circ \gamma(0) = \varphi(x) > 0 > \varphi(y) = \varphi \circ \gamma(1)$, donc d'après le théorème des valeurs intermédiaires, il existe $c \in]0, 1[$, $\varphi \circ \gamma(c) = 0$, i.e. $\gamma(c) \in H$ ce qui est absurde. On en déduit donc que $\mathbb{R}^n \setminus H$ n'est pas connexe par arcs.

Méthode 2 (plus simple) : A_+ et A_- sont deux ouverts disjoints non vides dont l'union fait $\mathbb{R}^n \setminus H$, $\mathbb{R}^n \setminus H$ n'est alors pas connexe donc pas connexe par arcs.

Correction de l'exercice II.13. :

Soit $a \in \Omega$. Considérons A la composante connexe par arcs polygonaux de a dans Ω . Montrer que Ω est connexe par arcs polygonaux revient à montrer que $A = \Omega$. Ω étant connexe par arcs donc connexe, une idée serait de montrer que A est ouvert et fermé dans Ω .

→ Montrons que A est ouvert.

Soit $x \in A$. Il existe un arc polygonal γ reliant a et x . Ω étant ouvert, il existe $\varepsilon > 0$ tel que $B(x, \varepsilon) \subset \Omega$. soit $y \in B(x, \varepsilon)$. $B(x, \varepsilon)$ est convexe, $\theta(x, y)$ est donc un arc continu polygonal (c'est un segment) reliant x à y dans $B(x, \varepsilon)$ donc dans Ω . On en déduit donc que $\gamma \bullet \theta(x, y)$ est un arc polygonal qui relie a à y dans Ω , donc $y \in A$ et alors $B(x, \varepsilon) \subset A$. A est donc ouvert.

→ Montrons que $\Omega \setminus A$ est aussi ouvert.

Soit $b \in \Omega \setminus A$ et B la composante connexe par arcs de b . Par le raisonnement précédent, B est ouvert et contient b , c'est donc un voisinage de b inclus dans $\Omega \setminus A$. $\Omega \setminus A$ est donc ouvert. Ω est connexe et A est ouvert et fermé dans Ω , ce qui nous permet d'affirmer finalement que $A = \Omega$.

Correction de l'exercice III.4. :

Soit $p \in \mathbb{N}^*$ tel que $\underbrace{f \circ \dots \circ f}_{p \text{ fois}} = Id$. Cette inégalité nous permet de dire que f est bijective sur un

intervalle et alors par la proposition III.2., f est strictement monotone. $f(0) = 0$, donc f est strictement croissante. Supposons par l'absurde qu'il existe $x \in [0, 1]$ tel que $f(x) < x$, on a alors

$$x > f(x) > f \circ f(x) > \dots > \underbrace{f \circ \dots \circ f}_{p \text{ fois}}(x) = x$$

ce qui est absurde. De même, on obtient la même contradiction lorsqu'on suppose que $f(x) > x$. Donc a bien que $f = Id$.

Correction de l'exercice III.5. :

Supposons que $f \neq 0$ et posons $A = \{x \in [0, 1], f'(x) = 1\}$. Montrons que A est fermé et ouvert dans $[0, 1]$ et est donc égal à $[0, 1]$ par connexité de $[0, 1]$.

→ A est fermé car c'est l'image réciproque du fermé $\{1\}$ par l'application continue f' .

→ Montrons que A est ouvert. Soit $a \in A$.

- Si $f(a) \neq 0$, alors par continuité de f , il existe un voisinage U de a où f est non nulle, et alors l'égalité $f \times (f' - 1) = 0$ entraîne que $f' = 1$ sur U , i.e. $U \subset A$.
- Si $f(a) = 0$, alors on a

$$f(a + h) = f'(a)h + o(h) = h \underbrace{(1 + o(1))}_{\varepsilon(h)}$$

$\varepsilon(h) \xrightarrow[h \rightarrow 0]{} 1$, donc il existe $\eta > 0$ tel que pour tout $h \in B_f(0, \eta) \setminus \{0\}$, $|\varepsilon(h)| > \frac{1}{2}$ et alors pour tout $h \in B_f(0, \eta) \setminus \{0\}$, $f(a + h) > \frac{h}{2} > 0$ et alors l'égalité $f \times (f' - 1) = 0$ entraîne

$f'(a+h) = 1$. On en déduit donc que $[a-h, a+h] \subset A$, donc A est bien ouvert et finalement $A = [0, 1]$.

Finalement on déduit de ce qui précède que les fonctions $f \in \mathcal{C}^1([0, 1], \mathbb{R})$ vérifiant $f \times (f' - 1) = 0$ sont la fonction nulle et les fonctions de la forme $f : x \mapsto x + C$ avec $C \in \mathbb{R}$.

Correction de l'exercice III.6. :

Supposons par l'absurde que \mathbb{R} et \mathbb{R}^2 sont homéomorphes. Il existe alors une fonction f bijective continue de \mathbb{R} dans \mathbb{R}^2 d'inverse continu. $\mathbb{R}^2 \setminus \{f(0)\}$ est connexe par arcs, f^{-1} est continue donc $f^{-1}(\mathbb{R}^2 \setminus \{f(0)\})$ est connexe par arcs d'après la proposition II.5 mais $f^{-1}(\mathbb{R}^2 \setminus \{f(0)\}) = \mathbb{R}^*$ et \mathbb{R}^* n'est pas connexe par arcs, ce qui est absurde.

Correction de l'exercice III.7. :

Soit A une partie de \mathbb{R} . Supposons que A est homéomorphe à $S(0, 1)$, i.e. il existe un homéomorphisme $f : S(0, 1) \rightarrow A$. $S(0, 1)$ est connexe par arcs, donc $A = f(S(0, 1))$ est compact (c'est l'image d'un compact par une application continue) connexe par arcs, i.e. c'est un intervalle fermé, on pose alors $A = [a, b]$ avec $a < b$. Soit $c = \frac{a+b}{2}$ et $B = S(0, 1) \setminus \{f^{-1}(c)\}$. B est connexe par arcs et f est continue, donc $f(B)$ est connexe par arcs. Mais $f(B) = A \setminus \{c\}$ et $A \setminus \{c\}$ n'est pas connexe par arcs ce qui est absurde.

Correction de l'exercice III.8. :

- Si f est surjective, alors elle est bijective. Montrons que c'est bien un homéomorphisme. Pour tout fermé F de $S(0, 1)$, $(f^{-1})^{-1}(F) = f(F)$ qui est fermé d'après le corollaire VI.2 du chapitre 11.5. On a montré que l'image réciproque de tout fermé de $S(0, 1)$ par f^{-1} est fermé, donc f^{-1} est continue et finalement f est une homéomorphisme.
- Si f n'est pas surjective, alors posons $f(S(0, 1)) = S' \subset S(0, 1)$. Quitte à composer par une rotation, on suppose que $-1 \notin f(S(0, 1))$. Considérons l'application

$$\text{Arg} : \begin{cases} S' & \longrightarrow]-\pi, \pi[\\ x + iy & \longmapsto 2 \arctan \left(\frac{y}{x+1} \right) \end{cases}$$

Soit $x + iy \in S'$. Posons $\theta = \text{Arg}(x + iy)$. On a

$$\begin{aligned} \cos(\theta) &= \frac{1 - \tan\left(\frac{\theta}{2}\right)^2}{1 + \tan\left(\frac{\theta}{2}\right)^2} = \frac{1 - \left(\frac{y}{x+1}\right)^2}{1 + \left(\frac{y}{x+1}\right)^2} \\ &= \frac{x^2 + 2x + 1 - y^2}{x^2 + 2x + 1 + y^2} = \frac{2x^2 + 2x}{2x + 2} \\ &= \frac{2x(x+1)}{2(x+1)} = x \end{aligned}$$

On peut montrer de la même manière que $\sin(\theta) = y$, donc pour tout $z = x + iy$ et $z' = x' + iy'$ dans $S(0, 1)$, $\text{Arg}(z) = \text{Arg}(z')$ donne en composant par cos et sin que $x = x'$ et $y = y'$, i.e. $z = z'$. Donc Arg est bien injective.

Soit $g = \text{Arg} \circ f$. g est une injection continue de $S(0, 1)$ dans \mathbb{R} et $S(0, 1)$ est connexe par arcs, donc il existe $a, b \in \mathbb{R}$ tels que $a < b$ et $g(S(0, 1)) = [a, b]$ (c'est un intervalle fermé car il s'agit de l'image d'un compact par une application continue, i.e. un compact). g est donc une bijection continue de $S(0, 1)$ dans $[a, b]$ qui sont deux compacts, donc par un raisonnement similaire au début de l'exercice, g est un homéomorphisme. On a montré que $S(0, 1)$ est homéomorphe à un segment de \mathbb{R} ce qui est impossible d'après l'exercice précédent. On en déduit donc que f est bijective et que finalement que f est un homéomorphisme en se ramenant au premier cas.



Convexité

I Enveloppe convexe

Dans ce chapitre, on considère E un \mathbb{R} -espace vectoriel et A une partie de E .

Définition I.1.

Posons $P_A = \{C \in \mathcal{P}(E), A \subset C \text{ et } C \text{ est convexe}\}$. L'enveloppe convexe de A est définie par

$$\text{conv}(A) = \bigcap_{C \in P_A} C$$

Lemme I.2.

Soit C une partie convexe de E . On a

$$\forall p \in \mathbb{N}^*, \forall (z_1, \dots, z_p) \in C^p, \forall (\lambda_1, \dots, \lambda_p) \in \mathbb{R}^{+p}, \lambda_1 + \dots + \lambda_p = 1 \implies \sum_{k=1}^p \lambda_k z_k \in C$$

Preuve : Montrons la propriété par récurrence sur p .

- Le cas $p = 1$ est évident et le cas $p = 2$ correspond à la définition de la convexité.
- Soit $p \in \mathbb{N}^*$, supposons que la propriété soit vraie pour p . Soit $z_1, \dots, z_{p+1} \in C$ et $\lambda_1, \dots, \lambda_{p+1} \in \mathbb{R}^+$ tels que $\lambda_1 + \dots + \lambda_{p+1} = 1$. On a lorsque $\lambda_{p+1} \neq 1$,

$$\sum_{k=1}^{p+1} \lambda_k z_k = (1 - \lambda_{p+1}) \sum_{k=1}^p \underbrace{\frac{\lambda_k}{1 - \lambda_{p+1}} z_k}_{\mu_k} + \lambda_{p+1} z_{p+1}$$

De plus

$$\mu_1 + \dots + \mu_p = \frac{\lambda_1 + \dots + \lambda_p}{1 - \lambda_{p+1}} = \frac{1 - \lambda_{p+1}}{1 - \lambda_{p+1}} = 1$$

Donc par hypothèse de récurrence, on a $\sum_{k=1}^p \mu_k z_k \in C$, et alors en appliquant la définition de la convexité (i.e. la propriété pour $p = 2$), on a

$$\sum_{k=1}^{p+1} \lambda_k z_k = (1 - \lambda_{p+1}) \underbrace{\sum_{k=1}^p \frac{\lambda_k}{1 - \lambda_{p+1}} z_k}_{\in C} + \lambda_{p+1} \underbrace{z_{p+1}}_{\in C} \in C$$

On a donc bien le résultat voulu. Il reste le cas $\lambda_{p+1} = 1$ qui est évident.

Proposition I.3.

1. L'intersection de deux ensembles convexes est convexe.
2. $\text{conv}(A)$ est le plus petit convexe contenant A .

3. $\text{conv}(A) = \left\{ x \in E, \exists p \in \mathbb{N}^*, \exists x_1, \dots, x_p \in A, \exists \lambda_1, \dots, \lambda_p \in \mathbb{R}^+, \begin{array}{l} \lambda_1 + \dots + \lambda_p = 1 \\ x = \sum_{k=1}^p \lambda_k x_k \end{array} \right\}$

Preuve

1. Cette preuve est laissée comme exercice au lecteur.
2. Par définition de $\text{conv}(A)$, tout convexe contenant A contient $\text{conv}(A)$, $\text{conv}(A)$ est alors le plus petit contenant A .
3. Montrons l'égalité par double inclusion

$\rightarrow (\supseteq)$ $A \subset \text{conv}(A)$ et $\text{conv}(A)$ est convexe, donc pour tout $x_1, \dots, x_p \in A \subset \text{conv}(A)$ et $\lambda_1, \dots, \lambda_p \in \mathbb{R}^+$ tels que $\lambda_1 + \dots + \lambda_p = 1$, $\sum_{k=1}^p \lambda_k x_k \in \text{conv}(A)$.

$\rightarrow (\subseteq)$ Posons $B = \left\{ x \in E, \exists p \in \mathbb{N}^*, \exists x_1, \dots, x_p \in A, \exists \lambda_1, \dots, \lambda_p \in \mathbb{R}^+, \begin{array}{l} \lambda_1 + \dots + \lambda_p = 1 \\ x = \sum_{k=1}^p \lambda_k x_k \end{array} \right\}$.

On a $A \subset B \subset \text{conv}(A)$, donc il suffit de montrer que B est convexe pour montrer l'égalité, car $\text{conv}(A)$ est le plus petit convexe au sens de l'inclusion contenant A .

Soit $x = \sum_{k=1}^p \lambda_k x_k \in B$, $y = \sum_{k=1}^p \mu_k y_k \in B$ et $\lambda \in [0, 1]$. On a

$$\lambda x + (1 - \lambda)y = \sum_{k=1}^p \lambda \lambda_k x_k + (1 - \lambda) \mu_k y_k$$

Posons

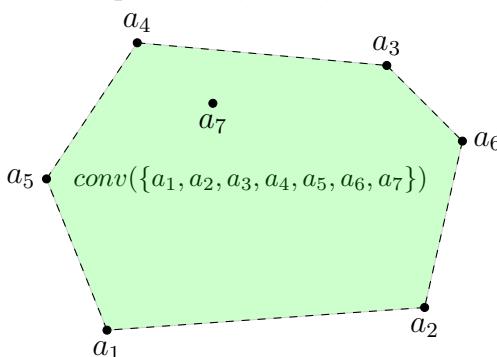
$$\begin{cases} (z_1, \dots, z_{2p}) = (x_1, \dots, x_p, y_1, \dots, y_p) \\ (\delta_1, \dots, \delta_{2p}) = (\lambda \lambda_1, \dots, \lambda \lambda_p, (1 - \lambda) \mu_1, \dots, (1 - \lambda) \mu_p) \end{cases}$$

On a $(z_1, \dots, z_{2p}) \in A^{2p}$, $(\delta_1, \dots, \delta_{2p}) \in \mathbb{R}^{+2p}$ et $\delta_1 + \dots + \delta_{2p} = 1$, donc on a

$$\lambda x + (1 - \lambda)y = \sum_{k=1}^{2p} \delta_k z_k \in C$$

Donc B est bien convexe, ce qui nous permet d'affirmer que $\text{conv}(A) = B$.

Exemple : On considère l'exemple suivant, où $\dim E = 2$. Le dessin suivant montre comment obtenir graphiquement l'enveloppe convexe des 7 points $a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in E$.



Exercice I.4.

Supposons que E est de dimension finie égale à d . Soit $p \geq d+1$ et $(a_0, \dots, a_p) \in E^{p+1}$. Montrer qu'il existe $(\alpha_0, \dots, \alpha_p) \in \mathbb{R}^{p+1} \setminus \{(0, \dots, 0)\}$ tel que

$$\sum_{k=0}^p \alpha_k a_k = 0 \text{ et } \alpha_0 + \dots + \alpha_p = 0$$

Exercice I.5.

Le résultat de cet exercice est connu sous le nom de théorème de Carathéodory.

Supposons que E soit de dimension finie égale à d . Soit $p \geq d+1$, $(a_0, \dots, a_p) \in E^{p+1}$, $(\lambda_0, \dots, \lambda_p) \in \mathbb{R}^{p+1}$ tel que $\lambda_0 + \dots + \lambda_p = 1$. Posons $b = \sum_{k=0}^p \lambda_k a_k$. Montrer qu'il existe $j \in \llbracket 0; p \rrbracket$ tel que

$$\exists (\mu_0, \dots, \mu_{j-1}, \mu_{j+1}, \dots, \mu_p) \in \mathbb{R}^{+p}, \quad \sum_{k=0, k \neq j}^p \mu_k = 1 \text{ et } \sum_{k=0, k \neq j}^p \mu_k a_k = b$$

Exercice I.6.

On suppose que E est de dimension finie. Soit K une partie compacte de E . Montrer que $\text{conv}(K)$ est une partie compacte de E .

II Projection et séparation

Exercice II.1.

Soit C un convexe non vide fermé de l'espace euclidien E muni du produit scalaire $\langle ., . \rangle$.

- Montrer que pour tout $a \in E$ il existe un unique $b \in C$ tel que

$$d(a, C) = \|a - b\|$$

- Montrer que $\forall x \in C$, $\langle a - b, x - b \rangle \leq 0$.
- On pose $b = p_C(a)$. Montrer que p_C est 1-lipschitzienne.

Exercice II.2.

Soit C un convexe non vide fermé de l'espace euclidien E muni du produit scalaire $\langle ., . \rangle$. Soit $a \notin C$. Montrer qu'il existe un hyperplan affine de E qui sépare strictement C de a .

Correction de l'exercice I.4. :

Posons pour tout $k \in \llbracket 1; p \rrbracket$, $x_k = a_k - a_0$. La famille (x_1, \dots, x_p) est liée car le nombre de vecteurs de cette famille est supérieur à la dimension de E . Il existe donc $(\beta_1, \dots, \beta_p) \in \mathbb{R}^p \setminus \{(0, \dots, 0)\}$ tel que

$$\sum_{k=1}^p \beta_k x_k = 0$$

i.e.

$$-\left(\sum_{k=1}^p \beta_k\right)a_0 + \beta_1 a_1 + \cdots + \beta_p a_p = 0$$

En posant $\alpha_0 = -\left(\sum_{k=1}^p \beta_k\right)$ et pour tout $k \in \llbracket 1; p \rrbracket$, $\alpha_k = \beta_k$, on a

$$\alpha_0 + \cdots + \alpha_p = 0 \text{ et } \sum_{k=0}^p \alpha_k a_k = 0$$

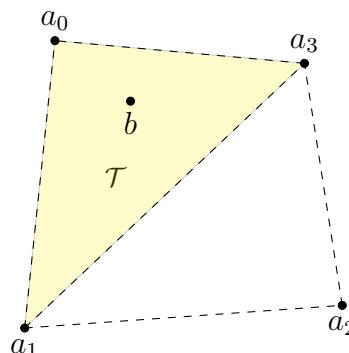
D'où le résultat voulu.

Correction de l'exercice I.5. : (Théorème de Carathéodory)

Remarquons qu'une autre manière de formuler ce théorème est la suivante :

Soit $p \geq d + 1$, $b \in E$ et $a_0, \dots, a_p \in E$ tel que $b \in \text{conv}(\{a_0, \dots, a_p\})$. Il existe alors $j \in \llbracket 0; p \rrbracket$ tel que $b \in \text{conv}(\{a_0, \dots, a_{j-1}, a_{j+1}, \dots, a_p\})$.

Pour avoir une intuition du résultat, observons le dessin suivant.



Dans le dessin ci-dessus, on regarde le cas $d = 2$ et $p = 3 \geq d + 1$. b appartient au quadrilatère $a_1 a_2 a_3 a_0$, i.e. $b \in \text{conv}(\{a_0, a_1, a_2, a_3\})$. Il existe donc $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}^+$ tels que

$$\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = 1 \text{ et } b = \lambda_0 a_0 + \lambda_1 a_1 + \lambda_2 a_2 + \lambda_3 a_3$$

Mais on voit aussi que b appartient au triangle jaune $\mathcal{T} = \text{conv}(\{a_0, a_1, a_3\})$, il existe donc μ_0, μ_1, μ_3 tels que

$$\mu_0 + \mu_1 + \mu_3 = 1 \text{ et } b = \mu_0 a_0 + \mu_1 a_1 + \mu_3 a_3$$

Remarquons que le point qu'on peut enlever à la combinaison convexe n'est pas unique : on aurait pu faire la même chose enlevant le point a_1 et en considérant le triangle $\mathcal{T}' = \text{conv}(\{a_0, a_3, a_2\})$.

Montrons à présent cette propriété dans le cas général.

On considère $\alpha_0, \dots, \alpha_p$ $p + 1$ réels vérifiant la propriété montrée dans l'exercice précédent, i.e.

$$\alpha_0 + \cdots + \alpha_p = 0 \text{ et } \sum_{k=0}^p \alpha_k a_k = 0$$

Posons pour tout $k \in \llbracket 0; p \rrbracket$ et $\tau \in \mathbb{R}$, $\nu_k(\tau) = \lambda_k - \tau \alpha_k$. On a alors pour tout $\tau \in \mathbb{R}$

$$\sum_{k=0}^p \nu_k(\tau) a_k = \sum_{k=0}^p \lambda_k a_k - \tau \sum_{k=0}^p \alpha_k a_k = \sum_{k=0}^p \lambda_k a_k = b$$

et

$$\sum_{k=0}^p \nu_k(\tau) = \sum_{k=0}^p \lambda_k - \tau \sum_{k=0}^p \alpha_k = 1$$

On souhaite choisir τ de manière à ce que tous les $\nu_k(\tau)$ soient positifs et que au moins un seul parmi ces coefficients soit nul. Posons pour tout $k \in \llbracket 0; p \rrbracket$, $A_k = \{\tau \in \mathbb{R}, \nu_k(\tau) \geq 0\}$. Les A_k sont fermés et non vides car ils contiennent tous 0.

On a alors pour tout $k \in \llbracket 0; p \rrbracket$

- Si $\alpha_k > 0$, alors $A_k = \left] -\infty, -\frac{\lambda_k}{\alpha_k} \right]$.
- Si $\alpha_k = 0$, alors $A_k = \mathbb{R}$.
- Sinon, $A_k = \left[-\frac{\lambda_k}{\alpha_k}, +\infty \right[$.

Posons $S = \bigcap_{k=0}^p A_k$. On sait que $(\alpha_0, \dots, \alpha_p) \neq (0, \dots, 0)$ et $\sum_{k=0}^p \alpha_k = 0$, il existe donc k et l deux entiers

dans $\llbracket 0; p \rrbracket$ tels que $\alpha_k < 0$ et $\alpha_l > 0$. On peut donc affirmer que $S \subset \left] -\infty, -\frac{\lambda_l}{\alpha_l} \right]$ et $S \subset \left[-\frac{\lambda_k}{\alpha_k}, +\infty \right[$. S est donc une intersection d'intervalles majorée et minorée et contenant 0, c'est alors un segment borné non vide. S est une intersection finie de segments de la forme $\left[-\frac{\lambda_k}{\alpha_k}, +\infty \right[$ et $\left] -\infty, -\frac{\lambda_l}{\alpha_l} \right]$ avec $\alpha_l < 0$ et $\alpha_k > 0$, il y a donc au moins un $j \in \llbracket 0; p \rrbracket$ tel que $-\frac{\lambda_j}{\alpha_j} \in S$. Posons $\tau_0 = -\frac{\lambda_j}{\alpha_j}$.

On a alors pour tout $k \in \llbracket 0; p \rrbracket$, $\nu_k(\tau_0) \geq 0$ et $\nu_j(\tau_0) = 0$. On a donc finalement en posant pour tout $k \in \llbracket 0; p \rrbracket$, $\mu_k = \nu_k(\tau_0)$,

$$\sum_{k=0, k \neq j}^p \mu_k a_k = b \text{ et } \sum_{k=0, k \neq j}^p \underbrace{\mu_k}_{\geq 0} = 1$$

Ce qui est bien le résultat recherché.

Une conséquence de ce théorème est la suivante : Soit $p \geq d+1$, $b \in E$ et $a_0, \dots, a_p \in E$ tel que $b \in \text{conv}(\{a_0, \dots, a_p\})$. Il existe alors $S \subset \llbracket 0; p \rrbracket$ tel que $|S| = d+1$ vérifiant $b \in \text{conv}(\{a_k, k \in S\})$. Ce résultat est facilement prouvable en enlevant de la combinaison convexe des points jusqu'à ce que la condition $p \geq d+1$ ne soit plus vérifiée. Ceci entraîne que si A est une partie de E , alors tout élément de $\text{conv}(A)$ peut s'écrire comme combinaison convexe d'au plus $d+1$ éléments de A .

Correction de l'exercice I.6. :

Posons $d = \dim E$ et considérons l'ensemble

$$\Lambda = \{(\lambda_0, \dots, \lambda_d) \in \mathbb{R}_+^{d+1}, \lambda_0 + \dots + \lambda_d = 1\}$$

et considérons l'application

$$\varphi : \begin{cases} K^{d+1} \times \Lambda & \longrightarrow \text{conv}(K) \\ ((a_k)_{k \in \llbracket 0; d \rrbracket}, (\lambda_k)_{k \in \llbracket 0; d \rrbracket}) & \longmapsto \sum_{k=0}^p \lambda_k a_k \end{cases}$$

Le résultat énoncé à la fin de l'exercice précédent nous permet d'affirmer que tout élément de $\text{conv}(K)$ s'écrit comme combinaison linéaire d'au plus $d+1$ éléments de K , i.e. s'écrit de la forme $\varphi((a_k)_{k \in \llbracket 0; d \rrbracket}, (\lambda_k)_{k \in \llbracket 0; d \rrbracket})$ avec $((a_k)_{k \in \llbracket 0; d \rrbracket}, (\lambda_k)_{k \in \llbracket 0; d \rrbracket}) \in K^{d+1} \times \Lambda$. φ est donc surjective. De plus Λ est un fermé borné en dimension finie, c'est donc un compact. $K^{d+1} \times \Lambda$ est un produit de compacts, donc d'après la proposition III.1 du chapitre 11.5, c'est un compact. φ est continue car il s'agit de produit et somme de fonctions continues, donc d'après la proposition VI.1 du chapitre 11.5, $\varphi(K^{d+1} \times \Lambda)$ est compact, mais φ est surjective, donc

$\varphi(K^{d+1} \times \Lambda) = \text{conv}(K)$. On en déduit donc finalement que $\text{conv}(K)$ est compact.

Correction de l'exercice II.1. : (Projection sur un convexe fermé)

1. Soit $a \in E$.

→ Existence

Posons $\delta = \inf_{x \in C} \|x - a\| = d(a, C)$ et soit (x_n) une suite à valeurs dans C vérifiant $\|x_n - a\| \xrightarrow[n \rightarrow +\infty]{} \delta$. Pour n assez grand, $\|x_n - a\| \leq \delta + 1$, i.e. $x_n \in B_f(a, \delta + 1)$. Quitte à extraire, on suppose que (x_n) est à valeurs dans $C \cap B_f(a, \delta + 1)$. $C \cap B_f(a, \delta + 1)$ est un fermé borné en dimension finie, c'est donc un compact. Il existe donc une extractrice φ telle que $x_{\varphi(n)} \xrightarrow[n \rightarrow +\infty]{} b \in C$. On a donc $\|x_{\varphi(n)} - a\| \xrightarrow[n \rightarrow +\infty]{} \|b - a\|$ et finalement $\|b - a\| = \delta = d(a, C)$.

→ Unicité

Soit b et b' deux éléments de C tels que $\|a - b\| = \|a - b'\| = d(a, C)$. Supposons par l'absurde que $b \neq b'$. On a

$$\begin{aligned} 2d(a, C)^2 &= \underbrace{\|a - b\|^2}_u + \underbrace{\|a - b'\|^2}_v = 2 \left(\left\| \frac{u+v}{2} \right\|^2 + \left\| \frac{u-v}{2} \right\|^2 \right) \\ &= 2 \left\| a - \frac{b+b'}{2} \right\|^2 + \frac{1}{2} \|b - b'\|^2 > 2d(a, C)^2 \end{aligned}$$

Ce qui est absurde, donc $b = b'$. On a donc bien l'unicité. La dernière inégalité est vraie car $\frac{b+b'}{2} \in C$.

2. Posons pour tout $t \in]0, 1]$ et $x \in C$, $x_t = tx + (1-t)b$. On a alors pour tout $x \in C$ et $t \in]0, 1]$, $x_t \in C$, donc $\|a - x_t\|^2 \geq \|a - b\|^2$. On a de plus

$$\begin{aligned} \|a - x_t\|^2 \geq \|a - b\|^2 &\iff \|t(a - x) + (1-t)(a - b)\|^2 \geq \|a - b\|^2 \\ &\iff t^2 \|a - x\|^2 + (t^2 - 2t + 1) \|a - b\|^2 + 2t(1-t) \langle a - x, a - b \rangle \geq \|a - b\|^2 \\ &\iff t^2 \|a - x\|^2 + (t^2 - 2t) \|a - b\|^2 + 2t(1-t) \langle a - x, a - b \rangle \geq 0 \\ &\iff t \|a - x\|^2 + (t - 2) \|a - b\|^2 + 2(1-t) \langle a - x, a - b \rangle \geq 0 \end{aligned}$$

En faisant tendre t vers 0 on obtient que pour tout $x \in C$

$$\begin{aligned} \|a - x_t\|^2 \geq \|a - b\|^2 &\implies 2 \langle a - x, a - b \rangle \geq 2 \|a - b\|^2 \quad (*) \\ &\iff 2 \langle a - b + b - x, a - b \rangle \geq 2 \|a - b\|^2 \\ &\iff \langle b - x, a - b \rangle \geq 0 \\ &\iff \langle x - b, a - b \rangle \leq 0 \end{aligned}$$

On a donc bien le résultat voulu.

3. Soient $a, a' \in E$, $b = p_C(a)$ et $b' = p_C(a')$. D'après la question précédente on a

$$\langle a - b, b' - b \rangle \leq 0$$

et

$$\langle a' - b', b - b' \rangle \leq 0 \text{ i.e. } \langle b' - a', b' - b \rangle \leq 0$$

en sommant ces deux inégalités, on obtient

$$\langle b' - a' + a - b, b' - b \rangle \leq 0 \text{ i.e. } \|b' - b\|^2 \leq \langle a' - a, b' - b \rangle$$

On a donc finalement

$$\|b' - b\|^2 \leq \langle a' - a, b' - b \rangle \leq \|a' - a\| \times \|b' - b\|$$

↑
Cauchy-Schwarz

Si $b = b'$, alors on a

$$\|p_C(a) - p_C(a')\| = \|b - b'\| = 0 \leq \|a - a'\|$$

Sinon, en simplifiant des deux côtés par $\|b' - b\|$ on trouve que

$$\|b' - b\| \leq \|a' - a\| \text{ i.e. } \|p_C(a) - p_C(a')\| \leq \|a - a'\|$$

Ce qui est bien le résultat voulu.

Correction de l'exercice II.2. : (Séparation par un hyperplan)

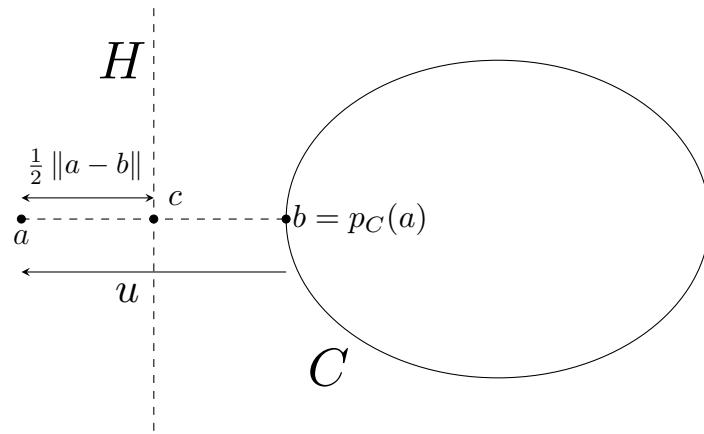
Tout hyperplan affine H de E s'écrit de la manière suivante

$$H = \{z \in \mathbb{E}, \langle u, z \rangle = k\}$$

avec $k \in \mathbb{R}$ et $u \in E$. L'hyperplan H sépare strictement a et C s'il vérifie la condition suivante :

$$\forall x \in C, \langle u, x \rangle < k \text{ et } \langle u, a \rangle > k$$

Pour comprendre l'intuition derrière la solution de cet exercice, observons le dessin suivant en dimension 2.



Nous allons construire l'hyperplan H en nous aidant du dessin ci-dessus.

Posons $b = p_C(a)$ la projection de a sur C , $u = a - b$ et $c = \frac{a+b}{2}$. Rappelons l'inégalité (*) de l'exercice précédent :

$$\forall x \in C, \langle a - x, a - b \rangle \geq \|a - b\|^2$$

On souhaite trouver un hyperplan orthogonal à $u = a - b$ séparant a et C . On a pour tout $x \in C$,

$$\begin{aligned} \langle a - x, a - b \rangle \geq \|a - b\|^2 &\iff \langle a - c + c - x, a - b \rangle \geq \|a - b\|^2 \\ &\iff \langle c - x, a - b \rangle \geq \frac{1}{2} \|a - b\|^2 \\ &\iff \langle x, u \rangle \leq \langle c, u \rangle - \frac{1}{2} \|a - b\|^2 < \langle c, u \rangle \end{aligned}$$

De plus, on a

$$\langle a - c, a - b \rangle = \left\langle \frac{a - b}{2}, a - b \right\rangle = \frac{1}{2} \|a - b\|^2$$

i.e.

$$\langle a, u \rangle = \langle c, u \rangle + \frac{1}{2} \|a - b\|^2 > \langle c, u \rangle$$

En prenant donc $k = \langle c, u \rangle$ et $H = \{z \in \mathbb{E}, \langle u, z \rangle = k\}$. On a bien

$$\forall x \in C, \langle u, x \rangle < k \text{ et } \langle u, a \rangle > k$$

H sépare donc bien a de C strictement.



CHAPITRE 19

Groupes

Définition .3.

Soit G un ensemble non vide muni d'une application $* : G \times G \rightarrow G$, appelée loi de composition interne. On dit que $(G, *)$ est un groupe si

- $*$ est associative : $\forall x, y, z \in G \quad x * (y * z) = (x * y) * z$
- $*$ admet un élément neutre, i.e. il existe $e \in G$ tel que pour tout $x \in G$, $x * e = x = e * x$.
- Tout élément admet un inverse, i.e. $\forall x \in G, \exists x^{-1} \in G, x * x^{-1} = e = x^{-1} * x$

Si $*$ est commutative, i.e. $\forall x, y \in G \quad x * y = y * x$, on dit alors que $(G, *)$ est un groupe commutatif ou groupe abélien.

Notations :

- Lorsque $(G, *)$ est un groupe commutatif, on notera plutôt $(G, +)$. Dans tout le reste du chapitre, on considère G un groupe d'élément neutre e .
- Lorsque A et B sont deux ensembles disjoints, on note $A \sqcup B$ au lieu de $A \cup B$.

Exercice .4.

Soit $(H, *)$ un monoïde (i.e. $*$ est associative et admet un élément neutre) tel que tout élément admet un inverse à gauche. Montrer que H est un groupe.

Définition .5.

On dit que $H \subset G$ est un sous-groupe du groupe $(G, *)$ si H est stable par $*$ et $(H, *|_{H \times H}) = (H, *)$ forme un groupe. On notera $H \leq G$.

Proposition .6.

$(H, *)$ est un sous-groupe de $(G, *)$ si et seulement si $H \neq \emptyset$ et

$$\forall x, y \in H \quad x * y^{-1} \in H$$

Proposition .7.

Soit $(H, *)$ un sous-groupe de $(G, *)$. Les propositions suivantes sont vraies.

1. G et H ont le même élément neutre.
2. Pour tout $x \in H$, l'inverse de x dans $(H, *)$ est égal à l'inverse de x dans $(G, *)$.
3. $\forall g, h \in G, (g * h)^{-1} = h^{-1} * g^{-1}$

Preuve

1. Posons e_G et e_H les éléments neutres respectifs de $(G, *)$ et $(H, *)$. On a $e_H * e_H = e_H$, donc en multipliant des deux côtés par l'inverse de e_H dans $(G, *)$, on obtient $e_H = e_G$.

2. Soit $a \in H$ et a_H^{-1}, a_G^{-1} ses inverses respectifs dans $(H, *)$ et $(G, *)$. On a $a_H^{-1} * a = e_H = e_G$ donc en multipliant des deux côtés à droite par a_G^{-1} , on obtient $a_G^{-1} = a_H^{-1}$.
3. Pour tout $g, h \in G$, on a $(g * h) * (h^{-1} * g^{-1}) = e$ et donc en multipliant par $(g * h)^{-1}$ des deux côtés à gauche, on obtient $(g * h)^{-1} = h^{-1} * g^{-1}$.

Proposition .8.

Soit $(G, *)$ un groupe et $S \subset G$. Alors il existe un (unique) sous-groupe minimum (pour l'inclusion) de G contenant S qu'on nomme sous-groupe engendré par S et note $\langle S \rangle$. On a alors

$$\langle S \rangle = \bigcap_{H \leq G, S \subset H} H$$

Preuve : Il suffit de vérifier qu'une intersection quelconque de sous-groupes est toujours un sous-groupe. Ceci étant clair, on a alors que $\bigcap_{H \leq G, S \subset H} H$ est bien un sous-groupe minimum (pour l'inclusion) contenant S et donc on a bien l'existence. L'unicité provient du fait que, dans un ensemble partiellement ordonné, le minimum est toujours unique s'il existe.

Exercice .9.

Soit H une partie non vide finie de G . Montrer que

$$H \leq G \iff \forall (x, y) \in H^2, x * y \in H$$

Notations :

→ (Translations dans un groupe G) Soit $a \in G$. On note

$$\gamma_a : \begin{cases} G & \longrightarrow G \\ x & \mapsto a * x \end{cases} \text{ et } \delta_a : \begin{cases} G & \longrightarrow G \\ x & \mapsto x * a \end{cases}$$

Il s'agit de permutations de G qui sont des morphismes seulement si $a = e$.

→ (Puissances dans un groupe G) Soit $n \in \mathbb{Z}^*$ et $x \in G$. On définit

$$x^n := \underbrace{x^\delta * \cdots * x^\delta}_{|n| \text{ fois}} \text{ où } \delta = \begin{cases} 1 & \text{si } n \geq 1 \\ -1 & \text{si } n \leq -1 \end{cases}$$

Pour $n = 0$ on définit $x^0 = e$. Compte tenu de cette définition, il est aisément de vérifier que

$$\forall (n, m) \in \mathbb{Z}^2, x^{n+m} = x^n * x^m$$

→ On note $Z(G) = \{x \in G, \forall y \in G x * y = y * x\}$.

Remarque : lorsqu'on note + au lieu de *, on note souvent nx au lieu de x^n .

Définition .10.

Soit f une application de G vers H . On dit que f est un morphisme (ou homomorphisme) de groupe de $(G, *)$ vers (H, \diamond) si

$$\forall x, y \in G, f(x * y) = f(x) \diamond f(y)$$

On notera $\text{Hom}(G, H)$ l'ensemble des morphismes de $(G, *)$ vers (H, \diamond) .

Exemples

1. Soit $a \in G$. L'application $j_a : \begin{cases} (\mathbb{Z}, +) & \longrightarrow (G, *) \\ n & \longmapsto a^n \end{cases}$ est un morphisme de groupe.
2. Soit $a \in G$. L'application $\sigma_a : \begin{cases} G & \longrightarrow G \\ x & \longmapsto a * x * a^{-1} \end{cases}$ est un morphisme de groupe bijectif, d'inverse $\sigma_{a^{-1}}$. Ce morphisme est nommé automorphisme intérieur associé à a .
En effet, en considérant $a, b, g \in G$, on peut affirmer que

$$\sigma_a \circ \sigma_b(g) = \sigma_a(b * g * b^{-1}) = a * b * g * b^{-1} * a^{-1} = (a * b) * g * (a * b)^{-1} = \sigma_{a * b}(g)$$

d'où $\sigma_{a * b} = \sigma_a \circ \sigma_b$ et donc, en particulier, $\sigma_a \circ \sigma_{a^{-1}} = \sigma_e = \text{Id} = \sigma_e = \sigma_{a^{-1}} \circ \sigma_a$ ce qui nous permet bien de dire que σ_a est un morphisme bijectif.

Vocabulaire : On dit que $x, y \in G$ sont conjugués s'il existe $a \in G$ tel que $y = a * x * a^{-1} = \sigma_a(x)$. La relation de conjugaison est en fait d'une relation d'équivalence sur G , qui donc le partitionne en classes d'équivalences de conjugaison.

Proposition .11.

Soit (G', \diamond) un groupe, e, e' les éléments neutres respectifs de G et G' et $f \in \text{Hom}(G, G')$.

1. $f(e) = e'$
2. Si $H \leq G$ alors $f(H) \leq G'$. En particulier, $\text{Im } f = f(G) \leq G'$.
3. Si $K \leq G'$ alors $f^{-1}(K) \leq G$. En particulier, $\text{Ker } f = f^{-1}(\{e'\}) \leq G$.
4. f est injective $\iff \text{Ker } f = \{e\} \iff \text{Ker } f \subset \{e\}$

Preuve : Les preuves de ces résultats sont laissées comme exercice au lecteur.

Proposition .12.

Soit (H, \diamond) et (H', \diamond') deux groupes.

1. Les homomorphismes se composent i.e. on peut composer $f \in \text{Hom}(H, H')$ avec $g \in \text{Hom}(G, H)$ pour obtenir $f \circ g \in \text{Hom}(G, H')$.
2. Les isomorphismes (morphismes bijectifs) se composent i.e. on peut composer $f \in \text{Hom}(H, H')$ isomorphisme avec $g \in \text{Hom}(G, H)$ isomorphisme pour obtenir $f \circ g \in \text{Hom}(G, H')$ isomorphisme.
3. L'ensemble des isomorphismes de G vers G , nommés automorphismes de G et notés $\text{Aut}(G)$, forment un groupe pour la loi \circ .

Notation : S'il existe un isomorphisme entre deux groupes G et H , on notera $G \simeq H$.

Exemple : L'application $\varphi : \begin{cases} G & \longrightarrow \text{Aut}(G) \\ a & \longmapsto \sigma_a \end{cases}$ est un morphisme de groupes de noyau

$$\text{Ker } \varphi = Z(G) = \{x \in G, \forall y \in G, x * y = y * x\}$$

En effet, pour tout $a \in G$,

$$a \in \text{Ker } f \iff \sigma_a = \text{Id} \iff \forall x \in G, a * x * a^{-1} = x \iff \forall x \in G, a * x = x * a$$

Exercice .13.

Montrer que l'application

$$\varphi : \begin{cases} (G, *) & \longrightarrow (\text{Bij}(G), \circ) \\ a & \longmapsto \gamma_a \end{cases}$$

où $\text{Bij}(G)$ désigne l'ensemble des applications bijectives de l'ensemble G dans lui-même, est un morphisme injectif de groupes.

Remarque : Cet exercice montre que tout groupe peut être vu comme un sous-groupe du groupe symétrique (groupe de permutations, éventuellement infini) et que donc si $|G| = n < \infty$, alors G peut être identifié à un sous-groupe de \mathcal{S}_n .

Notation : A partir de maintenant, lorsqu'il n'y a pas ambiguïté, pour tout $a, b \in G$, nous noterons ab ou $a \cdot b$ au lieu de $a * b$.

Définition .14.

Soit H un sous-groupe de G . On dit que H est distingué (ou normal) lorsque

$$\forall a \in G, \sigma_a(H) = aHa^{-1} \subset H$$

On note dans ce cas $H \trianglelefteq G$. Lorsque cette propriété est vérifiée, on a

$$\forall a \in G, aHa^{-1} = H \text{ et } aH = Ha$$

Remarque : Si G est abélien, alors tout sous-groupe $H \leq G$ est distingué.

Exemples

- $\{e\}$ et G sont des sous-groupes distingués de G .
- Si G' est un groupe, alors pour tout $f \in \text{Hom}(G, G')$, $\text{Ker } f$ est un sous-groupe distingué de G .
- Plus généralement, si G' est un groupe, $H'G'$ et $f \in \text{Hom}(G, G')$ alors $f^{-1}(H')G$.
- Si G' est un groupe, HG et $f \in \text{Hom}(G, G')$ alors $f(H) \text{Im } f = f(G)$.

Exercice .15.

Soit H et K deux sous-groupes de G . Montrer les propositions suivantes.

1. $HK = KH \iff HK$ est un sous-groupe de G
2. Si H est un sous-groupe distingué de G alors HK est un sous-groupe de G .
3. $H \cap K = \{e\} \iff f : \begin{cases} H \times K & \longrightarrow HK \\ (h, k) & \longmapsto hk \end{cases}$ est bijective.
4. Montrer que si H et K sont distingués et $H \cap K = \{e\}$ alors $\forall (h, k) \in H \times K, hk = kh$.
5. Montrer que si $H \cap K = \{e\}$ et $\forall (h, k) \in H \times K, hk = kh$ alors f est un isomorphisme.

I Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Soit $n \geq 2$. On note \sim la relation d'équivalence sur \mathbb{Z} définie par $a \sim b \iff n|a - b \iff a - b \in n\mathbb{Z}$. On note finalement $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences pour \sim . Une telle classe s'écrit $\bar{x} = x + n\mathbb{Z}$. Il est aisé de vérifier que $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \bar{n-1}\} = \{\bar{m}, \dots, \bar{m+n-1}\}$ pour tout m et que ces n éléments sont distincts.

Proposition I.1.

Si X, Y sont deux classes dans $\mathbb{Z}/n\mathbb{Z}$ et $x \in X, y \in Y$, alors $\overline{x+y}$ ne dépend que de X et Y .

Remarque : La proposition ci-dessus permet donc de définir une loi $+$ sur $\mathbb{Z}/n\mathbb{Z}$ qui en fait un groupe abélien.

Proposition I.2.

1. L'application $\varphi : \begin{cases} \mathbb{Z}/n\mathbb{Z} & \longrightarrow \mathbb{U}_n \\ \bar{k} & \longmapsto e^{\frac{i2\pi k}{n}} \end{cases}$ est bien définie et est un isomorphisme.
2. L'application $\pi : \begin{cases} \mathbb{Z} & \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto \bar{x} \end{cases}$ est un morphisme surjectif de noyau $\text{Ker}(\pi) = n\mathbb{Z}$

II Ordre d'un élément

Soit $a \in G$. Remarquons que $\langle a \rangle = \{a^k, k \in \mathbb{Z}\}$. Introduisons tout d'abord le morphisme suivant

$$j_a : \begin{cases} \mathbb{Z} & \longrightarrow \langle a \rangle \\ m & \longmapsto a^m \end{cases}$$

Pour tout $a \in G$, j_a est un morphisme de groupe surjectif. D'après la proposition I.9, $\text{Ker } j_a$ est un sous groupe de $(\mathbb{Z}, +)$. Il est bien connu que les sous groupes de \mathbb{Z} sont les groupes de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$. Deux cas se présentent donc.

- Si $n \neq 0$, alors $\text{Ker } j_a = n\mathbb{Z}$. On note alors $\omega(a) = n$ et on dit que l'ordre de a est égal à n .
- Sinon, $\text{Ker } j_a = \{0\}$ et alors j_a est un isomorphisme. Dans ce cas, on note $\omega(a) = \infty$ et on dit que l'ordre de a est infini.

Remarque : Pour tout $a \in G$, on peut également définir $\omega(a)$ comme

$$\omega(a) = \min\{k \in \mathbb{N}^*, a^k = e\}$$

Proposition II.1.

Supposons que $\text{Ker } j_a \neq \{0\}$ et posons $n = \omega(a)$. Les propositions suivantes sont vraies.

1. $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$ et ces éléments sont distincts. De plus, $\forall k \in \mathbb{Z}, a^k = e \iff n|k$.
2. $n = \min\{m \in \mathbb{N}^*, a^m = e\}$
3. $\forall m \in \mathbb{Z}, \exists! k \in [0; n-1], a^m = a^k$
4. $\forall k \in \mathbb{Z}, \omega(a^k) = \frac{n}{n \wedge k}$
5. Si $q|n$ alors $\omega(a^q) = \frac{n}{q}$.

Preuve :

1. Montrons d'abord la deuxième partie de ce point. Pour tout $k \in \mathbb{Z}$, on a

$$a^k = e \iff k \in \text{Ker } j \iff k \in n\mathbb{Z} \iff n|k$$

et en particulier $a^n = e$. Montrons ensuite que $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$.

$\rightarrow (\supset)$ Cette inclusion est évidente.

$\rightarrow (\subset)$ Soit $k \in \mathbb{Z}$. Faisons la division euclidienne de k par n : $k = qn + b$ avec $b \in \llbracket 0; n - 1 \rrbracket$. On a alors $a^k = (a^n)^q a^b = e^q a^b = a^b$. Ces éléments sont de plus distincts car si $i, j \in \llbracket 0; n - 1 \rrbracket$ vérifient $a^i = a^j$ alors $a^{i-j} = e$ et donc $n|i - j$ d'où $i = j$.

2. D'après le point 1, $\forall k \in \llbracket 1; n - 1 \rrbracket$ $a^k \neq e$ et $a^n = e$ d'où le résultat.

3. Ce point est une conséquence directe du point (1).

4. Soit $k, l \in \mathbb{Z}$. On a

$$(a^k)^l = e \iff a^{kl} = e \iff n|kl \iff \frac{n}{n \wedge k} \left| \frac{k}{n \wedge k} l \right. \stackrel{\text{Gauß}}{\iff} \frac{n}{n \wedge k} | l$$

L'avant dernière équivalence provient du fait que $\frac{k}{n \wedge k} \wedge \frac{n}{n \wedge k} = \frac{n \wedge k}{n \wedge k} = 1$.

a^k étant clairement d'ordre fini, en utilisant le point 2, on a $\omega(a^k) = \min\{l \in \mathbb{N}^* \mid (a^k)^l = e\} = \frac{n}{n \wedge k}$.

5. Ce point est une conséquence directe du point précédent.

III Actions de morphismes

Proposition III.1.

Soit G' un groupe d'élément neutre e' , $a \in G$, et $f \in \text{Hom}(G, G')$. Les propositions suivantes sont vraies.

1. Si $\omega(a) < \infty$, alors $\omega(f(a))|\omega(a)$.
2. Si f est injective, alors $\omega(a) = \omega(f(a))$.
3. Si a et b sont deux éléments de G conjugués, i.e. il existe $c \in G$ tel que $a = cbc^{-1}$, alors $\omega(a) = \omega(b)$. En particulier, $\forall x, y \in G$, $\omega(xy) = \omega(yx)$.

Preuve :

1. Supposons que $\omega(a) < \infty$. On a $f(a)^{\omega(a)} = f(a^{\omega(a)}) = f(e) = e'$ et donc $\omega(f(a)) < \infty$ et $\omega(f(a))|\omega(a)$

2. Supposons que f est injective. Deux cas se présentent.

\rightarrow Si $\omega(a) = \infty$, alors il est facile de vérifier que $\langle f(a) \rangle = f(\langle a \rangle)$. f est injective et $\langle a \rangle$ est infini, donc $\langle f(a) \rangle$ aussi et donc en utilisant le point 1 de la proposition III.1, on voit qu'on ne peut pas avoir $\omega(a) < \infty$.

\rightarrow Si $\omega(a) = n \in \mathbb{N}^*$, alors

$$f(a)^k = e' \iff f(a^k) = f(e) \underset{f \text{ injective}}{\iff} a^k = e \iff \omega(a)|k$$

On en déduit donc que $\omega(a)|\omega(f(a))$. En combinant ce résultat avec le point (1), on obtient bien que $\omega(a) = \omega(f(a))$.

3. Le fait que a et b soient conjugués se traduit par le fait qu'il existe $z \in G$ tel que $b = \sigma_z(a)$. σ_z est un morphisme injectif, donc en utilisant le point (2), on voit que $\omega(b) = \omega(\sigma_z(a)) = \omega(a)$. Enfin, pour montrer la deuxième partie de ce point, il suffit de voir que $xy = \sigma_x(yx)$.

Exercice III.2.

Soit $m, n \geq 1$ tel que $m \wedge n = 1$. Déterminer $\text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$.

Exercice III.3.

Soit $(a, b) \in G^2$ tels que $\omega(a) = m \leq \omega(b) = n < \infty$.

1. A-t-on $\omega(ab) < \infty$? Indice : Penser aux symétries dans \mathbb{R}^2 .
2. Supposons que $ab = ba$ et $\omega(a) \wedge \omega(b) = 1$. Montrer que $\omega(ab) = mn$.
3. On suppose toujours que $ab = ba$. Montrer qu'il existe $c \in G$ tel que $\omega(c) = n \vee m$.
4. On suppose maintenant que G est abélien et fini. Montrer qu'il existe $z \in G$ tel que $\forall x \in G, \omega(x) | \omega(z)$. En particulier, on montrera l'existence de $z \in G$ tel que $\omega(z) = \bigvee_{x \in G} \omega(x)$.

Proposition (Théorème faible de Lagrange) III.4.

Supposons que G est commutatif et soit $a \in G$. On a $\omega(a) | |G|$.

Preuve : On sait que γ_a est bijective, on a donc

$$\prod_{g \in G} g = \prod_{g \in G} \gamma_a(g) = \prod_{g \in G} (ag) = a^{|G|} \prod_{g \in G} g$$

En multipliant par l'inverse de $\prod_{g \in G} g$ on obtient que $a^{|G|} = e$, ce qui implique d'après la proposition III.1 que $\omega(a) | |G|$.

IV Groupes cycliques**Définition IV.1.**

On dit que G est monogène s'il est engendré par un seul élément, i.e. il existe $a \in G$ tel que $G = \langle a \rangle$. Si de plus G est fini, alors on dit qu'il est cyclique.

Remarque IV.2.

Supposons que G est monogène, i.e. qu'il existe $a \in G$ tel que $G = \langle a \rangle$. Deux cas se présentent.

1. Si $\omega(a) = \infty$, alors $j : \begin{cases} \mathbb{Z} & \longrightarrow \langle a \rangle \\ m & \longmapsto a^m \end{cases}$ est un isomorphisme.
2. Si $\omega(a) < \infty$, alors $G = \langle a \rangle = \{e, a, \dots, a^{n-1}\}$ avec ces éléments distincts. En particulier, on a $|G| = \omega(a)$.

Vocabulaire : Pour tout $a \in G$, lorsque $G = \langle a \rangle$, on dit que a est un élément générateur de G .

Proposition IV.3.

Soit $n \in \mathbb{N}^*$. G est cyclique de cardinal n si et seulement si G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. De plus, si $\psi : (G, *) \longrightarrow (\mathbb{Z}/n\mathbb{Z}, +)$ et $b \in G$ un générateur de G , i.e. $G = \langle b \rangle$, alors $\psi(b) = \bar{1}$ implique que ψ est un isomorphisme.

Preuve : Montrons tout d'abord l'équivalence.

\rightarrow (\Leftarrow) Cette implication est facile à montrer.

→ (⇒) Supposons que G est cyclique de cardinal fini égal à n . Il existe donc $a \in G$ tel que $G = \{e, a, \dots, a^{n-1}\}$. Considérons le morphisme de groupe suivant

$$\psi : \begin{cases} (\mathbb{Z}/n\mathbb{Z}, +) & \longrightarrow (G, *) \\ \bar{k} & \longmapsto a^k \end{cases}$$

On peut facilement montrer que ψ est bien défini et bijectif et alors $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Le dernier point de la proposition découle directement du raisonnement effectué ci-dessus.

Exercice IV.4.

Supposons que G est cyclique d'ordre (de cardinal) n et soit a un générateur de G . Soit H un sous groupe de G . Posons $d = |H|$. Montrer que $H = \langle a^{\frac{n}{d}} \rangle$.

Remarque : Cette remarque peut être très utile dans quelques exercices difficiles. Soit $n \geq 1$. L'ensemble $D_n = \{k \geq 1 \mid k|n\}$ vérifie $|D_n| \leq 2\sqrt{n} + 1$. En effet, l'application

$$\varphi : \begin{cases} D_n \cap [1; \lfloor \sqrt{n} \rfloor] & \longrightarrow D_n \cap [\lfloor \sqrt{n} \rfloor; n] \\ d & \longmapsto \frac{n}{d} \end{cases}$$

est une bijection et donc

$$\begin{aligned} |D_n| &= |D_n \cap [1; \lfloor \sqrt{n} \rfloor]| + |D_n \cap [1 + \lfloor \sqrt{n} \rfloor; n]| \\ &\leq |D_n \cap [1; \lfloor \sqrt{n} \rfloor]| + |D_n \cap [\lfloor \sqrt{n} \rfloor; n]| + 1 \\ &= 2|D_n \cap [1; \lfloor \sqrt{n} \rfloor]| + 1 \leq 2\sqrt{n} + 1 \end{aligned}$$

Exercice IV.5.

Supposons que G est cyclique et posons $|G| = n \geq 2$ et soit a un générateur de G .

1. Montrer que pour tout $k \in \mathbb{Z}$, a^k génère G si et seulement si $k \wedge n = 1$.
2. Posons $\varphi(n) = |\{k \in [1; n] \mid k \wedge n = 1\}|$. Cette application est nommée l'indicatrice d'Euler. En utilisant la question précédente, montrer que $\sum_{d|n} \varphi(d) = n$.

Exercice IV.6.

1. Soit $(G_1, *)$ et (G_2, \diamond) deux groupes cycliques. On considère la loi de composition intérne $\otimes : G_1 \times G_2 \longrightarrow G_1 \times G_2$ définie par

$$\forall (g_1, g_2, g'_1, g'_2) \in G_1 \times G_2 \times G_1 \times G_2, (g_1, g_2) \otimes (g'_1, g'_2) = (g_1 * g'_1, g_2 \diamond g'_2)$$

Trouver une condition nécessaire et suffisante pour que $(G_1 \times G_2, \otimes)$ soit cyclique.

2. (Théorème des restes chinois) Soit $a, b \geq 2$. Montrer que $\varphi : \begin{cases} \mathbb{Z}/ab\mathbb{Z} & \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ \bar{x} & \longmapsto (\bar{x}, \bar{x}) \end{cases}$ est bien définie puis que φ est un isomorphisme si et seulement si $a \wedge b = 1$.

Exercice IV.7.

Soit A un anneau commutatif unitaire.

1. Soit $P, Q \in A[X]$ avec Q de coefficient dominant égal à 1 (i.e. $Q = 1$ ou Q est unitaire) (ici, on désigne par 1 l'élément neutre pour la multiplication de l'anneau A). Montrer que l'on peut effectuer "la" division euclidienne de P par Q
2. On suppose que A est intègre et $\deg P \geq 0$. Montrer que P possède au plus $\deg P$ racines distinctes
3. Soit $(\mathbb{K}, +, \times)$ un corps et (G, \times) un sous-groupe fini de (\mathbb{K}^*, \times) , où \mathbb{K}^* est l'ensemble des éléments de \mathbb{K} inversible pour la loi \times . Montrer que G est cyclique.

Remarque à propos de l'exercice V.7 : La question 1 demande montrer que lorsqu'un polynôme $Q \in A[X]$ est de coefficient dominant égal à 1, on peut effectuer la division euclidienne de tout polynôme $P \in A[X]$ par Q . Ce résultat est aussi vrai lorsque le coefficient dominant de Q est inversible, mais devient faux lorsque ce n'est pas le cas. Lorsque A est un corps, tous les éléments de A sauf 0 sont inversibles, on peut donc toujours effectuer la division euclidienne par un polynôme non nul.

V Groupe engendré par une partie

Proposition V.1.

Pour tout $A \subset G$, il existe un plus petit sous-groupe $\langle A \rangle$ de G contenant A appelé sous-groupe engendré par A . De plus, on a

$$\langle A \rangle = \bigcap_{H \leq G, A \subset H} H = \{a_1^{\alpha_1} \dots a_n^{\alpha_n}, n \in \mathbb{N}, a_1, \dots, a_n \in A, \alpha_1, \dots, \alpha_n \in \mathbb{Z}\}$$

Preuve : L'existence et la première égalité ont déjà été établis à la proposition I.6. Montrons la seconde égalité, i.e.

$$\langle A \rangle = \underbrace{\{a_1^{\alpha_1} \dots a_n^{\alpha_n}, n \in \mathbb{N}, a_1, \dots, a_n \in A, \alpha_1, \dots, \alpha_n \in \mathbb{Z}\}}_B$$

Il est facile de montrer que B est bien un sous-groupe de G contenant A . On en déduit donc que $\langle A \rangle \subset B$. Montrons l'inclusion réciproque. Pour tout $n \in \mathbb{N}$ $a_1, \dots, a_n \in A \subset \langle A \rangle$ et $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$, par stabilité, on a $a_1^{\alpha_1} \dots a_n^{\alpha_n} \in \langle A \rangle$, d'où l'égalité voulue.

Vocabulaire : On dit que $S \neq \emptyset$ est générateur (de G) si $G = \langle S \rangle$

Exemple : (\mathcal{S}_n, \circ) est généré par les transposition de la forme $(i \ i+1)$, i.e.

$$\mathcal{S}_n = \langle \{(i \ i+1), i \in \llbracket 1; n-1 \rrbracket\} \rangle$$

Exercice V.2.

Supposons que $(G, *)$ soit un groupe fini abélien et soit p un nombre premier tel que $\forall g \in G, \omega(g)|p$ (ou d'une manière équivalente, $\forall g \in G, g^p = e$). Montrer qu'il existe $n \in \mathbb{N}$ tel que $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$.

Exercice V.3.

Soit $H \neq \{e\}$ un groupe où e est son élément neutre. Notons \mathbb{P} l'ensemble des nombres premiers. On pose $\text{Sg}(H)$ l'ensemble des sous-groupes de H . Montrer que les propositions suivantes sont équivalentes.

1. $\text{Sg}(H) = \{\{e\}, H\}$
2. $\exists p \in \mathbb{P}, H \simeq \mathbb{Z}/p\mathbb{Z}$
3. $\forall g \in H \setminus \{e\}, \langle g \rangle = H$
4. $\exists p \in \mathbb{P}, |H| = p$

VI Compléments

1. Classes latérales et groupe quotient

Proposition VI.1.

Soit H un sous-groupe de G . La relation \sim_g sur G^2 définie par

$$\forall a, b \in G, a \sim_g b \iff b \in aH$$

est une relation d'équivalence. La classe d'équivalence de a pour \sim_g est aH et est appelée classe à gauche selon H de a . On note cette classe \bar{a} .

Remarque :

- En fait, on peut également définir la même notion d'équivalence à droite \sim_d par $a \sim_d b \iff b \in Ha$. Ces deux relations sont les mêmes si et seulement si H est distingué. Dans ce cas, on la notera simplement \sim . Nous discuterons un peu plus de cette notion d'équivalence à droite et à gauche dans les compléments de ce chapitre.
- Une manière équivalente de définir cette relation est

$$a \sim_g b \iff b^{-1}a \in Ha \sim_d b \iff ab^{-1} \in H$$

Définition et Proposition VI.2.

Soit H un sous-groupe distingué de G . Les propriétés suivantes sont vraies.

1. Le produit de deux classes à gauche selon H est une classe à gauche selon H .
2. Pour ce produit, l'ensemble des classes à gauche selon H forme un groupe, noté G/H .
3. Pour tout $a, b \in G$, $\gamma_{ba^{-1}}$ est une bijection entre aH et bH et par conséquent lorsque H est fini, $\forall a \in G, |aH| = |H|$, i.e. toute classe à gauche selon H est en bijection avec H .
4. L'élément neutre de G/H est H (ou d'une manière équivalente \bar{e}).

Preuve :

1. Pour tout $a, b \in G$, on a $aH * bH = a * b * H * H = abH$.
2. Il suffit d'appliquer la définition d'un groupe pour démontrer ce point.
3. Remarquons que
 - $\gamma_{ba^{-1}}(aH) \subset bH$ et $\gamma_{ab^{-1}}(bH) \subset aH$

- L'application $\gamma_{ab^{-1}} : bH \longrightarrow aH$ est un inverse (et donc l'unique inverse) de $\gamma_{ba^{-1}}$ et donc $\gamma_{ba^{-1}}$ est bijective

Par conséquent, pour tout $a, b \in G$, $|aH| = |bH|$ et en particulier $|aH| = |eH| = |H|$.

4. $H = \bar{e}$ donc pour tout $a \in G$, $\bar{ea} = \bar{ae} = \bar{a}$ donc H est bien l'élément neutre de G/H .

Remarque :

- Pour bien comprendre cette notion de groupe quotient, il faut voir que pour tout $a \in G$, la classe \bar{a} comme une sorte d'ensemble d'éléments de même "reste" que a dans G pour une certaine "division". Lorsque $*$ est additive, on peut faire l'analogie avec $\mathbb{Z}/n\mathbb{Z}$. En effet, $(n\mathbb{Z}, +) \trianglelefteq (\mathbb{Z}, +)$ et le groupe quotient de \mathbb{Z} par $n\mathbb{Z}$ est tout simplement égal au groupe bien connu $\mathbb{Z}/n\mathbb{Z}$. Dans ce cas, lorsque $+$ est additive, en pensant à cet exemple, on peut voir les classes $\bar{a} = a + H$ comme l'ensemble des éléments de même "restes" que a "modulo H ". Dans l'exemple de $\mathbb{Z}/n\mathbb{Z}$, on a bien entendu $H = n\mathbb{Z}$.
- L'égalité $|H| = |aH| = |Ha|$ reste vraie même si H n'est pas distingué dans G .

Notation : Même lorsque H est un sous-groupe non distingué de G , on notera G/H l'ensemble des classes à gauche de G selon H , i.e. l'ensemble $\{\bar{g}, g \in G\} = \{gH, g \in G\}$. Dans ce cas, G/H n'est pas un groupe, car lorsque G est non abélien, le produit de deux classes à gauche n'est pas forcément une classe à gauche. De la même manière, on notera par $H\backslash G$ l'ensemble des classes à droite de G selon H i.e. l'ensemble $\{Hg, g \in G\}$.

Proposition VI.3.

Soit H un sous-groupe distingué de G . Les propositions suivantes sont vraies.

1. L'application $\pi : \begin{cases} G & \longrightarrow G/H \\ a & \mapsto aH \end{cases}$ est un morphisme surjectif de noyau $\text{Ker } \pi = H$. On l'appellera la surjection canonique.
2. Soit G' un groupe et $f \in \text{Hom}(G, G')$. Il existe $\tilde{f} \in \text{Hom}(G/\text{Ker } f, G')$ injective d'image $\text{Im } f$ tel que $f = \tilde{f} \circ \pi$. En particulier, $G/\text{Ker } f$ est isomorphe à $\text{Im } f$.

Preuve :

1. C'est clairement un morphisme par ce qui précède. Soit $a \in \text{Ker } \pi$. On a $aH = H$, il existe donc $g \in H$ tels que $ae = g$, i.e. $a = g \in H$. On en déduit donc que $\text{Ker } \pi \subset H$. L'implication réciproque est évidente.
2. Posons $H = \text{Ker } f$ et considérons l'application

$$\tilde{f} : \begin{cases} G/H & \longrightarrow G' \\ aH & \mapsto f(a) \end{cases}$$

Cette application est bien définie (elle est indépendante du représentant), est clairement un morphisme et est injective. En effet, pour tout $U \in \text{Ker } \tilde{f}$, il existe $a \in G$ tels que $U = aH$. On a alors

$$\tilde{f}(U) = e' \iff \tilde{f}(aH) = e' \iff f(a) = e' \iff a \in \text{Ker } f \iff aH = H$$

et donc $\text{Ker } \tilde{f} = \{H\}$, et H est l'élément neutre de G/H . On en déduit donc que \tilde{f} induit un isomorphisme entre G/H et $\text{Im } f$ et que en particulier $G/\text{Ker } f$ et $\text{Im } f$ sont isomorphes.

Théorème (Théorème de Lagrange) VI.4.

Supposons que G est fini. Soit H un sous-groupe de G . On a $|H| \mid |G|$.

Preuve : Les classes à gauche selon H , $\{aH, a \in G\}$, sont disjointes et en nombre fini. Il existe donc $p \in \mathbb{N}^*$ et $a_1, \dots, a_p \in G$ tels que $G = \bigsqcup_{k=1}^p a_k H$. Cette union étant disjointe et d'après la proposition VII.1 tous ces ensembles sont de même cardinal égal à $|H|$, on peut écrire

$$|G| = \left| \bigsqcup_{k=1}^p a_k H \right| = \sum_{k=1}^p |a_k H| = p |H|$$

et alors finalement $|H| \mid |G|$.

Remarques :

- Avec ce théorème, on aurait pu facilement montrer la proposition IV.4. En effet, pour tout $a \in G$, $\langle a \rangle$ est un sous-groupe de G , donc d'après le théorème de Lagrange, on a $|\langle a \rangle| \mid |G|$. D'après la proposition III.1, on a $|\langle a \rangle| = \omega(a)$, ce qui permet de conclure.
- En rejetant un coup d'œil à la preuve du théorème, il est facile de voir que lorsque H est un sous-groupe de G avec G fini, alors $|G| = |G/H| \times |H|$ et par conséquent $|G/H| = |G| / |H|$.
On notera $[G : H] := |G/H|$ qu'on nommera l'indice de H dans G . Ce dernier peut être défini même si G est infini et que, si G est fini, on obtient $[G : H] = |G| / |H|$.

Exercice VI.5.

Soit p, q deux nombres premiers distincts et $(H, *)$ un groupe abélien tel que $|H| = pq$. Montrer que $H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

Exercice VI.6.

Supposons que G est un groupe fini et H un sous-groupe de G d'indice $[G : H] = 2$ i.e. $|G| = 2|H|$. Montrer que H est un sous-groupe distingué de G et que donc H contient tous les carrés.

2. Actions de groupes

Dans cette partie, on considère X un ensemble non vide.

Définition VI.7.

Une action de groupe (à gauche) est une application $\bullet : G \times X \rightarrow X$, telle que

- $\forall x \in X, e \bullet x = x$
- $\forall g, h \in G \forall x \in X (gh) \bullet x = g \bullet (h \bullet x)$

Remarque : On peut également définir les actions de groupe d'une autre manière. En effet, en considérant $\phi : G \rightarrow \text{Bij}(X)$ un morphisme de groupe de $(G, *)$ dans $(\text{Bij}(X), \circ)$, pour tout $g \in G$ et $x \in X$, on peut remplacer $g \bullet x$ par $\phi(g)(x)$.

Exemples :

- Lorsque $X = G$, $\phi_1 : (g, h) \mapsto \gamma_g(h)$ ($g \bullet h = \gamma_g(h)$) et $\phi_2 : (g, h) \mapsto \sigma_g(h)$ ($g \bullet h = \sigma_g(h)$) sont des actions de groupe. ϕ_1 est appelée action de translation à gauche et ϕ_2 est appelée action de conjugaison.
- $\phi_3 : (g, h) \mapsto \delta_g(h)$ une action de groupe seulement si G est abélien.

Définition VI.8.

Soit $x \in X$.

- L'ensemble $O(x) = \{g \bullet x, g \in G\}$ est appelé orbite de x .
- L'ensemble $\text{Stab}(x) = \{g \in G, g \bullet x = x\}$ est appelé stabilisateur de x .

Proposition VI.9.

Soit $\bullet : G \times X \mapsto X$ une action de groupe. Les propositions suivantes sont vraies.

1. Pour tous $x, y \in X$, on a $O(x) \cap O(y) = \emptyset$ ou $O(x) = O(y)$. De plus, on a $X = \bigcup_{x \in X} O(x)$.
2. Pour tout $x \in X$, $\text{Stab}(x)$ est un sous-groupe de G . De plus, on a l'implication suivante pour tout $y \in X$

$$y = g \bullet x \implies \text{Stab}(y) = g\text{Stab}(x)g^{-1} = \sigma_g(\text{Stab}(x))$$

3. Soit $x \in X$. L'application $\phi_x : \begin{cases} G/\text{Stab}(x) & \longrightarrow O(x) \\ \bar{g} & \longmapsto g \bullet x \end{cases}$ est bien définie et est une bijection. En particulier, si G est fini, $|G/\text{Stab}(x)| = |G|/|\text{Stab}(x)| = |O(x)|$.
4. (Formule des classes) Supposons G et X sont finis et soit $k \in \mathbb{N}^*$ et $(x_i)_{i \in \llbracket 1; k \rrbracket}$ un système de représentants des orbites de G i.e. $X = \bigsqcup_{i \in \llbracket 1; k \rrbracket} O(x_i)$ et pour tout $i, j \in \llbracket 1; k \rrbracket$ différents, $O(x_i) \neq O(x_j)$. On a $|X| = \sum_{i \in \llbracket 1; k \rrbracket} |O(x_i)| = \sum_{i \in \llbracket 1; k \rrbracket} \frac{|G|}{|\text{Stab}(x_i)|}$.

Preuve :

1. Soit \sim la relation sur X^2 définie par $\forall x, y \in X, x \sim y \iff y \in O(x)$. Montrons que la relation \sim est une relation d'équivalence.
 - Réflexivité : on a pour tout $x \in X$, $e \bullet x = x$ donc $x \in O(x)$ et alors $x \sim x$.
 - Symétrie : soit $x, y \in X$. Supposons que $x \sim y$. On dispose donc de $g \in G$ tel que $g \bullet x = y$. On a alors $g^{-1} \bullet y = g^{-1} \bullet g \bullet x = x$ et alors $x \in O(y)$, i.e. $y \sim x$.
 - Transitivité : soit $x, y, z \in X$ tels que $x \sim y$ et $y \sim z$. Il existe donc $g, h \in G$ tels que $g \bullet x = y$ et $h \bullet y = z$ et alors $g \bullet h \bullet x = z$. On en déduit donc que $gh \bullet x = z$ et donc $z \in O(x)$, i.e. $x \sim z$.

On peut également facilement voir que pour tout $x \in X$, $O(x)$ est la classe d'équivalence de x pour \sim . On peut donc partitionner X en classes d'équivalences pour \sim , i.e. pour tout $x, y \in X$, on a $O(x) \cap O(y) = \emptyset$ ou $O(x) = O(y)$ et $X = \bigcup_{x \in X} O(x)$.

2. Soit $x \in X$. La preuve du fait que $\text{Stab}(x)$ est un sous-groupe de G ne présente pas de difficulté et est donc laissé comme exercice au lecteur. Soit $y \in G$ et $h \in G$, on a alors

$$\begin{aligned} h \in \text{Stab}(y) &\iff h \in \text{Stab}(g \bullet x) \iff h \bullet (g \bullet x) = g \bullet x \\ &\iff (g^{-1}hg) \bullet x = x \iff g^{-1}hg \in \text{Stab}(x) \\ &\iff h \in g\text{Stab}(x)g^{-1} \end{aligned}$$

Et donc $\text{Stab}(g \bullet x) = g\text{Stab}(x)g^{-1}$

3. D'abord ϕ_x est clairement bien définie (indépendante du représentant). Montrons que ϕ_x est injective. Soit $g, h \in G$. On a

$$\begin{aligned}\phi_x(\bar{g}) = \phi_x(\bar{h}) &\implies g \bullet x = h \bullet x \implies (g^{-1}h) \bullet x = x \\ &\implies g^{-1}h \in \text{Stab}(x) \implies h \in g\text{Stab}(x) \\ &\implies h \in \bar{g} \implies \bar{h} = \bar{g}\end{aligned}$$

Donc ϕ_x est bien injective. Elle est de plus clairement surjective par définition de $O(x)$, ce qui nous permet de conclure qu'elle est bien bijective.

4. On sait d'après le point (1) que les ensembles $(O(x_i))_{i \in [\![1;k]\!]}$ sont disjoints. De plus, d'après le point 3, pour tout $x \in X$, $G/\text{Stab}(x)$ est en bijection avec $O(x)$, i.e. $|G/\text{Stab}(x)| = |O(x)|$. On en déduit donc que

$$|X| = \left| \bigsqcup_{i \in [\![1;k]\!]} O(x_i) \right| = \sum_{i=1}^k |O(x_i)| = \sum_{i=1}^k |G/\text{Stab}(x_i)| = \sum_{i=1}^k \frac{|G|}{|\text{Stab}(x_i)|}$$

Exercice VI.10.

Soit G un groupe fini et $H \leq G$ tel que $[G : H] = p$ où p est le plus petit premier qui divise l'ordre de G . Montrer que HG et que donc H contient toutes les puissances p -èmes

3. Application : action de conjugaison

Cette section traite le cas particulier de l'action par conjugaison/automorphisme intérieur sur G fini

$$\bullet : \begin{cases} G \times G & \longrightarrow G \\ (g, a) & \longmapsto gag^{-1} \end{cases}$$

Définition VI.11.

Soit $a \in G$.

- L'ensemble $O(a) = \{xax^{-1}, x \in G\}$ est appelé orbite de a .
- L'ensemble $C(a) = \{x \in G, xa = ax\} = \{x \in G, xax^{-1} = a\} = \text{Stab}(a)$ est appelé commutant de a . Il s'agit de l'ensemble des éléments de G qui commutent avec a .

Remarque : Pour tout $a \in G$, on a $a \in Z(G) \iff C(a) = G \iff O(a) = \{a\}$.

Proposition VI.12.

Soit $a \in G$. Les propositions suivantes sont vraies.

1. $C(a)$ est un sous-groupe de G et $|G/C(a)| = |O(a)|$.
2. $|G| = |C(a)| \times |O(a)|$
3. (Formule des classes) Soit R un ensemble de représentants des classes de conjugaison (ou des orbites) non réduites à un singleton et R' les représentants des orbites réduites à un singleton (i.e. les éléments qui commutent avec tous les éléments de G), alors

$$|G| = \sum_{x \in R'} |O(x)| + \sum_{x \in R} |O(x)| = |Z(G)| + \sum_{x \in R} \frac{|G|}{|C(x)|}$$

Preuve : Les preuves de ces résultats sont des applications directes de la proposition VII.9.

L'exercice suivant est une application de la proposition ci-dessus.

Exercice VI.13.

Soit $n \in \mathbb{N}^*$ et p un nombre premier. On suppose que $|G| = p^n$. Montrer que le centre de G , $Z(G)$, n'est pas réduit à un singleton. En particulier, si $n \leq 2$ alors G est abélien

Le théorème suivant est également une application de la proposition ci-dessus.

Théorème (Théorème de Cauchy) VI.14.

Supposons que G est fini et soit p un nombre premier tel que $p||G|$. Il existe $x \in G$, $\omega(x) = p$.

Preuve : Posons $n = |G|$ et considérons l'ensemble $E = \{(x_1, \dots, x_p) \in G^p \mid x_1 \dots x_p = e\}$. Il est aisément de voir que

$$\begin{aligned} |E| &= |\{(x_1, \dots, x_p) \in G^p \mid x_1 \dots x_p = e\}| \\ &= \left| \{(x_1, \dots, x_{p-1}, x_{p-1}^{-1} \dots x_1^{-1}), (x_1, \dots, x_{p-1}) \in G^{p-1}\} \right| = |G^{p-1}| \end{aligned}$$

et alors $|E| = n^{p-1}$. Considérons l'action de groupe de permutation circulaire sur E

$$\bullet : \begin{cases} \mathbb{Z}/p\mathbb{Z} \times E & \longrightarrow E \\ (\bar{k}, (x_1, \dots, x_p)) & \mapsto (x_{\sigma^k(1)}, \dots, x_{\sigma^k(p)}) \end{cases}$$

où $\sigma = (1 \ 2 \ \dots \ p)$. On notera par abus de notation $k \bullet x$ au lieu de $\bar{k} \bullet x$ (remarquer au passage que ce n'est pas vraiment un abus de notation vu que c'est plutôt l'action de \mathbb{Z} qui est court-circuitée par $\mathbb{Z}/p\mathbb{Z}$). Remarquons que pour tout $k, l \in \mathbb{Z}$, $k \bullet (l \bullet x) = (k + l) \bullet x$. S'il existe $k \in \mathbb{Z}$ tel que $\bar{k} \neq \bar{0}$ et $k \bullet x = x$, alors d'après Bezout, étant donné que k est premier avec p , il existe $u, v \in \mathbb{Z}$ tels que $uk + vp = 1$ et alors, en supposant sans perte de généralité que $u \geq 0$ et $v \leq 0$

$$1 \bullet x = (uk + vp) \bullet x = vp \bullet (uk \bullet x) = \underbrace{-p \bullet \dots \bullet -p}_{-v \text{ fois}} \bullet \underbrace{k \bullet \dots \bullet k}_{u \text{ fois}} \bullet x = x$$

Le fait que $1 \bullet x = x$ est équivalent à $(x_1, x_2, \dots, x_p) = (x_2, x_3, \dots, x_p, x_1)$ i.e.

$$x_1 = x_2, \quad x_2 = x_3, \quad \dots, \quad x_{p-1} = x_p$$

et alors pour tout $k \in \mathbb{Z}$, $k \bullet x = x$ i.e. $O(x)$ ne contient qu'un seul élément. On en déduit que pour tout $x \in E$, deux cas sont possibles : $\forall k, l \in \mathbb{Z}$, $k \bullet x \neq l \bullet x$ et alors $O(x)$ contient p éléments, ou alors $\forall k \in \mathbb{Z}$, $k \bullet x = x$ et donc $O(x)$ contient un seul élément. En posant S_1 l'ensemble des orbites à un seul élément et S_2 l'ensemble des orbites à p éléments, le fait que E est union disjointe des orbites de l'action de groupe \bullet nous permet de dire que

$$|G|^{p-1} = |E| = \left| \bigcup_{X \in S_1} X \right| + \left| \bigcup_{X \in S_2} X \right| = |S_1| + p|S_2|$$

p divise $|G|$, donc p divise aussi $|S_1| = |K|$. $O((e, \dots, e)) \in S_1$ et $p \geq 2$ donc $|K| = |S_1| \geq 2$. Il existe donc $x \in E \setminus \{e\}$ tel que $x^p = e$.

Lorsque G est abélien, on dispose d'une preuve plus rapide.

Exercice (Inspiré du TD d'Alain Troesh) VI.15.

Supposons que G est un groupe abélien fini et soit p un nombre premier.

1. Soit K un sous groupe distingué de G . Montrer que s'il existe $x \in G/K$ d'ordre p alors il en existe un aussi d'ordre p dans G .
2. On suppose que $p||G|$, montrer qu'il existe $x \in G$, $\omega(x) = p$.
3. Soit $a \geq 1$. On suppose que $p^a||G|$. Montrer que $\exists H \leq G$ d'ordre p^a
4. Soit H et L deux sous groupes de G tels que $|H| \wedge |L| = 1$. G est commutatif, donc HL est un sous-groupe de G . Considérons le morphisme de groupes

$$\psi : \begin{cases} H \times L & \longrightarrow HL \\ (h, l) & \longmapsto hl \end{cases}$$

Montrer que ψ est bijectif et en déduire que $|HL| = |H| \times |L|$.

5. En déduire que pour tout $n \in \mathbb{N}^*$, si $n||G|$, alors il existe H un sous groupe de G tel que $|H| = n$.

Correction de l'exercice I.2. :

Soit e' l'élément neutre de H . Pour tout $a \in H$, on note a_g^{-1} un inverse à gauche de a , i.e. un élément de H tel que $a_g^{-1}a = e'$. Soit $a \in H$. On a

$$a_g^{-1}aa_g^{-1} = e'a_g^{-1} = a_g^{-1}$$

On a donc

$$a \cdot a_g^{-1} = e' \cdot a \cdot a_g^{-1} = (a_g^{-1})_g^{-1}a_g^{-1} \cdot a \cdot a_g^{-1} = (a_g^{-1})_g^{-1}a_g^{-1} = e'$$

a admet donc aussi un inverse à droite qui est forcément le même qu'à gauche et donc H est un groupe.

Correction de l'exercice I.7. :

$\rightarrow (\Rightarrow)$ Cette implication est évidente.

$\rightarrow (\Leftarrow)$ $*$ est associative sur H , il faut donc simplement vérifier l'existence de l'inverse dans H et l'élément neutre. Soit $a \in H$. H étant fini, on dispose de $i, j \in \mathbb{N}$ tels que $1 \leq i < j$ et $a^i = a^j$. Si $j = i + 1$ alors $a = e$ et donc $a^{-1} = e \in H$. Sinon, $j \geq i + 2$ et donc $b = a^{j-i-1} \in H$. Montrons que $b = a^{-1}$. On a

$$ba = a^{j-i-1}a = a^{j-i} = e = aa^{j-i-1} = ab$$

donc tout élément de H admet un inverse dans H pour $*$. L'existence de l'élément neutre vient simplement du fait que si $a \in H$, alors $a^{-1} \in H$ et alors $e = a * a^{-1} \in H$.

Correction de l'exercice I.11. :

Le fait que ce soit un morphisme est clair. En effet, pour tout $a, b \in G$ et $x \in G$, on a

$$\varphi(a * b)(x) = \gamma_{a * b}(x) = a * b * x = \gamma_a \circ \gamma_b(x) = \varphi(a) \circ \varphi(b)(x)$$

et alors $\varphi(a * b) = \varphi(a) \circ \varphi(b)$.

Montrons à présent que φ est injective. Pour cela, on va montrer que $\text{Ker } \varphi = \{\text{Id}\}$. Soit $a \in \text{Ker } \varphi$. On a $\varphi(a)(e) = e$ et donc $a \cdot e = e$ d'où $a = e$ et alors $\text{Ker } \varphi = \{e\}$.

Remarque : Le seul élément a de G tel que γ_a admet un point fixe est e .

Correction de l'exercice I.13. :

1. Montrons cette proposition par double implication.

$\rightarrow (\Rightarrow)$ Supposons que HK est un sous-groupe de G . On a alors

$$HK \underset{HK \leq G}{=} (HK)^{-1} = K^{-1}H^{-1} \underset{H \text{ et } K \leq G}{=} KH$$

La première égalité est due au fait qu'étant donné que HK est un sous-groupe de G , alors l'application $i : \begin{cases} HK & \longrightarrow HK \\ x & \longmapsto x^{-1} \end{cases}$ est bijective.

$\rightarrow (\Rightarrow)$ Supposons que $HK = KH$ utilisons la proposition I.4 pour montrer que HK est un sous-groupe de G . $HK \neq \emptyset$ il suffit donc de vérifier que

$$\forall (h, k, h', k') \in H \times K \times H \times K, (hk)(h'k')^{-1} \in HK$$

Méthode 1 (Rapide) : On a pour tout $(h, k, h', k') \in H \times K \times H \times K$,

$$(hk)(h'k')^{-1} = hkk'^{-1}h'^{-1} \underset{K \leq G}{\in} hKh'^{-1} \underset{H \leq G}{\subset} HKH \underset{HK = KH}{=} HHK \underset{H \leq G}{=} HK$$

Méthode 2 (Même chose mais en plus détaillé) : Soit $(h, k, h', k') \in H \times K \times H \times K$. On a $(hk)(h'k')^{-1} = \underbrace{hkh'^{-1}}_{\in HK=KH} h'^{-1}$. Il existe donc $(h'', k'') \in H \times K$ tel que $hkh'^{-1} = k''h''$, et alors on peut écrire $(hk)(h'k')^{-1} = k''h''h' \in KH = HK$.

2. Supposons que H est un sous-groupe distingué de G . Deux méthodes sont possibles.

→ **Méthode 1 :** On a pour tout $(h, k, h', k') \in H \times K \times H \times K$, $(hk)(h'k') = hkh'k' = hkh'k^{-1}kk'$. H est un sous-groupe distingué de G , donc $kh'k^{-1} \in H$. Il existe donc $h'' \in H$ tel que $kh'k^{-1} = h''$. On a donc $(hk)(h'k') = hh''k' \in HK$. De plus, HK est non vide, donc d'après l'exercice I.7, HK est bien un sous-groupe de G .

→ **Méthode 2 :** En utilisant la proposition VII.1, on peut écrire

$$HK = \bigcup_{k \in K} Hk \underset{HG}{=} \bigcup_{k \in K} kH = KH$$

3. Montrons le résultat par double implication.

→ (\Leftarrow) Soit $x \in H \cap K$. On a $f(x, e) = x = f(e, x)$ et donc, par injectivité, $x = e$.

→ (\Rightarrow) Supposons que $H \cap K = \{e\}$. f est surjective par définition. Soit $(h, k, h', k') \in H \times K \times H \times K$. On a

$$f(h, k) = f(h', k') \iff hk = h'k' \iff h'^{-1}h = k'k^{-1} \underset{H \cap K = \{e\}}{=} e \iff h = h' \text{ et } k = k'$$

donc f est bijective.

Remarque : Si les éléments de H et K ne commutaient pas entre eux, f ne serait pas forcément un morphisme.

4. Supposons que H et K sont des sous-groupes distingués de G et que $H \cap K = \{e\}$. Pour tout $(h, k, h', k') \in H \times K \times H \times K$, on a

$$hkh^{-1}k^{-1} \in hKh^{-1}k^{-1} \cap hkHk^{-1} \underset{H \text{ et } KG}{=} Kk^{-1} \cap hH \underset{H \text{ et } K \leq G}{=} K \cap H = \{e\}$$

et donc $hk = kh$

5. Supposons que les éléments de H et K commutent entre eux et que $H \cap K = \{e\}$. D'après la question 3, f est bijective. De plus, f est un morphisme (facile à vérifier) et donc un isomorphisme.

Correction de l'exercice IV.2. :

Notons $\bar{1}_{\mathbb{Z}/m\mathbb{Z}}$ la classe de 1 dans $\mathbb{Z}/m\mathbb{Z}$. Soit $f \in \text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$. On sait que $f(\bar{1}_{\mathbb{Z}/m\mathbb{Z}}) \in \mathbb{Z}/n\mathbb{Z}$ et donc $nf(\bar{1}_{\mathbb{Z}/m\mathbb{Z}}) = 0$. En particulier, $\omega(f(\bar{1}_{\mathbb{Z}/m\mathbb{Z}}))|n$. De même, $\omega(f(\bar{1}_{\mathbb{Z}/m\mathbb{Z}}))|\omega(\bar{1}_{\mathbb{Z}/m\mathbb{Z}}) = m$ et donc $\omega(f(\bar{1}_{\mathbb{Z}/m\mathbb{Z}}))|m \wedge n = 1$ i.e. $f(1) = 0$ et alors $f = 0$. On en déduit donc que $\text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \{0\}$.

Attention : La loi considérée ici est additive, donc pour tout $a \in \mathbb{Z}/m\mathbb{Z}$ (ou $\mathbb{Z}/n\mathbb{Z}$), on note $\omega(a) = \min\{k \geq 1, ka = 0\}$ au lieu de $\omega(a) = \min\{k \geq 1, a^k = 1\}$.

Correction de l'exercice IV.3. :

1. Considérons l'exemple où $(G, *) = (\text{GL}(\mathbb{R}^2), \circ)$. Soit $\theta, \theta' \in \mathbb{R}$ et $S_\theta, S_{\theta'}$ les symétries par rapport aux axes faisant respectivement un angle θ et θ' par rapport à l'axe des abscisses dans le sens trigonométrique. On rappelle que

$$S_\theta \circ S_{\theta'} = R_{\theta-\theta'}$$

où pour tout $\alpha \in \mathbb{R}$, R_α désigne la rotation d'angle α dans le sens trigonométrique dans \mathbb{R}^2 .

En particulier, si on prend θ et θ' vérifiant $\frac{\theta - \theta'}{2\pi} \in \mathbb{R} \setminus \mathbb{Q}$ alors

$$S_\theta^2 = \text{Id}, S_{\theta'}^2 = \text{Id} \text{ et } \forall n \in \mathbb{N}, R_{\theta-\theta'}^n = R_{n(\theta-\theta')}$$

Pour tout $n \in \mathbb{N}$, $n(\theta - \theta') \notin 2\pi\mathbb{Z}$ car $\frac{\theta - \theta'}{2\pi} \notin \mathbb{Q}$ et alors $R_{n(\theta-\theta')} \neq \text{Id}$. On en déduit donc que S_θ et $S_{\theta'}$ sont d'ordre 2 mais leur produit est d'ordre infini.

2. On a $(ab)^{mn} = (a^m)^n(b^n)^m = e$, donc ab est d'ordre fini et $\omega(ab)|mn$. Posons $l = \omega(ab)$. Remarquons maintenant que $(ab)^l = e$ et donc $(ab)^{lm} = e = (a^m)^l b^{lm} = b^{lm}$ d'où $n|ml$ et donc par Gauß, étant donné que $m \wedge n = 1$, on a $n|l$. On peut montrer de la même manière que $m|l$ et donc, vu que $m \wedge n = 1$, on a $mn|l$ et finalement $l = mn$.
3. Décomposons m et n en facteurs premiers. Soit $r \in \mathbb{N}$, p_1, \dots, p_r des nombres premiers distincts et $\alpha_1, \dots, \alpha_r \in \mathbb{N}$, $\beta_1, \dots, \beta_r \in \mathbb{N}$ tels que

$$m = p_1^{\alpha_1} \dots p_r^{\alpha_r} \text{ et } n = p_1^{\beta_1} \dots p_r^{\beta_r}$$

Quitte à réordonner les p_i , supposons sans perte de généralité qu'il existe $k \in \llbracket 1; r \rrbracket$ tel que

$$\forall i \in \llbracket 1; k \rrbracket, \max(\alpha_i, \beta_i) = \alpha_i \text{ et } \forall i \in \llbracket k+1; r \rrbracket, \max(\alpha_i, \beta_i) = \beta_i$$

posons ensuite

$$m' = p_{k+1}^{\alpha_{k+1}} \dots p_r^{\alpha_r}, \quad n' = p_1^{\beta_1} \dots p_k^{\beta_k}, \quad a' = a^{m'} \text{ et } b' = b^{n'}$$

On a alors $\omega(a') = \frac{m}{m'}$ et $\omega(b') = \frac{n}{n'}$ ce qui donne

$$\omega(a') \wedge \omega(b') = \frac{n \wedge m}{n' m'} = \frac{n \wedge m}{p_1^{\min(\alpha_1, \beta_1)} \dots p_r^{\min(\alpha_r, \beta_r)}} = \frac{n \wedge m}{n \wedge m} = 1$$

et donc d'après la question précédente

$$\omega(a'b') = \omega(a')\omega(b') = \frac{mn}{m'n'} = \frac{mn}{m \wedge n} = m \vee n$$

4. Posons $S = \{\omega(x), x \in G\}$. Étant donné que S est fini non vide, on peut, en utilisant la question précédente, trouver un élément $z \in G$ tel que $\omega(z) = \bigvee_{m \in S} m$ qui vérifie bien la propriété voulue.

Correction de l'exercice V.4. :

On envisage deux méthodes.

→ **Méthode 1 (plus intuitive)** : H est un sous-groupe de G qui est généré par a , donc tout élément de H s'écrit sous forme de a^l avec $l \in \mathbb{N}$. Soit $l = \min\{k \in \mathbb{N}^*, a^k \in H\}$. Montrons que $\langle a^l \rangle = H$. Supposons le contraire, i.e. qu'il existe $m \in \mathbb{N}$ tel que $a^m \notin \langle a^l \rangle$ et $a^m \in H$. On peut donc écrire $m = ql + r$ avec $q \in \mathbb{Z}$ et $r \in \llbracket 0; l-1 \rrbracket$ (car k ne divise pas m). On a alors

$$a^r = a^{-ql} a^{ql+r} = (a^l)^{-q} a^m \in H$$

ce qui est absurde par définition de l . On en déduit donc que $H = \langle a^l \rangle$. D'après la proposition IV.4, $\omega a^l | H$, on a alors $(a^l)^d = e$ et donc $a^{dl} = e$. D'après le point 1 de la proposition 1, on a $n|dl$. De plus, d'après la proposition IV.4, H étant un sous-groupe cyclique de G , on a $d|n$ et donc $\frac{n}{d}|l$. Posons donc $l = \alpha \frac{n}{d}$ avec $\alpha \in \mathbb{N}$. On a alors

$$H = \langle a^l \rangle = \langle a^{\alpha \frac{n}{d}} \rangle \subset \langle a^{\frac{n}{d}} \rangle$$

On a de plus d'après le point 5 de la proposition III.1, $|\langle a^{\frac{n}{d}} \rangle| = \frac{n}{n/d} = d = |H|$ et donc $|H| = \langle a^{\frac{n}{d}} \rangle$.

→ **Méthode 2 (plus rapide)** : a est un générateur de G donc l'application $\varphi : \begin{cases} \mathbb{Z} & \longrightarrow G \\ k & \longmapsto a^k \end{cases}$ est surjective et $\text{Ker } \varphi = n\mathbb{Z}$. On a donc $H = \varphi(\varphi^{-1}(H))$ et d'après la proposition I.9, $\varphi^{-1}(H)$ est un sous-groupe de \mathbb{Z} , i.e. de la forme $k\mathbb{Z}$ avec $k \in \mathbb{N}$. De plus, $\{e\} \subset H$ et donc

$$n\mathbb{Z} = \varphi^{-1}(\{e\}) \subset \varphi^{-1}(H) = k\mathbb{Z}$$

On en déduit alors que $k|n$ et que

$$H = \varphi(k\mathbb{Z}) = \{a^l, l \in k\mathbb{Z}\} = \langle a^k \rangle$$

De plus, $d = |H| = |\langle a^k \rangle| = \frac{n}{k}$ et donc $k = \frac{n}{d}$ et finalement $H = \langle a^{\frac{n}{d}} \rangle$.

Correction de l'exercice V.5. :

1. Soit $k \in \mathbb{Z}$. D'après le point (4) de la proposition III.1, on a $\omega(a^k) = \frac{\omega(a)}{\omega(a) \wedge k} = \frac{n}{n \wedge k}$. On en déduit donc que

$$G = \langle a^k \rangle \iff \omega(a^k) = n \iff \frac{n}{n \wedge k} = n \iff n \wedge k = 1$$

2. On envisage deux méthodes.

→ **Méthode 1** : Notons pour tout $d \in \mathbb{N}^*$ diviseur de n $G_d = \{b \in G, \omega(b) = d\}$. On sait que d'après l'exercice V.4, pour tout d diviseur positif de n , tout sous-groupe de cardinal d est égal à $H_d = \langle a^{\frac{n}{d}} \rangle$. On a donc

$$b \in G_d \iff |\langle b \rangle| = d \iff \langle b \rangle = H_d$$

On a donc pour tout d diviseur positif de n ,

$$\begin{aligned} |G_d| &= |\{b \in G, \omega(b) = d\}| \\ &= \left| \left\{ \left(a^{\frac{n}{d}} \right)^k, k \in \mathbb{N}, \langle a^{\frac{kd}{n}} \rangle = H_d \right\} \right| \\ &= |\{k \in \llbracket 1; d \rrbracket, k \wedge d = 1\}| = \varphi(d) \end{aligned}$$

L'avant dernière égalité est due au fait que $a^{\frac{n}{d}}$ est un générateur de H_d et donc d'après la question précédente $\left(a^{\frac{n}{d}} \right)^k$ génère H_d si et seulement si $k \wedge d = 1$. On a alors

$$n = |G| = \left| \bigsqcup_{d|n, d \geq 1} G_d \right| = \sum_{d|n, d \geq 1} |G_d| = \sum_{d|n, d \geq 1} \varphi(d)$$

→ **Méthode 2 :** On a

$$\begin{aligned}
 n = |\llbracket 1; n \rrbracket| &= \left| \bigsqcup_{d|n, d \geq 1} \{k \in \llbracket 1; n \rrbracket \mid k \wedge n = d\} \right| \\
 &= \sum_{d|n, d \geq 1} |\{k \in \llbracket 1; n \rrbracket \mid k \wedge n = d\}| \\
 &= \sum_{d|n, d \geq 1} \left| \left\{ k \in d \times \llbracket 1; \frac{n}{d} \rrbracket, \frac{k}{d} \wedge \frac{n}{d} = 1 \right\} \right| \\
 &= \sum_{d|n, d \geq 1} \left| \left\{ k \in \llbracket 1; \frac{n}{d} \rrbracket, k \wedge \frac{n}{d} = 1 \right\} \right| \\
 &= \sum_{d|n, d \geq 1} \varphi\left(\frac{n}{d}\right) = \sum_{d|n, d \geq 1} \varphi(d)
 \end{aligned}$$

La dernière égalité est vraie car

$$h : \begin{cases} \{d \geq 1, d|n\} & \longrightarrow \{d \geq 1, d|n\} \\ d & \longmapsto \frac{n}{d} \end{cases}$$

est une bijection.

Correction de l'exercice V.6. :

1. Notons $n = |G_1|$, $m = |G_2|$ et a, b des générateurs de G_1 et G_2 respectivement. On note également e_1 et e_2 les éléments neutres respectifs de $(G_1, *)$ et $(G_2, *)$. On envisage deux cas possibles.

→ **Cas 1 : $n \wedge m = 1$.**

Soit $z = (a, b) = (e_1, b) \otimes (a, e_2)$. On a clairement $\omega((a, e_2)) = n$ et $\omega((e_1, b)) = m$ donc d'après l'exercice IV.3. $\omega(z) = mn$ et donc étant donné que $|G_1 \times G_2| = mn$, alors $G_1 \times G_2 = \langle z \rangle$, i.e. $(G_1 \times G_2, \otimes)$ est cyclique.

→ **Cas 2 : $n \wedge m \neq 1$.**

Posons alors $l = n \vee m$. Il est clair que $\forall z \in G_1 \times G_2, z^l = (e_1, e_2)$ et donc $G_1 \times G_2$ ne peut pas être cyclique car pour tout $z \in G$, $|\langle z \rangle| \leq l < mn = |G_1 \times G_2|$.

On en déduit donc que $G_1 \times G_2$ est cyclique si et seulement si $|G_1| \wedge |G_2| = 1$.

2. Pour vérifier que f est bien définie, il faut vérifier que tout élément de $\mathbb{Z}/ab\mathbb{Z}$ a une image unique par f . On doit donc vérifier que pour tout $x, y \in \mathbb{Z}$, si dans $\mathbb{Z}/ab\mathbb{Z}$ on a $\bar{x} = \bar{y}$, alors $\varphi(\bar{x}) = \varphi(\bar{y})$. Notons pour tout $z \in \mathbb{Z}$ et $r \geq 2$, $\bar{z}_{(r)}$ la classe de z dans $\mathbb{Z}/r\mathbb{Z}$.

Considérons donc $x, y \in \mathbb{Z}$ tels que dans $\mathbb{Z}/ab\mathbb{Z}$, on ait $\bar{x} = \bar{y}$. Il existe donc $k \in \mathbb{Z}$ tel que $x = y + kab$. On a alors

$$\varphi(\bar{x}_{(ab)}) = (\bar{x}_{(a)}, \bar{x}_{(b)}) = (\bar{y}_{(a)} + \overline{kab}_{(a)}, \bar{y}_{(b)} + \overline{kab}_{(b)}) = (\bar{y}_{(a)}, \bar{y}_{(b)}) = \varphi(\bar{y}_{(ab)})$$

φ est donc bien définie. Il est également facile de vérifier qu'il s'agit d'un morphisme. Montrons maintenant qu'il s'agit d'un isomorphisme si et seulement si $a \wedge b = 1$.

→ (\Leftarrow) Supposons que $a \wedge b = 1$. On a $\varphi(\bar{1}_{(ab)}) = (\bar{1}_{(a)}, \bar{1}_{(b)})$. D'après la question 1, étant donné que $\bar{1}_{(a)}$ et $\bar{1}_{(b)}$ sont d'ordre respectivement a et b et $a \wedge b = 1$, alors $\omega((\bar{1}_{(a)}, \bar{1}_{(b)})) = ab$. On a de plus

$$\langle (\bar{1}_{(a)}, \bar{1}_{(b)}) \rangle = \langle \varphi(\bar{1}_{(ab)}) \rangle \subset \text{Im } \varphi$$

et donc

$$|\text{Im } \varphi| \geq |\langle (\bar{1}_{(a)}, \bar{1}_{(b)}) \rangle| = ab$$

or $|\text{Im } \varphi| \leq |\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}| = ab$, donc $|\text{Im } \varphi| = ab$ et alors $\text{Im } \varphi = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, i.e. φ est surjective. De plus, on a $|\mathbb{Z}/ab\mathbb{Z}| = ab = |\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}|$ donc la surjectivité de φ nous donne directement que φ est bijective, c'est donc un isomorphisme.

→ (\Rightarrow) Supposons que $a \wedge b = d > 1$. On a alors $a \vee b \in]0, ab[$ et donc $\overline{a \vee b}_{(ab)} \neq \overline{0}_{(ab)}$, mais

$$\varphi(\overline{a \vee b}_{(ab)}) = (\overline{a \vee b}_{(a)}, \overline{a \vee b}_{(b)}) = (\overline{0}_{(a)}, \overline{0}_{(b)})$$

On en déduit que $\text{Ker } \varphi \neq \{\overline{0}_{(ab)}\}$ et que donc φ n'est pas injective. φ ne peut donc pas être un isomorphisme.

Correction de l'exercice V.7. :

- Soit $P \in A[X]$ et $Q \in A[X]$ de coefficient dominant égal à 1. Il s'agit de montrer la proposition suivante

$$\exists! B, R \in A[X], P(X) = B(X)Q(X) + R(X), \deg R < \deg Q$$

→ **Existence :** Procédons par récurrence forte sur le degré de P . Posons $n = \deg P$.

- Si $\deg P = 0$, alors si $\deg Q > 0$, $B = 0$ et $R = P$ conviennent. si $\deg Q = 0$ i.e. $Q = 1$, alors $R = 0$ et $B = P$ conviennent.
- Soit $n \in \mathbb{N}$. Supposons que la propriété est vraie pour tout n , i.e. pour tout polynôme P de degré inférieur ou égal à n ,

$$\exists B, R \in A[X], P(X) = B(X)Q(X) + R(X), \deg R < \deg Q$$

Montrons que la propriété est vraie pour $n + 1$. On suppose que P est de degré $n + 1$ et on pose

$$P(X) = \sum_{k=0}^{n+1} a_k X^k \text{ et } Q(X) = X^r + H(X)$$

avec $r = \deg Q$ et $H \in A[X]$ tel que $\deg H < r$. Si $r > n + 1$, alors $B = 0$ et $R = Q$ conviennent. Si $r \leq n + 1$ on a alors

$$P(X) - a_{n+1}X^{n+1-r}Q(X) = \sum_{k=0}^n a_k X^k - a_{n+1}X^{n+1-r}H(X)$$

On a donc

$$\deg(P(X) - a_{n+1}X^{n+1-r}Q(X)) = \deg \left(\sum_{k=0}^n a_k X^k - a_{n+1}X^{n+1-r}H(X) \right) \leq n$$

Par hypothèse de récurrence, il existe $\tilde{B}, \tilde{R} \in A[X]$ tels que $\deg \tilde{R} < \deg Q$ tels que

$$P(X) - a_{n+1}X^{n+1-r}Q(X) = \tilde{B}(X)Q(X) + \tilde{R}(X)$$

et alors on a

$$P(X) = (\tilde{B}(X) + a_{n+1}X^{n+1-r})Q(X) + R(X)$$

on en déduit que $B(X) = \tilde{B}(X) + a_{n+1}X^{n+1-r}$ et $R(X) = \tilde{R}(X)$ conviennent, d'où l'existence.

→ **Unicité :** Soit $B_1, B_2, R_1, R_2 \in A[X]$ tels que $\deg R_1 \leq \deg Q$, $\deg R_2 \leq \deg Q$ et

$$P(X) = B_1(X)Q(X) + R_1(X) = B_2(X)Q(X) + R_2(X)$$

On a alors

$$(B_1(X) - B_2(X))Q(X) = R_1(X) - R_2(X)$$

Si $B_1 - B_2 \neq 0$, alors étant donné que Q est non nul, on a

$$\deg(R_1 - R_2) = \deg((B_1 - B_2)Q) \quad (1)$$

$$= \deg((B_1 - B_2)X^r + (B_1 - B_2)H)) \quad (2)$$

$$= \deg(B_1 - B_2) + \deg Q \geq \deg Q \quad (3)$$

ce qui est absurde. On en déduit que $B_1 = B_2$ et que $R_1 = R_2$, d'où l'unicité.

Attention : Lorsque $U, V \in A[X]$ et que A n'est pas intègre, on a pas forcément l'égalité $\deg(UV) = \deg U + \deg V$, mais ici, on peut passer de la ligne (2) à (3) car le coefficient dominant de Q est égal à 1. Ce passage serait également vrai si le coefficient dominant de Q n'est pas un diviseur de zéro.

2. Montrons ce résultat par récurrence sur le degré de P encore une fois.

- Lorsque $\deg P = 0$, P n'a clairement pas de racines (le cas $P = 0$ correspond à $\deg P = -\infty$).
- Soit $n \in \mathbb{N}$. Supposons que la propriété est vraie lorsque $\deg P \in \llbracket 0; n \rrbracket$ et supposons maintenant que $\deg P = n + 1$. Si P n'admet pas de racines, la propriété est vraie. Supposons que P admet une racine $a \in A$. La question précédente nous permet d'effectuer la division euclidienne de P par $X - a$ (ce polynôme est de coefficient dominant égal à 1). Il existe donc $B, R \in A[X]$ tel que

$$\deg R < \deg(X - a) = 1 \text{ et } P(X) = (X - a)B(X) + R(X)$$

On a de plus $0 = P(a) = R(a)$ et R est constant donc $R = 0$. B est de degré n , donc par hypothèse de récurrence, B admet au plus n racines et donc $P(X) = (X - a)B(X)$ admet au plus $n + 1 = \deg P$ racines.

3. Si G est cyclique, alors nécessairement on a $|G| = \bigvee_{x \in G} \omega(x)$. Notre intuition est donc de considérer un élément de G d'ordre le plus grand qu'on peut trouver (ici égal à n) et d'essayer de montrer qu'il engendre G . Posons $n = \bigvee_{x \in G} \omega(x)$. D'après la question 4 de l'exercice IV.3, il existe $z \in G$ tel

que $\omega(z) = \bigvee_{x \in G} \omega(x) = n$. n est un multiple de tous les ordres des éléments de G , donc pour tout $x \in G$, $x^n = 1$. On posant Z l'ensemble des racines de $X^n - 1$ dans \mathbb{K} , on voit que $G \subset Z$. D'après la question précédente, le polynôme $X^n - 1$ admet au plus n racines, donc on a $|G| \leq |Z| \leq n$. De plus, on a $n = |\langle z \rangle| \leq |G|$ et donc $|G| = n = |\langle z \rangle|$ et $\langle z \rangle \subset G$, et finalement $G = \langle z \rangle$, i.e. G est cyclique.

Correction de l'exercice VI.2. :

On peut voir G comme un $\mathbb{Z}/p\mathbb{Z}$ -espace vectoriel. En effet, en considérant les lois (bien définies)

$$+ : \begin{cases} G \times G & \longrightarrow G \\ (x, y) & \longmapsto x * y \end{cases} \text{ et } : \begin{cases} \mathbb{Z}/p\mathbb{Z} \times G & \longrightarrow G \\ (\bar{k}, x) & \longmapsto x^k \end{cases}$$

on peut voir que $(G, +, \cdot)$ est un $\mathbb{Z}/p\mathbb{Z}$ -espace vectoriel. G est fini et donc de dimension finie. En posant $n = \dim_{\mathbb{Z}/p\mathbb{Z}} G$, on peut affirmer l'existence d'une base de G , (x_1, \dots, x_n) . On peut donc affirmer que tout $x \in G$ s'écrit d'une manière unique sous forme de

$$x = \overline{k_1} \cdot x_1 + \cdots + \overline{k_n} \cdot x_n, \quad \overline{k_1}, \dots, \overline{k_n} \in \mathbb{Z}/p\mathbb{Z}$$

En considérant donc l'isomorphisme (il est facile de montrer qu'il est bien défini et qu'il s'agit d'un isomorphisme)

$$\varphi : \begin{cases} G & \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n \\ \overline{k_1}x_1 + \cdots + \overline{k_n}x_n & \longmapsto (\overline{k_1}, \dots, \overline{k_n}) \end{cases}$$

On voit donc que $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$. En particulier, on remarquera que $|G| = |\mathbb{Z}/p\mathbb{Z}|^n = p^n$.

Remarque : En utilisant le théorème de Cauchy (VII.14), on peut très facilement montrer qu'il existe $n \in \mathbb{N}^*$ tel que $|G| = p^n$. En effet, pour tout $g \in G \setminus \{e\}$, $g^p = e$ et donc $\omega(g)|p$ i.e. $\omega(g) = p$. Pour tout nombre premier q , si $q | |G|$, alors par le théorème de Cauchy il existe $g \in G$ tel que $\omega(g) = q$ et alors $q = p$. p est donc le seul nombre premier qui divise $|G|$ ce qui signifie qu'il existe $n \in \mathbb{N}^*$ tel que $|G| = p^n$.

Correction de l'exercice VI.3. :

Montrons le résultat par implications successives.

$\rightarrow (1) \Rightarrow (2)$ Montrer que $H \simeq \mathbb{Z}/p\mathbb{Z}$ est équivalent à montrer que H est engendré par un élément d'ordre p premier. En effet, s'il existe $x \in H$ tel que $\langle x \rangle = G$ et $\omega(x) = p \in \mathbb{P}$, alors il est facile de montrer que l'application $\psi : \begin{cases} H & \longrightarrow \mathbb{Z}/p\mathbb{Z} \\ x^k & \longmapsto \bar{k} \end{cases}$ est bien définie et est un isomorphisme et que donc en particulier $H \simeq \mathbb{Z}/p\mathbb{Z}$.

Montrons maintenant que G est engendré par un élément d'ordre premier. Soit $x \in G \setminus \{e\}$. $\langle x \rangle \in \text{Sg}(H) \setminus \{\{e\}\}$ et donc $\langle x \rangle = H$. Montrons que $\omega(x)$ est premier.

Si $\omega(x) = \infty$, alors $\langle x^2 \rangle$ est un sous-groupe de G . Il est facile de vérifier que $\langle x^2 \rangle \neq \langle x \rangle$ et alors on a $\langle x^2 \rangle = \{e\}$, i.e. $\omega(x) \leq 2$ ce qui est en contradiction avec le fait que $\omega(x) = \infty$. On en déduit donc que $\omega(x)$ est fini.

Soit d un diviseur de $\omega(x)$ supérieur ou égal à 2. D'après la proposition III.1, on a $\omega(x^d) = \frac{\omega(x)}{d}$ ce qui donne nécessairement $\langle x^d \rangle \in \text{Sg}(H) \setminus \{H\}$ et donc $\langle x^d \rangle = \{e\}$, ce qui signifie que $x^d = e$, et alors encore d'après la proposition III.1 $\omega(x)|d$ et finalement $d = \omega(x)$. On en déduit donc que les seuls diviseurs positifs de $\omega(x)$ sont 1 et $\omega(x)$, i.e. que $\omega(x)$ est premier (ou égal à 1, mais ce cas est impossible car $x \neq e$). En posant $p = \omega(x)$, on en déduit d'après ce qui précède que $H \simeq \mathbb{Z}/p\mathbb{Z}$ avec p premier.

$\rightarrow (2) \Rightarrow (3)$ Si $H \simeq \mathbb{Z}/p\mathbb{Z}$, alors et $|G| = |\mathbb{Z}/p\mathbb{Z}| = p$, ce qui implique d'après le théorème de Lagrange faible (IV.4) que tout élément a de $H \setminus \{e\}$ divise p et donc $\omega(a) \in \{1, p\}$. On en déduit alors que pour tout $a \in H \setminus \{e\}$, $|\langle a \rangle| = \omega(a) = p = |H|$ i.e. $\langle a \rangle = H$, d'où le résultat.

$\rightarrow (3) \Rightarrow (4)$ G est monogène, on peut donc considérer $g \in G$ tel que $\langle g \rangle = G$. Deux cas se présentent.

- Si $\omega(g) = \infty$, on a par hypothèse $\langle g^2 \rangle = G$ ce qui est impossible. En effet, $g \notin \langle g^2 \rangle$ car sinon il existerait $k \in \mathbb{Z}$ tel que $g^{2k} = g$, i.e. $g^{2k-1} = e$ ce qui est absurde.
- Si $\omega(g) = n \in \mathbb{N}^*$, alors le morphisme

$$\psi' : \begin{cases} \mathbb{Z}/n\mathbb{Z} & \longrightarrow H \\ \bar{k} & \longmapsto g^k \end{cases}$$

est bien défini et est bijectif. On en déduit alors que $H \simeq \mathbb{Z}/n\mathbb{Z}$. De plus, si d est un diviseur positif de n différent de n , alors d'après le point 5 de la proposition III.1, $|\langle g^d \rangle| = \omega(g^d) = \frac{n}{d}$.

On a donc

$$\frac{n}{d} = \omega(g^d) = |\langle g^d \rangle| = |H| = n$$

et donc $d = 1$. On en déduit alors que les seuls diviseurs de n sont 1 et n , i.e. que n est premier et alors $|H| = |\mathbb{Z}/n\mathbb{Z}| = n \in \mathbb{P}$.

$\rightarrow (4) \Rightarrow (1)$ Soit L un sous-groupe de H . H est cyclique donc d'après le résultat de l'exercice V.4 L est également cyclique. On a donc d'après le théorème faible de Lagrange (IV.4) $|L| | |H|$, mais H est premier, donc $|L| \in \{1, |H|\}$ et finalement $\text{Sg}(H) = \{H, \{e\}\}$.

Correction de l'exercice VII.5. :

D'après le théorème faible de Lagrange (IV.4), l'ordre de tout élément de H divise pq et donc pour tout $a \in H \setminus \{e\}$, $\omega(a) \in \{p, q, pq\}$.

- Si tout élément de $H \setminus \{e\}$ est d'ordre p , alors d'après l'exercice VI.2, il existe $n \in \mathbb{N}$ tel que $|H| = p^n$ ce qui est absurde.
- De même, si tout élément de $H \setminus \{e\}$ est d'ordre q , alors il existe $n \in \mathbb{N}$ tel que $|H| = q^n$ ce qui est absurde.
- S'il existe un élément $a \in H$ d'ordre pq , alors $\langle a \rangle = H$ et donc d'après la proposition V.3, $H \simeq \mathbb{Z}/pq\mathbb{Z}$.
- S'il existe un élément $a \in H$ d'ordre p et un élément $b \in H$ d'ordre q , alors d'après la question 2 de l'exercice IV.3, $\omega(ab) = pq$ et donc $H = \langle ab \rangle$ et alors pour les mêmes raisons qu'au point précédent, on a $H \simeq \mathbb{Z}/pq\mathbb{Z}$.

D'après le théorème chinois (exercice V.6), on a $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ et finalement $H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Correction de l'exercice VII.6. :

On a par hypothèse $|G/H| = 2$ donc il y a deux classes à gauche. Soit $a \in G \setminus H$. On a $aH \neq H$, donc $G/H = \{H, aH\}$. De la même manière, G a deux classes à droite et donc étant donné que $Ha \neq H$, ces deux classes sont H et Ha . On a donc $G = aH \sqcup H = Ha \sqcup H$ et alors $aH = Ha = G \setminus H$. De même, lorsque $a \in H$, on a $aH = H = Ha$ et alors en déduit donc que H est bien un sous-groupe distingué de G . Montrons à présent que H contient tous les carrés. $|G/H| = 2$ donc l'ordre de tout élément de G/H divise 2, i.e. pour tout $x \in H$, $(xH)^2$ est égal à H , l'élément neutre du groupe G/H . On en déduit que pour tout $x \in G$, $H = xHxH = x^2H$ et alors $x^2 \in H$. H contient donc tous les carrés.

Correction de l'exercice VII.10. :

Intuition : Pour montrer que H est distingué, il faut et il suffit de montrer que pour tout $h \in H$ et $a \in G$, $haH = aH$. En effet, lorsque cela est vérifié, alors on a pour tout $a \in G$ et $h \in H$, $a^{-1}haH = a^{-1}aH = H$ et donc $a^{-1}ha \in H$. Ceci donne directement que $a^{-1}Ha = H$ ce qui signifie que H est un sous-groupe distingué de G .

Pour montrer que pour tout $h \in H$ et $a \in G$, $haH = H$, on va considérer une action de groupe \bullet telle que pour tout $h \in H$ et $a \in G$, $h \bullet aH = haH$.

Considérons donc l'action de groupe \bullet de H sur G/H définie par

$$\bullet : \begin{cases} H \times G/H & \longrightarrow G/H \\ (h, aH) & \longmapsto haH \end{cases}$$

Pour montrer que H est distingué, il suffit de montrer que pour tout $h \in H$ et $a \in G$, $haH = aH$, i.e. que $O(aH) = \{aH\}$. Soit $a \in G$. Supposons que $|O(aH)| \neq 1$. D'après le point 3 de la proposition VII.9, on a $|O(aH)| |H|$. De plus, par le théorème de Lagrange (VII.4), H étant un sous-groupe de G , on a $|H| | |G|$ et donc $|O(aH)| | |G|$. p étant le plus petit diviseur de $|G|$ strictement supérieur à 1, on en déduit que $|O(aH)| \geq p$. Remarquons de plus que pour tout $h \in H$, $h \bullet H = H$ et donc $O(H) = \{H\}$.

On a alors d'après le point 4 de la proposition VII.9, si R est l'ensemble des représentants des orbites de l'action \bullet de H sur G/H , alors

$$p = |G/H| = \sum_{x \in R} |O(x)| \geq |O(H)| + |O(aH)| \geq p + 1$$

ce qui est absurde, donc $|O(aH)| = 1$ i.e. $O(aH) = \{aH\}$ donc H est bien un sous-groupe distingué de G .

Une version plus courte utilisant des notion plus avancées sera exposée dans un chapitre complément à

celui-ci qui sera publié plus-tard.

Correction de l'exercice VII.13. :

Soit R l'ensemble des représentants de classes de conjugaison de G non réduites à un singleton. En appliquant la formules des classes à G (point 3 de la proposition VII.12), on obtient

$$|Z(G)| = |G| - \sum_{x \in R} |O(x)| = |G| - \sum_{x \in R} \frac{|G|}{|C(x)|}$$

On a de plus pour tout $x \in R$, $\frac{|G|}{|C(x)|} \mid |G|$ et $|G| = p^n$, donc tous les diviseurs strictement positifs de $|G|$

sont de la forme p^k avec $k \in \llbracket 0; n \rrbracket$. De plus, pour tout $x \in R$, $\frac{|G|}{|C(x)|} = |O(x)| \neq 1$ et alors

$$\forall x \in R, \exists k \in \llbracket 1; n \rrbracket, \frac{|G|}{|C(x)|} = p^k$$

et donc

$$Z(G) \equiv p^n - \sum_{x \in R} \frac{|G|}{|C(x)|} \equiv 0[p]$$

De plus, $e \in Z(G)$ donc $Z(G) \geq p$. $Z(G)$ n'est alors pas réduit à un singleton.

Supposons à présent que $n \leq 2$ et montrons que G est abélien.

- Si $n = 1$, alors on a $p = |G| \geq |Z(G)| \geq p$ donc $|Z(G)| = p$ et alors $Z(G) = G$ i.e. G est abélien.
- Si $n = 2$, alors on sait que $Z(G)$ est un sous-groupe de G , donc par le théorème de Lagrange (VII.4), $|Z(G)| \mid |G|$ et donc $|Z(G)| = p$ ou $|Z(G)| = p^2$. Si $|Z(G)| = p^2$, alors on peut dire comme avant que $Z(G) = G$ et alors que G est abélien.

Soit $x \in G \setminus Z(G)$. On sait encore une fois, d'après le théorème de Lagrange (VII.4), que $|\langle x \rangle| \mid |G|$, et $x \neq e$, donc $|\langle x \rangle| \in \{p, p^2\}$. Si $|\langle x \rangle| = p^2$, alors $G = \langle x \rangle$ et on en déduit immédiatement que G est commutatif. Sinon, on a encore une fois d'après Lagrange $|\langle \{x\} \cup Z(G) \rangle| \in \{p, p^2\}$ et $|\langle \{x\} \cup Z(G) \rangle| > |\langle x \rangle| = p$ et donc $|\langle \{x\} \cup Z(G) \rangle| = p^2$ et alors $\langle \{x\} \cup Z(G) \rangle = G$. D'après la proposition VI.1, on peut écrire

$$G = \langle \{x\} \cup Z(G) \rangle = \{a_1^{\alpha_1} \dots a_n^{\alpha_n}, n \in \mathbb{N}, a_1, \dots, a_n \in \{x\} \cup Z(G), \alpha_1, \dots, \alpha_n \in \mathbb{Z}\}$$

il est facile de montrer que ce groupe est abélien, et donc on en déduit que G est abélien.

Correction de l'exercice VII.15. :

1. Soit $x \in G$ tel que $\omega(\bar{x}) = p$. En considérant le morphisme introduit à la proposition VII.3

$$\pi : \begin{cases} G & \longrightarrow G/K \\ x & \longmapsto \bar{x} = xK \end{cases}$$

on peut affirmer d'après le point 1 de la proposition IV.1 que $\omega(\pi(x)) \mid \omega(x)$ i.e. $p \mid \omega(x)$. On a alors d'après le point 5 de la proposition III.1, $\omega\left(x^{\frac{\omega(x)}{p}}\right) = \frac{\omega(x)}{\omega(x)/p} = p$.

2. Posons $G = kp$ avec $k \in \mathbb{N}^*$ et procédons par récurrence forte sur k

→ Si $k = 1$, alors $|G| = p$, alors la propriété est vraie d'après l'exercice VI.3.

→ Soit $k \in \mathbb{N}$, supposons que pour tout $l \in \llbracket 1; k \rrbracket$, si $|G| = lp$, alors G vérifie la propriété voulue. Supposons maintenant que $|G| = (k+1)p$ et montrons qu'il existe un élément de G d'ordre p .

Soit $x \in G \setminus \{e\}$.

- Si $p|\omega(x)$, alors encore une fois, d'après le point 5 de la proposition III.1,

$$\omega\left(x^{\frac{\omega(x)}{p}}\right) = \frac{\omega(x)}{\omega(x)/p} = p$$

- Si $p \nmid \omega(x)$, alors on a $|G/\langle x \rangle| = \frac{|G|}{\omega(x)} = \frac{k+1}{\omega(x)}p$ et $\frac{k+1}{\omega(x)} \in \llbracket 1; k \rrbracket$ (bien entendu, $\frac{k+1}{\omega(x)} \in \mathbb{N}$ car étant donné que $\omega(x) \wedge p = 1$, d'après Gauss $\omega(x)|k+1$). On en déduit alors par hypothèse de récurrence qu'il existe $y \in G/\langle x \rangle$ tel que $\omega(y) = p$ et alors d'après la question 1, il existe $z \in G$ tel que $\omega(z) = p$ ce qui bien le résultat voulu.

3. Procédons par récurrence forte sur a .

- Lorsque $a = 1$, la propriété est vraie d'après la question précédente.
- Soit m le plus grand entier tel que $p^m| |G|$ et soit $k \in \llbracket 1; m-1 \rrbracket$. Supposons que le résultat est vrai pour tout $a \in \llbracket 1; k \rrbracket$ et montrons qu'il est également vrai pour $a = k+1$. Par hypothèse de récurrence, il existe H sous-groupe de G tel que $|H| = p^k$. On a alors $|G/H| = |G|/p^k$ et $k \leq m-1$ donc $p| |G/H|$. On sait donc d'après la question précédente (qui donne le résultat pour $a = 1$) qu'il existe M un sous-groupe de G/H tel que $|M| = p$. Considérons l'endomorphisme (identique à celui considéré à la question 1)

$$\pi : \begin{cases} G & \longrightarrow G/H \\ x & \longmapsto xH \end{cases}$$

et en posant $L = \pi^{-1}(M)$ (c'est un groupe) et considérant le morphisme de groupe

$$\tilde{\pi} : \begin{cases} L & \longrightarrow M \cap \text{Im } \pi \\ x & \longmapsto \pi(x) \end{cases}$$

π est surjective par définition, donc $M \cap \text{Im } \pi = M$. On a de plus d'après la proposition VII.3,

$$L / \text{Ker } \tilde{\pi} \simeq \text{Im } \tilde{\pi} \tag{4}$$

On a de plus, M est un sous-groupe de G/H et contient donc son élément neutre H , et alors

$$H = \text{Ker } \pi = \pi^{-1}(\{H\}) \subset \pi^{-1}(M) = L$$

et alors

$$\text{Ker } \tilde{\pi} = L \cap \text{Ker } \pi = \text{Ker } \pi = H$$

et donc $\text{Ker } \tilde{\pi} = \text{Ker } \pi$. De plus, on a également

$$\text{Im } \tilde{\pi} = \pi(L) = \pi(\pi^{-1}(M)) = M \cap \text{Im } \pi \underset{\pi \text{ surjective}}{=} M \cap G/H = M$$

et donc on peut réécrire l'égalité (1) comme $L/H = M$ ce qui donne

$$|L| = |H| \times |M| = p^k \times p = p^{k+1}$$

L est donc un sous-groupe de G de cardinal p^{k+1} , ce qui est bien le résultat voulu.

4. D'abord, par commutation, $HL = LH$ et donc ce dernier est bien un sous-groupe de G (voir question 1 exercice I.13). De même, par commutation, ψ est bien un morphisme de groupes. Montrons maintenant que ψ est injective. On envisage deux méthodes.

→ **Méthode 1 (à la main)** : Soit $(h, l) \in \text{Ker } \psi$. On a alors $hl = e$. Posons $p = \omega(h)$ et $q = \omega(l)$. D'après le théorème de Lagrange, on a $p \mid |H|$ et $q \mid |L|$. De plus, on a $|H| \wedge L = 1$ ce qui donne $p \wedge q = 1$. On a alors d'après Bezout, il existe $u, v \in \mathbb{Z}$ tels que $up + vq = 1$. On a alors

$$e = (hl)^{vq} = h^{1-up}l^{vq} = h \text{ et } e = (hl)^{up} = h^{up}l^{1-vq} = l$$

et donc $(h, l) = (e, e)$. On en déduit donc que $\text{Ker } \psi = \{(e, e)\}$ et que donc ψ est injective.

→ **Méthode 2** : Soit $(h, l) \in \text{Ker } \psi$. On a alors $hl = e$ et donc $h = l^{-1} \in H \cap L$.

Or, $H \cap L \leq H$ et $H \cap L \leq L$ et donc, par Lagrange, $|H \cap L| \mid |H| \wedge |L| = 1$ i.e. $H \cap L = \{e\}$.

Ainsi, $h = l = e$ et donc ψ est injective.

ψ est clairement surjective donc bijective et donc $|HL| = |H \times L| = |H| \times |L|$.

5. On peut montrer facilement par récurrence en utilisant la question précédente le résultat suivant. Pour tout $r \in \mathbb{N}^*$, si H_1, \dots, H_r sont r sous-groupes de G tels que pour tout $i, j \in \llbracket 1; r \rrbracket$ différents, $|H_i| \wedge |H_j| = 1$, alors $H_1 \dots H_r$ est un sous-groupe de G et

$$|H_1 \dots H_r| = |H_1| \times \dots \times |H_r|$$

Écrivons maintenant la décomposition en produits de nombres premiers de n ($n = 1$ étant trivial). Soit $r \in \mathbb{N}^*$, $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$ et p_1, \dots, p_r r nombres premiers distincts tels que $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. D'après la question 3, pour tout $k \in \llbracket 1; r \rrbracket$, il existe H_k un sous groupe de G tel que $|H_k| = p_k^{\alpha_k}$. De plus, on a clairement pour tout $i, j \in \llbracket 1; r \rrbracket$ différents $|H_i| \wedge |H_j| = 1$ et alors on en déduit que $H_1 \dots H_r$ est un sous-groupe de G et que $|H_1 \dots H_r| = p_1^{\alpha_1} \dots p_r^{\alpha_r} = n$.



Polynômes

Notations

Soit \mathbb{K} un corps et $P \in \mathbb{K}[X]$.

- On note $Z_{\mathbb{K}}(P)$ l'ensemble des racines de P dans \mathbb{K} . Lorsqu'il n'y a pas ambiguïté sur \mathbb{K} , on note simplement $Z(P)$.
- On note $\text{val } P$ la valuation de P , c'est à dire le coefficient du terme de plus petit degré de P .

I Préambule

Dans tout le chapitre, \mathbb{K} désigne un corps.

Proposition I.1.

Soit $P \in \mathbb{K}[X]$:

1. Si $\deg P = 1$, alors P est irréductible.
2. Si $\deg(P) \in \{2, 3\}$, alors P est irréductible si et seulement s'il n'a pas de racine.

Preuve

1. Clair car si $P = QR$ et $\deg P = 1$ alors nécessairement Q ou R est constant.
2. Montrons les deux implications.

- (\Rightarrow) Si P est irréductible de degré $n \geq 2$, il est sans racine (s'il admet une racine a , $P = (X - a)Q$ avec Q non constant, absurde).
- (\Leftarrow) Procédons par contraposée. si $\deg P \in \{2, 3\}$ se factorise de manière non triviale, $P = QR$ avec $1 \leq \deg Q \leq \deg R$ et $\deg P = \deg Q + \deg R$, donc $1 \leq \deg Q \leq \frac{\deg(P)}{2} \leq 1.5$, donc $\deg Q = 1$ et Q admet une racine dans \mathbb{K} et finalement P aussi.

Contre exemple : Pour $\deg P \geq 4$, la propriété (2) n'est plus vraie. En effet, $X^4 + 1$ dans $\mathbb{R}[X]$ est réductible car sa factorisation dans $\mathbb{R}[X]$ est $(X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$ mais n'admet pas de racine dans \mathbb{R} .

Proposition I.2.

Si $\mathbb{K} \subset \mathbb{L}$ sont deux corps et $(A, B) \in (\mathbb{K}[X] - \{0\})^2$, alors $A \wedge B$ et $A \vee B$ sont les mêmes dans $\mathbb{L}[X]$ et dans $\mathbb{K}[X]$.

Preuve

- Pour $A \wedge B$: le calcul de cette quantité se fait par l'algorithme d'Euclide qui manipule des éléments de $\mathbb{K}[X]$. Tous ces éléments restent dans $\mathbb{K}[X]$ au fil des étapes de l'algorithme, donc le résultat de l'algorithme, i.e. $A \wedge B$, reste dans $\mathbb{K}[X]$.
- Pour $A \vee B$: $A \vee B = \frac{AB}{A \wedge B}$, il s'agit donc du rapport de deux éléments de $\mathbb{K}[X]$ et est de plus le même vu l'invariance de $A \wedge B$.

II Polynômes complexes

Théorème (Théorème de D'Alembert-Gauss) II.1.

les polynômes irréductibles de $\mathbb{C}[X]$ sont de degré 1. D'une manière équivalente, pour tout $P \in \mathbb{C}[X]$ non constant, il existe $\lambda_1, \dots, \lambda_n, a \in \mathbb{C}$ tels que

$$P(X) = a \prod_{i=1}^n (X - \lambda_i)$$

Preuve : La preuve de ce théorème dépasse le cadre de ce cours et ne sera donc pas faite.

Proposition II.2.

Soit $P, Q \in \mathbb{K}[X]$, $\lambda, \mu \in \mathbb{K}^*$ et $z_1, \dots, z_r \in \mathbb{K}$ distincts tels que

$$P(X) = \lambda \prod_{i=1}^r (X - z_i)^{\alpha_i} \text{ et } Q(X) = \mu \prod_{i=1}^r (X - z_i)^{\beta_i}$$

On a

$$P \wedge Q = \prod_{i=1}^r (X - z_i)^{\min(\alpha_i, \beta_i)} \text{ et } P \vee Q = \prod_{i=1}^r (X - z_i)^{\max(\alpha_i, \beta_i)}$$

Exemple : Pour tout $m, n \in \mathbb{N}^*$, on a, dans $\mathbb{C}[X]$, $X^m - 1 \wedge X^n - 1 = X^{m \wedge n} - 1$. En effet, on a

$$\begin{aligned} X^m - 1 \wedge X^n - 1 &= \prod_{\omega \in \mathbb{U}_m} (X - \omega) \wedge \prod_{\omega \in \mathbb{U}_n} (X - \omega) \\ &= \prod_{\omega \in \mathbb{U}_m \cap \mathbb{U}_n} (X - \omega) \\ &= \prod_{\omega \in \mathbb{U}_{m \wedge n}} (X - \omega) = X^{m \wedge n} - 1 \end{aligned}$$

Justifions le fait que $\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{n \wedge m}$.

- (\subset) Pour tout $z \in \mathbb{U}_{n \wedge m}$, on a $z^n = 1$ et $z^m = 1$ car $n \wedge m$ divise n et m .
- (\supset) D'après Bezout, il existe $a, b \in \mathbb{Z}$ tels que $am + bn = a \wedge b$, donc pour tout $z \in \mathbb{U}_n \cap \mathbb{U}_m$, on a $z^{n \wedge m} = (z^n)^a \cdot (z^m)^b = 1$, i.e. $z \in \mathbb{U}_{n \wedge m}$.

Proposition (Localisation des racines) II.3.

Soit $P \in \mathbb{C}_n[X]$ unitaire : $P = X^n + a_{n-1}X^{n-1} + \dots + a_0$. Pour tout $z \in \mathbb{C}$, si $P(z) = 0$, alors

$$|z| \leq 1 + \max_{k \in \llbracket 0; n \rrbracket} |a_k|$$

Preuve : La preuve de ce résultat a déjà été faite au chapitre 1.

Proposition II.4.

Pour toute suite $(P_k)_k$ à valeurs dans $\mathbb{C}_n[X]$, la suite de fonctions (P_k) converge simplement vers $P \in \mathbb{C}_n[X]$ si et seulement si les coefficients de (P_k) convergent vers ceux de P .

Preuve

CPGE
paradise

- (\Leftarrow) Supposons que les coefficients de (P_k) convergent vers ceux de P . Soit $a \in \mathbb{C}$. Il est facile de voir que $P_k(a) \xrightarrow{k \rightarrow +\infty} P(a)$ en passant à la limite.
- (\Rightarrow) Supposons que (P_k) converge simplement vers P . Soit $b_0, \dots, b_n \in \mathbb{C}$ deux à deux différents. Considérons les deux normes suivantes dans $\mathbb{C}_n[X]$

$$\| \cdot \|_{\infty, \text{coeff}} : \begin{cases} \mathbb{C}_n[X] & \longrightarrow \mathbb{R}^+ \\ P & \mapsto \max_{i \in \llbracket 0; n \rrbracket} |\alpha_i| \end{cases} \quad \| \cdot \| : \begin{cases} \mathbb{C}_n[X] & \longrightarrow \mathbb{R}^+ \\ P & \mapsto \sum_{i=0}^n |P(b_i)| \end{cases}$$

avec $P(X) = \alpha_n X^n + \dots + \alpha_1 X + \alpha_0$.

$\mathbb{C}_n[X]$ est de dimension finie, donc les normes $\| \cdot \|_{\infty, \text{coeff}}$ et $\| \cdot \|$ sont équivalentes. Le fait que (P_k) converge simplement vers P implique que (P_k) converge vers P pour $\| \cdot \|$ et donc par équivalence des normes, P_k converge vers P pour $\| \cdot \|_{\infty, \text{coeff}}$, i.e. les coefficients des termes de (P_k) convergent vers ceux de P .

Exercice II.5.

Soit $n \geq 1$ et $(P_k)_{k \in \mathbb{N}}$ une suite de polynômes unitaires de $\mathbb{C}_n[X]$. On suppose que (P_k) converge simplement vers $P \in \mathbb{C}_n[X]$ unitaire de degré n . Soit U un ouvert non vide de \mathbb{C} tel que U contient $l \in \mathbb{N}$ racines de P comptées avec multiplicité et qu'aucune racine de P n'est dans la frontière de U qu'on note $\partial U = \overline{U} \setminus U$. Montrer qu'il existe $K \in \mathbb{N}$ tel que pour tout $k \geq K$, U contient exactement l racines de P_k comptées avec multiplicité.

III Polynômes réels

Proposition III.1.

Les polynômes irréductibles (unitaires) de $\mathbb{R}[X]$ sont ceux de la forme

- $X - a$ avec $a \in \mathbb{R}$.
- $X^2 - aX + b$ avec $a, b \in \mathbb{R}$ et $\Delta = a^2 - 4b < 0$.

Preuve : Soit $P \in \mathbb{R}[X]$ unitaire non constant. Si $\deg P \geq 3$, alors deux cas se présentent.

- P admet une racine $z \in \mathbb{R}$, et alors P est réductible car il est divisible par $X - z$.
- P admet une racine $z \in \mathbb{C} \setminus \mathbb{R}$ et P est à coefficients réels, donc \bar{z} est aussi une racine de P . P est alors divisible par $(X - z)(X - \bar{z}) = X^2 - 2\operatorname{Re}(z)X + |z|^2 \in \mathbb{R}[X]$ et est donc réductible.

Si $\deg P = 1$, alors d'une manière évidente P s'écrit $X - a$ avec $a \in \mathbb{R}$ et est irréductible et si $\deg P = 2$, alors P est irréductible s'il n'admet pas de racine réelle, i.e. son discriminant est négatif.

Remarque : Les polynômes irréductibles de $\mathbb{R}[X]$ de degré 2 s'écrivent aussi de la forme $(X - a)^2 + b^2$ avec $a \in \mathbb{R}$ et $b > 0$.

Exercice III.2.

Montrer que tout polynôme $P \in \mathbb{R}[X]$ positif sur \mathbb{R} s'écrit de la forme $P = A^2 + B^2$ avec $A, B \in \mathbb{R}[X]$.

Proposition III.3.

Soit $P \in \mathbb{R}[X]$ non constant unitaire : $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$

1. Si P est scindé alors P' et $P + \alpha P'$, $\alpha \in \mathbb{R}$ aussi. Si P est dissocié (i.e. scindé à racines simples), P' aussi.
2. Si P est dissocié alors $\forall k \in \llbracket 0, n-1 \rrbracket$, $a_k^2 + a_{k+1}^2 > 0$.
3. Si P est scindé, alors $\forall k \in \llbracket 1, n-1 \rrbracket$, $a_k a_{k+2} \leq a_{k+1}^2$.
4. Si une suite $(P_k) \in \mathbb{R}_n[X]^{\mathbb{N}}$ de polynômes non constants unitaires scindés (pas forcément tous de même degré) converge simplement vers un polynôme $Q \in \mathbb{R}[X]$, alors Q est non constant et est scindé.

Preuve :

1. Montrons la propriété successivement pour P' et $P + \alpha P'$.

→ Si $a_1 < \cdots < a_r$ sont les racines de P de multiplicités respectives $\alpha_1, \dots, \alpha_r$, alors pour tout i , a_i est racine de P' de multiplicité $\alpha_i - 1$. On trouve ainsi $\alpha_1 + \cdots + \alpha_r - r = n - r$ racines de P' avec multiplicité. De plus, en appliquant le théorème de Rolle sur les segments $[a_i, a_{i+1}]$ on peut affirmer que P' s'annule en b_1, \dots, b_{r-1} tels que $a_1 < b_1 < a_2 < \cdots < a_{r-1} < b_{r-1} < a_r$, soit $r-1$ racines (simples) supplémentaires. On a donc un total de $n - r + r - 1 = n - 1$ racines de P' comptées avec multiplicité et P' est de degré $n-1$, donc P' est scindé. Cette preuve montre aussi que P' est dissocié si P l'est.

→ Soit $\alpha \in \mathbb{R}$. Si $\alpha = 0$ alors il s'agit du cas précédent. Sinon considérons $f : t \mapsto e^{\beta t}P(t)$ où $\beta = \frac{1}{\alpha}$. On a alors pour tout $t \in \mathbb{R}$,

$$f'(t) = 0 \iff e^{\beta t}(\beta P(t) + P'(t)) = 0 \iff P(t) + \alpha P'(t) = 0$$

Le reste est similaire à la discussion précédente : Si λ est racine de P de multiplicité $\delta \geq 1$ alors elle l'est dans $P + \alpha P'$ de multiplicité exactement $\delta - 1$. Pour retrouver les autres racines manquantes, il suffit d'appliquer Rolle à f entre chaque deux racines consécutives.

Remarquons au passage que cette propriété n'est pas vraie pour tout corps \mathbb{K} . En effet, lorsque $\mathbb{K} = \mathbb{Q}[\sqrt{6}]$ et $P(X) = X^3 - 6X$, on voit que P est scindé dans \mathbb{K} mais pas P' .

2. Supposons que P est dissocié. Procédons par l'absurde. Supposons qu'il existe $k \in \llbracket 0; n-1 \rrbracket$ tel que $a_k = a_{k+1} = 0$. On a alors

$$P^{(k)}(X) = k!a_k + (k+1)!a_{k+1}X + \frac{(k+2)!}{2}a_{k+2}X^2 + \cdots + \frac{n!}{(n-k)!}a_nX^{n-k}$$

0 est alors racine de multiplicité 2. De plus, P est dissocié et donc d'après la propriété précédente, $P^{(k)}$ aussi, ce qui est absurde. On en déduit donc que pour tout $k \in \llbracket 0; n-1 \rrbracket$, $a_k^2 + a_{k+1}^2 > 0$.

3. On sait que

$$\frac{P'}{P} = \sum_{i=1}^n \frac{1}{X - \lambda_i}$$

avec les $\lambda_1, \dots, \lambda_n$ les racines de P . Donc

$$\left(\frac{P'}{P} \right)' = - \sum_{i=1}^m \frac{1}{(X - \lambda_i)^2} \text{ et alors } \frac{P''P - P'^2}{P^2} \leq 0$$

sur $\mathbb{R} \setminus Z(P)$. On a alors en particulier, en le démontrant par la limite si $0 \in Z(P)$

$$P''(0)P(0) - P'(0)^2 \leq 0$$

On remplace P par $P^{(k)}$, également scindé et on trouve

$$P^{(k+2)}(0)P^{(k)}(0) \leq P^{(k+1)}(0)^2$$

soit

$$(k+2)!a_{k+2}k!a_k \leq (k+1)!^2 a_{k+1}^2 \quad \text{puis} \quad a_{k+2}a_k \leq \frac{k+1}{k+2}a_{k+1}^2 \leq a_{k+1}^2$$

d'où le résultat.

4. Soit $(P_k) \in \mathbb{R}_n[X]^{\mathbb{N}}$ une suite de polynômes non constants unitaires scindés convergeant simplement vers $Q \in \mathbb{R}[X]$. Posons pour tout $k \in \mathbb{N}$ et $z \in \mathbb{C}$,

$$P_k(z) = \prod_{j=1}^{\deg P_k} (z - a_{k,j})$$

On a alors pour tout $z \in \mathbb{C} \setminus \mathbb{R}$,

$$|P_k(z)| = \prod_{j=1}^{\deg P_k} |z - a_{k,j}| \geq |\operatorname{Im} z|^{\deg P_k} \geq \min(|\operatorname{Im} z|, |\operatorname{Im} z|^n)$$

En faisant tendre k vers l'infini, on obtient

$$|Q(z)| \geq \min(|\operatorname{Im} z|^n, |\operatorname{Im} z|) > 0$$

Q est donc soit constant soit scindé dans \mathbb{R} (il n'a pas de racine complexe non réelle) car pour tout $z \in \mathbb{C} \setminus \mathbb{R}$, $Q(z) \neq 0$. Le premier cas est impossible car si $Q(X) = C$ est constant alors en prenant $z = i(1 + |C|)$, on obtient une contradiction avec l'inégalité.

Exercice III.4.

Trouver les $P \in \mathbb{R}[X]$ unitaires à coefficients dans $\{-1, 0, 1\}$ qui sont scindés sur \mathbb{R} .

Lemme (Formules de Vieta) III.5.

Soit $n \in \mathbb{N}^*$, $P(X) = a_0 + a_1X + \dots + a_nX^n$ et $\lambda_1, \dots, \lambda_n$ les racines (non nécessairement différentes) de P . Supposons que $a_n \neq 0$. On a pour tout $l \in \llbracket 0; n \rrbracket$

$$\sum_{1 \leq i_1 < i_2 < \dots < i_l \leq n} \left(\prod_{j=1}^l \lambda_{i_j} \right) = (-1)^l \frac{a_{n-l}}{a_n}$$

Preuve : Nous ne ferons pas la preuve détaillée de ce résultat mais nous en donnerons uniquement l'idée principale. Pour voir d'où vient cette formule, il suffit de développer $a_n(X - \lambda_1) \dots (X - \lambda_n)$ et d'identifier les coefficients de ce polynôme avec ceux de P . En particulier, il est facile de voir cette propriété pour $l = n$ et $l = 1$ qui s'écrivent

$$(-1)^n \frac{a_0}{a_n} = \lambda_1 \dots \lambda_n \quad \text{et} \quad -\frac{a_{n-1}}{a_n} = \lambda_1 + \dots + \lambda_n$$

IV Polynômes à coefficients rationnels

Exercice IV.1.

Soit $n \geq 1$, $a_0, \dots, a_n \in \mathbb{Z}$ tels que $a_0 \neq 0$ et $a_n \neq 0$. On pose $P(X) = a_n X^n + \dots + a_1 X + a_0$. Soit $a \in \mathbb{Q}$. Trouver une condition nécessaire sur a pour qu'il soit racine de P .

Exercice IV.2.

Soit $P \in \mathbb{Q}[X]$ irréductible et a une racine complexe de P . Montrer que a est une racine simple de P .

Exercice IV.3.

Soit $P \in \mathbb{Q}[X]$ de degré égal à 5. Montrer que si P admet une racine double dans \mathbb{C} , alors il possède une racine dans \mathbb{Q} .

V Irréductibilité de $\mathbb{Z}[X]$

Exercice V.1.

Soient $n \geq 1$ et $a_1, \dots, a_n \in \mathbb{Z}$ deux à deux distincts. Soit $P = 1 + \prod_{i=1}^n (X - a_i)^2$. Montrer que P est irréductible dans $\mathbb{Z}[X]$.

Exercice (Critère d'Eisenstein) V.2.

Soit $P(X) = X^n + a_{n-1} X^{n-1} + \dots + a_0 \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que $p^2 \nmid a_0$ et pour tout $i \in \llbracket 0; n-1 \rrbracket$, $p \mid a_i$. Montrer que P est irréductible dans $\mathbb{Z}[X]$.

Exercice V.3.

Montrer que $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$ et que pour tout p premier, $X^4 + 1$ est réductible dans $\mathbb{Z}/p\mathbb{Z}$.

VI Complément : lemme de Gauß

Dans cette partie, on dit que $P \in \mathbb{Z}[X] - \{0\}$ est irréductible dans $\mathbb{Z}[X]$ si on ne peut pas l'écrire sous forme de QR avec $Q, R \in \mathbb{Z}[X]$ et $\deg Q \geq 1$ et $\deg R \geq 1$. On mentionne ceci car pour certains auteurs $2X$ par exemple est réductible car 2 n'est pas inversible dans \mathbb{Z} . En d'autres termes, dans notre définition, les termes constants ne comptent pas comme un facteur même s'ils sont non inversibles dans \mathbb{Z} .

Exercice VI.1.

Le but de cet exercice est de montrer qu'un polynôme $P \in \mathbb{Z}[X]$ non constant est irréductible dans $\mathbb{Z}[X]$ si et seulement s'il l'est sur $\mathbb{Q}[X]$. Le sens réciproque étant clair, on se propose alors de montrer le sens direct.

1. Posons pour tout polynôme $P = \sum_{k=0}^n a_k X^k$ non nul $c(P) = \prod_{i=0}^n a_i$ son contenu. Montrer que

$$\forall P, Q \in \mathbb{Z}[X] - \{0\}, c(PQ) = c(P)c(Q)$$

2. En déduire le résultat

Correction de l'exercice II.5 :

Notons pour tout polynôme Q , $F(Q)$ le nombre de racines de Q dans U . Supposons par l'absurde que la propriété qu'on veut démontrer est fausse, i.e.

$$\forall K \geq 0, \exists k \geq K, F(P_k) \neq l$$

D'une manière équivalente, que l'ensemble $A = \{k \in \mathbb{N}, F(P_k) \neq l\}$ est infini. A étant infini, il existe une extractrice ψ telle que pour tout $k \in \mathbb{N}$, $\psi(k) \in A$. Pour alléger les notations, on va noter (P_k) au lieu de $(P_{\psi(k)})$ car $(P_{\psi(k)})$ converge aussi vers P .

On sait d'après la proposition II.4 que les coefficients des termes de (P_k) convergent vers ceux de P . En particulier, P étant unitaire, le coefficient devant X^n des termes de (P_k) converge vers 1 et est donc non nul à partir d'un certain rang et alors il existe $A > 0$ tel que pour tout $k \geq A$, $\deg P_k = n$. Posons alors pour tout $k \geq A$, $\lambda_{k,1}, \dots, \lambda_{k,n}$ les racines de P_k . Les coefficients de P_k convergent et sont donc tous bornés. En utilisant la proposition II.3, on peut en déduire que les suites $(\lambda_{k,1})_{k \geq A}, \dots, (\lambda_{k,n})_{k \geq A}$ sont toutes bornées. Par conséquent, d'après Bolzano-Weierstraß, il existe une extractrice φ (la même pour les n suites, quitte à faire des extractions successives) et $\lambda_1, \dots, \lambda_n$ tels que

$$\forall i \in \llbracket 1; n \rrbracket, \lambda_{\varphi(k),i} \xrightarrow[k \rightarrow +\infty]{} \lambda_i$$

En utilisant ce qu'on vient de voir, il est facile de voir (soit en utilisant les relations coefficient racines, ou alors en passant par la convergence simple) que

$$P_{\varphi(k)}(X) = \prod_{i=1}^n (X - \lambda_{\varphi(k),i}) \xrightarrow[k \rightarrow +\infty]{} \prod_{i=1}^n (X - \lambda_i)$$

coefficient par coefficient et donc que $P(X) = \prod_{i=1}^n (X - \lambda_i)$. On a alors pour tout $i \in \llbracket 1; n \rrbracket$,

- Soit $\lambda_i \in U$, et alors U étant ouvert, il existe $K > 0$ tel que pour tout $k > K$, $\lambda_{i,\varphi(k)} \in U$
- Soit $\lambda_i \notin U$ et alors par hypothèse (pas de racines dans la frontière) $\lambda_i \in \mathbb{C} \setminus \overline{U}$. Cet ensemble est ouvert, il existe donc $K > 0$ tel que pour tout $k \geq K$, $\lambda_{i,\varphi(k)} \in \mathbb{C} \setminus \overline{U}$ et alors $\lambda_{i,\varphi(k)} \notin U$.

Ceci permet de dire que pour k assez grand, $\lambda_{i,\varphi(k)}$ et λ_i sont soit tous les deux dans U soit tout les deux à l'extérieur de U et donc en particulier que $F(P_{\varphi(k)}) = F(P) = l$, ce qui est absurde par hypothèse.

Correction de l'exercice III.2. :

Posons

$$\mathcal{S} = \{P \in \mathbb{R}[X], \exists A, B \in \mathbb{R}[X], P = A^2 + B^2\}$$

Le but de l'exercice est de montrer que l'ensemble des polynômes positifs sur \mathbb{R} est inclus dans \mathcal{S} (au passage, ces deux ensembles sont égaux car l'inclusion réciproque est évidente).

Montrons d'abord que \mathcal{S} est stable par multiplication. On a pour tout $A, B, C, D \in \mathbb{R}[X]$,

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

ce qui nous donne bien la stabilité par multiplication.

Soit P un polynôme positif sur \mathbb{R} . Si P est constant alors le résultat est évident. Supposons désormais $\deg P \geq 1$. On peut alors écrire

$$P(X) = \lambda \prod_{i=1}^r (X - a_i)^{\alpha_i} \prod_{i=1}^s \underbrace{(X^2 + b_i X + c_i)}_{\text{irréductible}}$$

avec pour tout i , $a_i, b_i, c_i \in \mathbb{R}$, $b_i^2 - 4c_i < 0$ et les a_i distincts. On a alors

$\rightarrow \lambda > 0$ car $P(x) \xrightarrow[x \rightarrow +\infty]{} +\infty$, donc $\lambda \in \mathcal{S}$.

\rightarrow Pour tout $i \in \llbracket 1; s \rrbracket$, $X^2 + b_i X + c_i = \left(X + \frac{b_i}{2}\right)^2 + \sqrt{\frac{-b_i^2 + 4c_i}{4}}^2 \in \mathcal{S}$.

\rightarrow Pour tout $i \in \llbracket 1; r \rrbracket$, on peut écrire $P(X) = Q(X)(X - a_i)^{\alpha_i}$ avec $Q \in \mathbb{R}[X]$. On a $Q(a_i) \neq 0$ et alors $Q(a_i) > 0$, ceci car $P(a_i + 1) = Q(a_i) \geq 0$. Il existe donc $\varepsilon > 0$ tel que pour tout $x \in]a_i - \varepsilon, a_i]$, $Q(x) > 0$ et alors pour tout $x \in]a_i - \varepsilon, a_i]$, $(x - a_i)^{\alpha_i} \geq 0$, ce qui nous donne nécessairement que α_i est pair. On en déduit que $(X - a_i)^{\alpha_i} = \left((X - a_i)^{\frac{\alpha_i}{2}}\right)^2 \in \mathcal{S}$.

P est donc produit d'éléments de \mathcal{S} et donc par stabilité par multiplication, il est bien dans \mathcal{S} .

Correction de l'exercice III.4. :

On suppose $P(X) = a_n X^n + \dots + a_1 X + a_0$ scindé avec $a_n = 1$. On se ramène à $P(0) \neq 0$ en factorisant éventuellement par X^k pour k la valuation de P (0 sera alors racine réelle et le caractère scindé du polynôme en sera inchangé).

Soient x_1, \dots, x_n les racines de P . On a,

$$\prod_{k=1}^n x_k = (-1)^n P(0) \quad \text{donc} \quad \prod_{k=1}^n x_k^2 = P(0)^2 = 1$$

Pour obtenir la première égalité, il suffit de remplacer X par 0 dans la décomposition de P .

L'inégalité arithmético-géométrique donne alors

$$\sum_{k=1}^n x_k^2 \geq n \sqrt[n]{x_1^2 \dots x_n^2} = n \tag{5}$$

et en utilisant les formules de Vieta,

$$n \leq \sum_{k=1}^n x_k^2 = \left(\sum_{k=1}^n x_k\right)^2 - 2 \sum_{k < l} x_k x_l = (-a_{n-1})^2 - 2a_{n-2} \leq a_{n-1}^2 + 2|a_{n-1}| \leq 3 \tag{6}$$

et donc $n \leq 3$. Le cas $n = 3$ impose le cas d'égalité dans les inégalités ci-dessus

\rightarrow Égalité dans (1), i.e. le cas d'égalité de l'inégalité arithmético-géométrique qui donne nécessairement : $x_1^2 = \dots = x_n^2$. En utilisant l'égalité $\prod_1^n x_k^2 = 1$ on obtient que $x_1^2 = \dots = x_n^2 = 1$ i.e. $Z(P) \subset \{-1, 1\}$.

\rightarrow Égalité dans l'inégalité de droite de (2), i.e. $a_{n-1}^2 - 2a_{n-2} = 3 \iff a_{n-1} = \pm 1$ et $a_{n-2} = -1$.

En particulier, la condition $n = 3$ impose que

$$P \in \underbrace{\{(X-1)^3\}}_{P_1}, \underbrace{\{(X-1)^2(X+1)\}}_{P_2}, \underbrace{\{(X-1)(X+1)^2\}}_{P_3}, \underbrace{\{(X+1)^3\}}_{P_4}$$

Il est clair que les coefficients de P_1 et P_4 ne sont pas tous dans $\{-1, 0, 1\}$ et donc ne vérifient pas les conditions voulues. Cependant P_2 et P_3 conviennent.

Pour le cas $n = 2$, on peut écrire $P = X^2 + aX + b$ où $b = \pm 1$ et $a \in \{-1, 0, 1\}$. La condition est alors $\Delta = a^2 - 4b \geq 0$ et donc les seuls polynômes convenables sont $X^2 - X - 1$, $X^2 - 1$ et $X^2 + X - 1$.

Pour $n = 1$ la propriété voulue est toujours vérifiée. En posant donc

$$A = \{X - 1, X + 1, X^2 - X - 1, X^2 - 1, X^2 + X - 1, (X - 1)^2(X + 1), (X + 1)^2(X - 1)\}$$

On déduit que l'ensemble des polynômes scindés à coefficients dans $\{-1, 0, 1\}$ est égal à

$$\{X^k Q, k \in \mathbb{N}, Q \in A\}$$

Correction de l'exercice IV.1. :

Soit a une racine de P . On a $a_0 \neq 0$ donc $a \neq 0$. Posons $a = \frac{p}{q}$ avec $p \wedge q = 1$. On a alors $P\left(\frac{p}{q}\right) = 0$, i.e.

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$

On a alors $p|a_0 q^n$ et $q|a_n p^n$ et donc par Gauß, $p|a_0$ et $q|a_n$.

Correction de l'exercice IV.2. :

Les seuls diviseurs unitaires de P sont P et 1 car P est irréductible, donc $P \wedge P' \in \{1, P\}$. Mais $\deg P' < \deg P$ donc P ne peut pas diviser P' et alors $P \wedge P' = 1$. On a alors d'après Bezout,

$$\exists U, V \in Q[X], UP + VP' = 1$$

En évaluant en a , on a $\underbrace{U(a)P(a)}_{=0} + V(a)P'(a) = 1$ et alors nécessairement $P'(a) \neq 0$, i.e. a est une racine simple de P .

Remarquer aussi que dire $P \wedge P' = 1$ est équivalent à dire que P et P' n'ont aucune racine complexe commune et que donc, en particulier, a n'est pas racine de P' , ce qui fournit le résultat.

Correction de l'exercice IV.3. :

Supposons sans perte de généralité que P est unitaire. P admet une racine double dans \mathbb{C} , donc d'après l'exercice précédent, P est réductible. On écrit $P = QR$ avec Q, R non constants, unitaires et irréductibles (s'il y a plus de deux facteurs irréductibles non constants, au moins un sera de degré 1 et donc P admet une racine rationnelle). Le cas $Q = R$ étant impossible vu que $\deg(P) = 5$ est impair, on a alors que Q et R sont premiers entre eux. En effet, Q et R étant irréductibles unitaires, on a $Q \wedge R \in \{1, Q\} \cap \{1, R\} = \{1\}$.

- Si $\deg Q = 1$, alors $Q = X - r$, avec $r \in \mathbb{Q}$ et donc r est racine rationnelle de P .
- Si $\deg Q = 2$, alors a est racine double de P mais d'après l'exercice précédent n'est racine double ni de Q ni de R et donc $Q(a) = R(a) = 0$ ce qui est absurde car $Q \wedge R = 1$.

On a donc bien le résultat voulu.

Correction de l'exercice V.1. :

Supposons par l'absurde que P est réductible. Il existe donc $Q, R \in \mathbb{Z}[X]$ tels que $\deg Q \geq 1$, $\deg R \geq 1$ et $P = QR$. On a alors

$$\forall i \in \llbracket 1; n \rrbracket, \underbrace{Q(a_i)}_{\in \mathbb{Z}} \underbrace{R(a_i)}_{\in \mathbb{Z}} = P(a_i) = 1$$

et alors

$$\forall i \in \llbracket 1; n \rrbracket, Q(a_i) = R(a_i) = \pm 1$$

De plus P est positif et ne s'annule pas sur R , donc Q et R aussi, sont de signe constant et ont le même signe. On suppose que $Q > 0$ et $R > 0$ (le cas $Q < 0$ et $R < 0$ se traite de la même manière), chose qui implique en particulier que Q et R sont unitaires (P est unitaire). On a alors

$$\forall i \in \llbracket 1; n \rrbracket, Q(a_i) - 1 = 0 \text{ et } R(a_i) - 1 = 0$$

$Q - 1$ et $R - 1$ admettent n racines distinctes, sont donc de degré au moins n et la somme de leurs degrés est $2n$. On en déduit que $\deg Q = \deg R = n$ et

$$Q(X) - 1 = R(X) - 1 = \prod_{i=1}^n (X - a_i)$$

et que finalement

$$\prod_{i=1}^n (X - a_i)^2 + 1 = P(X) = \left(\prod_{i=1}^n (X - a_i) + 1 \right)^2$$

ce qui est absurde. P est donc bien irréductible.

Correction de l'exercice V.2. :

Supposons par l'absurde que P est réductible dans $\mathbb{Z}[X]$, i.e. il existe $Q, R \in \mathbb{Z}[X]$ de degré supérieur ou égal à 1 tels que $P = QR$, qu'on peut supposer unitaires (P est unitaire). Il existe donc $r, s \in \mathbb{N}^*$, $(b_i)_{i \in \llbracket 0; r-1 \rrbracket} \in \mathbb{Z}^r$ et $(c_i)_{i \in \llbracket 0; s-1 \rrbracket} \in \mathbb{Z}^s$ tels que

$$Q(x) = X^r + b_{r-1}X^{r-1} + \cdots + b_1X + b_0 \quad \text{et} \quad R(X) = X^s + c_{s-1}X^{s-1} + \cdots + c_1X + c_0$$

On passe dans $\mathbb{Z}/p\mathbb{Z}[X]$: comme $\forall i \in \llbracket 0; n-1 \rrbracket, a_i \equiv 0 [p]$, on peut écrire dans $\mathbb{Z}/p\mathbb{Z}[X]$

$$P(X) = X^n + \underbrace{\overline{a_{n-1}}X^{n-1} + \cdots + \overline{a_1}X + \overline{a_0}}_{=0} = X^n$$

De plus, on a également dans $\mathbb{Z}/p\mathbb{Z}[X]$

$$X^n = P(X) = Q(X)R(X) = (X^r + \overline{b_{r-1}}X^{r-1} + \cdots + \overline{b_1}X + \overline{b_0})(X^s + \overline{c_{s-1}}X^{s-1} + \cdots + \overline{c_1}X + \overline{c_0})$$

Or par unicité de la décomposition de X^n en facteurs irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$, $Q(X)$ et $R(X)$ doivent être de la forme X^{s_1} et X^{s_2} . Pour qu'on ait la bonne puissance, il est nécessaire que $s_1 = r$ et $s_2 = s$, i.e., dans $\mathbb{Z}/p\mathbb{Z}[X]$, $Q(X) = X^r$ et $R(X) = X^s$, et alors

$$\overline{b_{r-1}} = \cdots = \overline{b_1} = \overline{b_0} = \overline{c_{s-1}} = \cdots = \overline{c_1} = \overline{c_0} = \overline{0}$$

Or $a_0 = c_0b_0$ et d'après l'égalité ci-dessus, $p|b_0$ et $p|c_0$ et donc $p^2|a_0$, ce qui est absurde.

Correction de l'exercice V.3. :

→ Irréductibilité dans $\mathbb{R}[X]$.

On décompose $X^4 + 1$

$$X^4 + 1 = (X^2 + 1)^2 - 2X^2 = \underbrace{(X^2 + \sqrt{2}X + 1)}_{A(X)} \underbrace{(X^2 - \sqrt{2}X + 1)}_{B(X)}$$

Si $X^4 + 1$ était réductible dans $\mathbb{Q}[X]$, on pourrait écrire $X^4 + 1 = QR$ tel que $Q, R \in \mathbb{Q}[X]$, $\deg R \geq \deg Q \geq 1$ et Q et R sont unitaires. Le cas $\deg Q = 1$ est impossible car $X^4 + 1$ n'admet pas de racine rationnelle. Le cas $\deg Q = 2$ est impossible car par unicité de la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$, on aurait $Q, R \in \{A, B\}$ ce qui est absurde car $A, B \notin \mathbb{Q}[X]$. On en déduit donc que $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$.

→ Irréductibilité dans $\mathbb{Z}/p\mathbb{Z}$.

Si $p = 2$, alors on peut écrire dans $\mathbb{Z}/p\mathbb{Z}$

$$X^4 + \overline{1} = X^4 + \overline{2}X^2 + \overline{1} = (X^2 + \overline{1})^2$$

donc $X^4 + 1$ est réductible. Supposons maintenant $p \geq 3$.

Si $\overline{2}$ est un carré modulo p , i.e. il existe $a \in \mathbb{Z}/p\mathbb{Z}$ tel que $a^2 = \overline{2}$, on peut écrire

$$X^4 + 1 = (X^2 + \overline{1})^2 - \overline{2}X^2 = (X^2 + \overline{1})^2 - a^2X^2 = (X^2 + \overline{1} + a)(X^2 + \overline{1} - a)$$

Si $\overline{-2}$ est un carré modulo p , i.e. il existe $b \in \mathbb{Z}/p\mathbb{Z}$ tel que $b^2 = \overline{-2}$, on peut écrire

$$X^4 + 1 = (X^2 - \overline{1})^2 - \overline{-2}X^2 = (X^2 - \overline{1})^2 - b^2X^2 = (X^2 + \overline{1} + b)(X^2 + \overline{1} - b)$$

Supposons maintenant que ni $\overline{2}$ ni $\overline{-2}$ ne sont des carrés modulo p . On a alors d'après le chapitre 21, $\overline{2}^{\frac{p-1}{2}} = \overline{-1}$ et $\overline{-2}^{\frac{p-1}{2}} = \overline{-1}$ et donc en faisant le produit des deux, $\overline{-4}^{\frac{p-1}{2}} = \overline{1}$. On peut donc écrire $\overline{1} = \overline{-4}^{\frac{p-1}{2}} = \overline{-1}^{\frac{p-1}{2}} \times \overline{4}^{\frac{p-1}{2}} = \overline{-1}^{\frac{p-1}{2}}$ ce qui nous permet de dire que -1 est un carré modulo p . En posant $c^2 = \overline{-1}$ avec $c \in \mathbb{Z}/p\mathbb{Z}$, on peut finalement écrire

$$X^4 + \overline{1} = X^4 - \overline{-1} = X^4 - c^2 = (X^2 - c)(X^2 + c)$$

On en déduit donc que $X^4 + 1$ est bien réductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Correction de l'exercice VI.1. :

1. Il est facile de voir que pour tout $P(X) = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X] \setminus \{0\}$ et $a \in \mathbb{N}^*$ tel que $a|c(P)$,

$$\frac{1}{a}c(P) = \prod_{i=0}^n \frac{a_i}{a} = c\left(\frac{P}{a}\right)$$

Donc montrer le résultat voulu est équivalent à montrer que

$$c\left(\frac{P}{c(P)} \times \frac{Q}{c(Q)}\right) = 1$$

et donc quitte à remplacer $\frac{P}{c(P)}$ par P et $\frac{Q}{c(Q)}$ par Q , il suffit de montrer que

$$\forall P, Q \in \mathbb{Z}[X] \setminus \{0\}, \quad c(P) = c(Q) = 1 \implies c(PQ) = 1$$

Soient $P, Q \in \mathbb{Z}[X] \setminus \{0\}$ et $p \in \mathbb{Z}$ premier. Si $p|c(PQ)$, alors dans $\mathbb{Z}/p\mathbb{Z}[X]$, $PQ = 0$ (car p divise tous les coefficients de PQ) et alors, $\mathbb{Z}/p\mathbb{Z}$ étant intègre, $P = 0$ ou $Q = 0$ dans $\mathbb{Z}/p\mathbb{Z}[X]$ et alors p divise tous les coefficients de P ou tous les coefficients de Q , i.e. $p|c(P)$ ou $p|c(Q)$ ce qui est absurde car $c(P) = c(Q) = 1$. On en déduit donc qu'on a bien $c(PQ) = 1$.

2. Soit $P \in \mathbb{Z}[X] \setminus \{0\}$ réductible dans $\mathbb{Q}[X]$. Étant donné que diviser P par un entier (qui divise tous les coefficients pour rester dans $\mathbb{Z}[X]$) ne change pas fait que P soit irréductible ou non dans $\mathbb{Z}[X]$, quitte à diviser par $c(P)$, on suppose que $c(P) = 1$.

Soit $\lambda \in \mathbb{Z}$ le coefficient dominant de P . P étant réductible dans $\mathbb{Q}[X]$, il existe $Q, R \in \mathbb{Q}[X]$ unitaires tels que $\deg Q \geq 1$, $\deg R \geq 1$ et $P = \lambda QR$. On va montrer que λ s'écrit $\lambda = cd$ avec $c, d \in \mathbb{Z}$ et $cQ, dR \in \mathbb{Z}[X]$.

Posons $a = \min \underbrace{\{k \geq 1, kQ \in \mathbb{Z}[X]\}}_{\neq \emptyset}$. On veut montrer que $c(aQ) = 1$. Supposons le contraire. On a

alors $\frac{aQ}{c(aQ)} \in \mathbb{Z}[X]$, et $c(aQ)$ divise le coefficient dominant de aQ qui est égal à a , donc $\frac{a}{c(aQ)} \in \mathbb{N}^*$ ce qui contredit la minimalité de a . En posant donc $b = \min\{k \geq 1, kR \in \mathbb{Z}[X]\}$, on a de même $c(bR) = 1$. On a alors

$$ab = ab \cdot c(P) = c(abP) = c(\lambda \times aQ \times bR) = |\lambda|c(aQ)c(bR) = |\lambda|$$

Quitte à changer le signe de a , on peut donc écrire $P = \underbrace{aQ}_{\in \mathbb{Z}[X]} \times \underbrace{bR}_{\in \mathbb{Z}[X]}$ et alors P est bien réductible dans $\mathbb{Z}[X]$.

On peut montrer d'une manière plus générale, par la même démonstration ci-haut, que si $P = \lambda \prod_{i=1}^r Q_i \in \mathbb{Z}[X] \setminus \{0\}$ est une factorisation de P dans $\mathbb{Q}[X]$ avec Q_i unitaires et λ le coefficient dominant de P , alors on peut écrire $\lambda = c(P)\lambda_1 \dots \lambda_r$ avec pour tout $i \in \llbracket 1; r \rrbracket$, $\lambda_i \in \mathbb{Z}$ et $\lambda_i Q_i \in \mathbb{Z}[X]$. En particulier

- Si $P = \lambda \prod_{i=1}^r Q_i$ est la factorisation en irréductibles dans $\mathbb{Q}[X]$, alors $P = c(P) \prod_{i=1}^r (\lambda_i Q_i)$ est une factorisation en irréductibles dans $\mathbb{Z}[X]$.
- Pour tout $Q \in \mathbb{Z}[X] \setminus \{0\}$,

$$Q|P \text{ dans } \mathbb{Z}[X] \iff Q|P \text{ dans } \mathbb{Q}[X] \text{ et } c(Q)|c(P)$$

Le cas particulier où $\pm Q$ est unitaire est assez connu et est une conséquence du fait qu'on peut effectuer la division euclidienne dans $\mathbb{Z}[X]$ par un polynôme unitaire (ou de coefficient dominant égal à -1) de $\mathbb{Z}[X]$ (en effet, lorsque \mathbb{K} n'est pas un corps, on ne peut pas toujours faire la division euclidienne dans $\mathbb{K}[X]$) et du fait que la division euclidienne dans $\mathbb{Z}[X]$ (lorsqu'elle est faisable dans $\mathbb{Z}[X]$) et $\mathbb{Q}[X]$ donne toujours le même résultat.

- Si P est unitaire et $P = \prod_{i=1}^r Q_i$ est une factorisation dans $\mathbb{Q}[X]$ avec les Q_i unitaires, alors pour tout $i \in \llbracket 1; r \rrbracket$, $Q_i \in \mathbb{Z}[X]$. En effet, en reprenant les notations vu précédemment, $1 = c(P)\lambda_1 \dots \lambda_r$ implique que pour tout $i \in \llbracket 1; r \rrbracket$, $\lambda_i \in \{-1, 1\}$. Cette propriété est particulièrement intéressante dans le cas où l'égalité $P = \prod_{i=1}^r Q_i$ est une factorisation en irréductibles dans $\mathbb{Q}[X]$, vu qu'elle donne que chaque facteur est en fait (unitaire et) dans $\mathbb{Z}[X]$.



Systèmes linéaires

Soit \mathbb{K} un corps et $m, n \in \mathbb{N}^*$.

I Généralités

D'une manière générale, un système linéaire s'écrit de la manière suivante.

$$(S) : \begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = b_1 \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n = b_m \end{cases} \iff AX = B$$

où $X = (x_1, \dots, x_n)^T$ sont les inconnus, $A = (a_{i,j})_{\substack{i \in \llbracket 1; m \rrbracket \\ j \in \llbracket 1; n \rrbracket}}$ une matrice à coefficients dans \mathbb{K} et $B = (b_1, \dots, b_m)^T$ un vecteur de \mathbb{K}^m .

Vocabulaire : On appelle rang du système (S) le rang de la matrice A . De plus, on dit que (S) est
 → Compatible lorsque l'ensemble des solutions, noté \mathcal{S} , est non vide.
 → Homogène lorsque $B = 0$.

On notera SS_0 l'ensemble des solutions de l'équation $AX = 0$.

Proposition I.1.

1. SS_0 est un sous-espace vectoriel de \mathbb{K}^n de dimension $n - \text{rg } A$.
2. SS est soit vide, soit un sous-espace affine de \mathbb{K}^n parallèle à SS_0 . En d'autres termes, SS est soit vide, soit $\text{SS} = X_0 + \text{SS}_0$ pour n'importe quel $X_0 \in \text{SS}$
3. $\text{SS} \neq \emptyset \iff B \in \text{Im } A$

Preuve :

1. On a $\text{SS}_0 = \text{Ker } A$ et donc par la formule du rang,

$$\dim \text{SS}_0 = \dim \text{Ker } A = n - \dim \text{Im } A = n - \text{rg } A$$

2. Supposons $\text{SS} \neq \emptyset$ et soit $X_0 \in \text{SS}$. On a

$$X \in \text{SS} \iff AX = B \iff AX = AX_0 \iff A(X - X_0) = 0 \iff X - X_0 \in \text{SS}_0$$

3. $\text{SS} \neq \emptyset \iff \exists X \in \mathbb{K}^n \ AX = B \iff B \in \text{Im } A$

On aura besoin du lemme assez connu suivant

Exercice I.2.

Soit $A \in \mathcal{M}_{n,m}(\mathbb{K})$, alors $\text{rg } A = \text{rg } A^T$

II Système de Cramer

Dans cette partie, on suppose que $m = n$ et donc $A \in \mathcal{M}_n(\mathbb{K})$.

Théorème II.1.

Les propositions suivantes sont équivalentes.

1. $A \in \mathrm{GL}_n(\mathbb{K})$
2. $\forall B \in \mathbb{K}^n, AX = B$ possède exactement une solution.
3. $\forall B \in \mathbb{K}^n, AX = B$ possède au moins une solution.
4. La seule solution de SS_0 est 0.
5. $\det A \neq 0$.

Si elles sont satisfaites, on dit que (S) est un système de Cramer.

Preuve :

- $\rightarrow (1) \Rightarrow (2)$ Si $A \in \mathrm{GL}_n(\mathbb{K})$, alors pour tout $B \in \mathbb{K}^n$ l'unique solution de (S) est $X = A^{-1}B$.
- $\rightarrow (2) \Rightarrow (3)$ Clair.
- $\rightarrow (3) \Rightarrow (4)$ L'application $f_A : \begin{cases} \mathbb{K}^n & \longrightarrow \mathbb{K}^n \\ X & \longmapsto AX \end{cases}$ est surjective et donc, par égalité des dimensions finies, est aussi injective et donc son noyau $\mathrm{SS}_0 = \{0\}$.
- $\rightarrow (4) \Rightarrow (5)$ Si la seule solution de SS_0 est 0, alors on a $\mathrm{Ker} A = \{0\}$ et donc A est inversible, i.e. $\det A \neq 0$.
- $\rightarrow (5) \Rightarrow (1)$ Clair.

Proposition (Formule de Cramer) II.2.

Supposons que (S) est de Cramer et posons C_1, \dots, C_n les colonnes de A et $X = (x_1, \dots, x_n)^T$ l'unique solution de (S) . On a nécessairement

$$\forall k \in \llbracket 1; n \rrbracket, x_k = \frac{\det(C_1, \dots, C_{k-1}, B, C_{k+1}, \dots, C_n)}{\det A}$$

Preuve : On a $B = AX = x_1C_1 + \dots + x_nC_n$ et alors pour tout $k \in \llbracket 1; n \rrbracket$

$$\begin{aligned} \frac{\det(C_1, \dots, C_{k-1}, B, C_{k+1}, \dots, C_n)}{\det A} &= \sum_{i=1}^n x_i \frac{\det(C_1, \dots, C_{k-1}, C_i, C_{k+1}, \dots, C_n)}{\det A} \\ &= x_k \frac{\det(C_1, \dots, C_{k-1}, C_k, C_{k+1}, \dots, C_n)}{\det A} = x_k \end{aligned}$$

Exemple : Lorsque $n = 2$, on peut écrire (S) sous la forme suivante

$$(S) : \begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases}$$

(S) est de cramer si et seulement si $\begin{vmatrix} a & b \\ a' & b' \end{vmatrix} = ab' - a'b \neq 0$ et dans ce cas, la seule solution de (S) est

$$x = \frac{\begin{vmatrix} c & b \\ c' & b' \end{vmatrix}}{\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}} = \frac{b'c - bc'}{ab' - a'b} y = \frac{\begin{vmatrix} a & c \\ a' & c' \end{vmatrix}}{\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}} = \frac{ac' - a'c}{ab' - a'b}$$

La propriété exposée dans cet exercice est essentielle et est utilisée dans le chapitre de réduction d'endomorphismes.

Exercice (Lemme d'Hadamard) II.3.

Soit $A = (a_{i,j})_{i,j \in \llbracket 1; n \rrbracket} \in \mathcal{M}_n(\mathbb{C})$ tel que pour tout $i \in \llbracket 1; n \rrbracket$, $|a_{i,i}| > \sum_{j=1, j \neq i}^n |a_{i,j}|$. Montrer que $A \in \mathrm{GL}_n(\mathbb{C})$.

Remarque : En transposant, on obtient un énoncé similaire mais en sommant sur la même colonne.

III Valeurs propres et systèmes homogènes

Vocabulaire : On dit que $\lambda \in \mathbb{K}$ est une valeur propre de A s'il existe $X \in \mathbb{K}^n \setminus \{0\}$ tel que $AX = \lambda X$.

Proposition III.1.

Soit $A \in \mathcal{M}_n(\mathbb{K})$, $\lambda \in \mathbb{K}$ et $f_A : \begin{cases} \mathbb{K}^n & \rightarrow \mathbb{K}^n \\ X & \mapsto AX \end{cases}$. Les propositions suivantes sont équivalentes.

1. λ valeur propre de A
2. $\mathrm{Ker}(f_A - \lambda \mathrm{Id}) \neq \{0\}$
3. $\det(A - \lambda I_n) = 0$
4. Le système $(A - \lambda I_n)X = 0$ a une solution $X \neq 0$.

Preuve : Il s'agit d'une conséquence directe de ce qui précède.

Exercice III.2.

Soit $A \in \mathcal{M}_n(\mathbb{C})$. Montrer que les valeurs propres complexes de A appartiennent à

$$\bigcup_{i=1}^n B_f \left(a_{i,i}, \sum_{j=1, j \neq i}^n |a_{i,j}| \right)$$

on peut améliorer cette borne en considérant aussi la transposée de A .

IV Matrices de permutation

Définition IV.1.

Pour tout $\sigma \in \mathcal{S}_n$, on pose $P_\sigma = (\delta_{i,\sigma(j)})_{i,j \in \llbracket 1; n \rrbracket}$. On appelle cette matrice la matrice de permutation associée à σ .

On présente ces propriétés qu'on utilisera dans la suite comme exercice.

Exercice IV.2.

Soit $\sigma, \sigma' \in \mathcal{S}_n$.

1. Calculer $\det P_\sigma$.
2. Montrer que $P_\sigma P_{\sigma'} = P_{\sigma \circ \sigma'}$ et en déduire que $P_\sigma^{-1} = P_{\sigma^{-1}}$.
3. En déduire que $G = \{P_\sigma, \sigma \in \mathcal{S}_n\}$ muni du produit matriciel est isomorphe à \mathcal{S}_n .
4. Soit $A = (a_{i,j})_{i,j \in \llbracket 1;n \rrbracket} \in \mathcal{M}_n(\mathbb{K})$ et $X = (x_i)_{i \in \llbracket 1;n \rrbracket} \in \mathbb{K}^n$. Calculer $P_\sigma A$, AP_σ et $P_\sigma X$.

V Comment déterminer $\text{Ker } A$ en pratique ?

1. Explication de l'algorithme

Le but de cette partie est de répondre à la question suivante : Étant donnée $A = (a_{i,j})_{i,j \in \llbracket 1;n \rrbracket} \in \mathcal{M}_n(\mathbb{K})$, comment déterminer $\text{Ker } A$? Cette question est équivalente à déterminer l'ensemble des solutions du système $AX = 0$. Posons alors $r = \text{rg } A$. Bien entendu, la réponse est claire lorsque $r = n$ car il s'agit d'un système de Cramer, on suppose donc que $r < n$.

$r \in \llbracket 1; n-1 \rrbracket$ donc il existe r lignes (qui forment une famille libre) de A telles que les $n-r$ lignes restantes sont combinaison linéaire de ces r lignes. Quitte à permutez les lignes de A , supposons que ces lignes sont les r premières. Écrivons alors le système $AX = 0$.

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = 0 \\ \vdots \\ a_{r,1}x_1 + \cdots + a_{r,n}x_n = 0 \\ a_{r+1,1}x_1 + \cdots + a_{r+1,n}x_n = 0 \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n = 0 \end{cases}$$

Il est facile de voir que si les r premières équations sont satisfaites, alors les $n-r$ suivantes aussi, donc il faut et il suffit de résoudre le système suivant.

$$(S) : \begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = 0 \\ \vdots \\ a_{r,1}x_1 + \cdots + a_{r,n}x_n = 0 \end{cases}$$

C'est à dire en posant $B = (a_{i,j})_{i \in \llbracket 1;r \rrbracket, j \in \llbracket 1;n \rrbracket}$, le système devient équivalent à $BX = 0$. Les lignes de B forment une famille libre, donc $\text{rg } B = r$ et alors quitte à permutez les colonnes de B , on peut affirmer que les r premières colonnes de B forment une famille libre, et donc que la matrice $B' = (a_{i,j})_{i,j \in \llbracket 1;r \rrbracket}$ est inversible. Posons alors $B'' = (a_{i,j})_{i \in \llbracket 1;r \rrbracket, j \in \llbracket n-r;n \rrbracket}$. En posant pour tout $X \in \mathbb{K}^n$, $X = \begin{pmatrix} X' \\ X'' \end{pmatrix}$ avec $X' \in \mathbb{K}^r$ et $X'' \in \mathbb{K}^{n-r}$, on peut écrire

$$(S) \iff BX = 0 \iff \begin{pmatrix} B' & B'' \end{pmatrix} \begin{pmatrix} X' \\ X'' \end{pmatrix} = 0 \iff B'X' + B''X'' = 0 \iff X' = -B'^{-1}B''X''$$

Remarquons qu'étant donné X'' , le système $B'X' = -B''X''$ est de Cramer et admet donc une unique

solution $-B'^{-1}B''X''$. On en déduit alors que pour tout $X = \begin{pmatrix} X' \\ X'' \end{pmatrix} \in \mathbb{K}^n$,

$$X \in \text{Ker } A \iff X' = -B'^{-1}B''X'' \text{ et alors } \text{Ker } A = \left\{ \begin{pmatrix} -B'^{-1}B''X'' \\ X'' \end{pmatrix}, X'' \in \mathbb{K}^{n-r} \right\}$$

Ensuite, en notant pour tout $j \in \llbracket 1; n-r \rrbracket$, $E_j = (\delta_{i,j})_{i \in \llbracket 1; n-r \rrbracket}$ le j -ème vecteur de la base canonique de \mathbb{K}^{n-r} on peut voir facilement que la famille

$$\mathcal{B} = \left\{ \begin{pmatrix} -B'^{-1}B''E_1 \\ E_1 \end{pmatrix}, \dots, \begin{pmatrix} -B'^{-1}B''E_{n-r} \\ E_{n-r} \end{pmatrix} \right\}$$

est une base de $\text{Ker } A$ (nous conseillons au lecteur de le montrer à titre d'exercice). En pratique, les vecteurs de cette base peuvent être retrouvés en résolvant les systèmes

$$B'X' = -B''E_1, \dots, B'X' = -B''E_{n-r}$$

qui permettent de retrouver respectivement les vecteurs $-B'^{-1}B''E_1, \dots, -B'^{-1}B''E_{n-r}$ en utilisant le pivot de Gauss. On en déduit donc que finalement

$$\text{Ker } A = \text{Vect} \left(\left\{ \begin{pmatrix} -B'^{-1}B''E_1 \\ E_1 \end{pmatrix}, \dots, \begin{pmatrix} -B'^{-1}B''E_{n-r} \\ E_{n-r} \end{pmatrix} \right\} \right)$$

Remarques :

→ Ici, on a supposé que les r première lignes de A forment une famille libre. Cette propriété est en général fausse. En pratique, après avoir trouvé des indices i_1, \dots, i_r tels que les lignes de A d'indices i_1, \dots, i_r forment une famille libre, la matrice B qu'on considérera sera égale à $\begin{pmatrix} L_{i_1} \\ \vdots \\ L_{i_r} \end{pmatrix}$ où L_1, \dots, L_n sont les lignes de A .

→ On a également supposé que les r premières colonnes de B forment une famille libre quitte à permuter les colonnes. Pour être un peu plus rigoureux, on doit introduire quelques éléments. Si on pose C_1, \dots, C_n les colonnes de B , $\sigma : \llbracket 1; n \rrbracket \longrightarrow \llbracket 1; n \rrbracket$ une permutation telle que $(C_{\sigma(1)}, \dots, C_{\sigma(r)})$ forment une famille libre et $P_\sigma = (\delta_{i,\sigma(j)})_{i,j \in \llbracket 1; n \rrbracket}$. D'après l'exercice IV.2, on a

$$BP_\sigma = \begin{pmatrix} C_{\sigma(1)} & \dots & C_{\sigma(n)} \end{pmatrix}$$

et alors on voit que le raisonnement ci-dessus est valable si on remplace B par $\tilde{B} = BP_\sigma$, i.e.

$$\tilde{B}X = 0 \iff X \in \text{Vect} \left(\left\{ \begin{pmatrix} -\tilde{B}'^{-1}\tilde{B}''E_1 \\ E_1 \end{pmatrix}, \dots, \begin{pmatrix} -\tilde{B}'^{-1}\tilde{B}''E_{n-r} \\ E_{n-r} \end{pmatrix} \right\} \right)$$

et donc on peut écrire

$$\begin{aligned} X \in \text{Ker } A &\iff BX = 0 \iff \tilde{B}P_\sigma^{-1}X = 0 \\ &\iff P_\sigma^{-1}X \in \text{Vect} \left(\left\{ \begin{pmatrix} -\tilde{B}'^{-1}\tilde{B}''E_1 \\ E_1 \end{pmatrix}, \dots, \begin{pmatrix} -\tilde{B}'^{-1}\tilde{B}''E_{n-r} \\ E_{n-r} \end{pmatrix} \right\} \right) \\ &\iff X \in \text{Vect} \left(\left\{ P_\sigma \begin{pmatrix} -\tilde{B}'^{-1}\tilde{B}''E_1 \\ E_1 \end{pmatrix}, \dots, P_\sigma \begin{pmatrix} -\tilde{B}'^{-1}\tilde{B}''E_{n-r} \\ E_{n-r} \end{pmatrix} \right\} \right) \end{aligned}$$

et donc en conclusion, on en déduit que

$$\text{Ker } A = \text{Vect} \left(\left\{ P_\sigma \begin{pmatrix} -\tilde{B}'^{-1} \tilde{B}'' E_1 \\ E_1 \end{pmatrix}, \dots, P_\sigma \begin{pmatrix} -\tilde{B}'^{-1} \tilde{B}'' E_{n-r} \\ E_{n-r} \end{pmatrix} \right\} \right)$$

- Dans le cas où A n'est pas carrée, on peut éliminer des lignes comme à l'étape 2 et appliquer exactement le même algorithme.
- Le raisonnement ci-dessus montre en particulier que $\dim \text{Ker } A = n - r$, c'est à dire la formule du rang $\text{rg } A + \dim \text{Ker } A = n$.

2. Algorithme en pratique

Résumons maintenant les étapes l'algorithme qui permet de trouver $\text{Ker } A$.

- Trouver le rang r de A (en échelonnant par exemple) et ensuite L_{i_1}, \dots, L_{i_r} r lignes de A formant une famille libre.

- Poser $B = \begin{pmatrix} L_{i_1} \\ \vdots \\ L_{i_r} \end{pmatrix}$. Trouver des indices j_1, \dots, j_n tels que si C_1, \dots, C_n sont les colonnes de B , alors les colonnes C_{j_1}, \dots, C_{j_r} forment une famille libre et poser

$$\tilde{B} = (C_{j_1} \ \dots \ C_{j_n}), \quad \tilde{B}' = (C_{j_1} \ \dots \ C_{j_r}), \quad \tilde{B}'' = (C_{j_{r+1}} \ \dots \ C_{j_n})$$

- Résoudre les systèmes

$$\tilde{B}' X' = -\tilde{B}'' E_1, \dots, \tilde{B}' X' = -\tilde{B}'' E_{n-r}$$

et poser $X_1, \dots, X_{n-r} \in \mathbb{K}^{n-r}$ les solutions de ces systèmes.

- Poser pour tout $i \in \llbracket 1; n-r \rrbracket$, $Y_i = \begin{pmatrix} X_i \\ E_i \end{pmatrix} = \begin{pmatrix} y_{i,j_1} \\ \vdots \\ y_{i,j_n} \end{pmatrix}$ où (E_1, \dots, E_{n-r}) est la base canonique de \mathbb{K}^{n-r} .

- En posant pour tout $i \in \llbracket 1; n-r \rrbracket$, $\tilde{Y}_i = \begin{pmatrix} y_{i,1} \\ \vdots \\ y_{i,n} \end{pmatrix}$ (on réordonne les coordonnées de Y_i en effectuant les opérations inverses appliquées à B), la famille $\mathcal{B} = (\tilde{Y}_1, \dots, \tilde{Y}_{n-r})$ est une base de $\text{Ker } A$.

Remarque : Si on reprend les notations de la remarque précédente, on a pour tout $k \in \llbracket 1; n \rrbracket$, $j_k = \sigma(k)$ et donc $\tilde{Y}_i = P_\sigma Y_i$ et $\tilde{B} = B P_\sigma$.

Appliquons cet algorithme via l'exemple suivant.

Application : On considère la matrice $A = \begin{pmatrix} 1 & 2 & 2 & 3 \\ 1 & 2 & 3 & 2 \\ 2 & 4 & 5 & 5 \\ -1 & -2 & -1 & -4 \end{pmatrix}$. Trouver $\text{Ker } A$.

→ **Étape 1 :** Trouver le rang r de A (en échelonnant par exemple) et ensuite L_{i_1}, \dots, L_{i_r} r lignes de A formant une famille libre.

On échelonne la matrice A par lignes en effectuant les opérations suivantes.

$$\begin{aligned} \text{ligne 2} &\leftarrow \text{ligne 2} - \text{ligne 1} \\ \text{ligne 3} &\leftarrow \text{ligne 3} - 2 \times \text{ligne 1} \\ \text{ligne 4} &\leftarrow \text{ligne 4} + \text{ligne 1} \\ \text{ligne 3} &\leftarrow \text{ligne 3} - \text{ligne 2} \\ \text{ligne 4} &\leftarrow \text{ligne 4} - \text{ligne 2} \end{aligned}$$

On obtient la matrice $\begin{pmatrix} 1 & 2 & 2 & 3 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ ce qui nous permet d'affirmer que A est rang 2. De plus, on voit que la première et la deuxième ligne de A forment une famille libre.

→ **Étape 2 :** Poser $B = \begin{pmatrix} L_{i_1} \\ \vdots \\ L_{i_r} \end{pmatrix}$. Trouver des indices j_1, \dots, j_n tels que si C_1, \dots, C_n sont les colonnes de B , alors les colonnes C_{j_1}, \dots, C_{j_r} forment une famille libre et poser

$$\tilde{B} = (C_{j_1} \ \dots \ C_{j_n}), \quad \tilde{B}' = (C_{j_1} \ \dots \ C_{j_r}), \quad \tilde{B}'' = (C_{j_{r+1}} \ \dots \ C_{j_n})$$

On pose donc

$$B = \begin{pmatrix} 1 & 2 & 2 & 3 \\ 1 & 2 & 3 & 2 \end{pmatrix}$$

Les deux premières colonnes de B ne forment pas une famille libre mais les deux dernières si, on permute alors les colonnes pour que les deux premières soient libres de la manière suivante

$$\begin{aligned} \text{colonne 1 de } \tilde{B} &\leftarrow \text{colonne 3 de } B \\ \text{colonne 3 de } \tilde{B} &\leftarrow \text{colonne 1 de } B \\ \text{colonne 2 de } \tilde{B} &\leftarrow \text{colonne 4 de } B \\ \text{colonne 4 de } \tilde{B} &\leftarrow \text{colonne 2 de } B \end{aligned}$$

C'est à dire $j_1 = 3, j_2 = 4, j_3 = 1$ et $j_4 = 2$. On pose alors

$$\tilde{B} = \begin{pmatrix} 2 & 3 & 1 & 2 \\ 3 & 2 & 1 & 2 \end{pmatrix}, \quad \tilde{B}' = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \text{ et } \tilde{B}'' = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

→ **Étape 3 :** Résoudre les systèmes

$$\tilde{B}'X' = -\tilde{B}''E_1, \dots, \tilde{B}'X' = -\tilde{B}''E_{n-r}$$

et poser $X_1, \dots, X_{n-r} \in \mathbb{K}^{n-r}$ les solutions de ces systèmes.

Ici, on a deux systèmes

$$\tilde{B}'X' = -\tilde{B}''E_1 \text{ et } \tilde{B}'X' = -\tilde{B}''E_2$$

i.e.

$$\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = - \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ et } \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = - \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

C'est à dire

$$\begin{cases} 2x + 3y = -1 \\ 3x + 2y = -1 \end{cases} \text{ et } \begin{cases} 2x + 3y = -2 \\ 3x + 2y = -2 \end{cases}$$

En résolvant ces deux systèmes, on trouve que leurs solutions sont respectivement

$$X_1 = \begin{pmatrix} -1/5 \\ -1/5 \end{pmatrix} \text{ et } X_2 = \begin{pmatrix} -2/5 \\ -2/5 \end{pmatrix}$$

→ **Étape 4 :** Poser pour tout $i \in \llbracket 1; n-r \rrbracket$, $Y_i = \begin{pmatrix} X_i \\ E_i \end{pmatrix} = \begin{pmatrix} y_{i,j_1} \\ \vdots \\ y_{i,j_n} \end{pmatrix}$ où (E_1, \dots, E_{n-r}) est la base canonique de \mathbb{K}^{n-r} .

On pose donc

$$Y_1 = \begin{pmatrix} -1/5 \\ -1/5 \\ 1 \\ 0 \end{pmatrix} \text{ et } Y_2 = \begin{pmatrix} -2/5 \\ -2/5 \\ 0 \\ 1 \end{pmatrix}$$

→ **Étape 5 :** En posant pour tout $i \in \llbracket 1; n-r \rrbracket$, $\tilde{Y}_i = \begin{pmatrix} y_{i,1} \\ \vdots \\ y_{i,n} \end{pmatrix}$ (on réordonne les coordonnées de Y_i), la famille $\mathcal{B} = (\tilde{Y}_1, \dots, \tilde{Y}_{n-r})$ est une base de $\text{Ker } A$.

On va effectuer la permutation inverse de celle de l'étape 2 aux lignes des Y_i , c'est à dire

$$\begin{aligned} \text{ligne 3 de } \tilde{Y}_i &\leftarrow \text{ligne 1 de } Y_i \\ \text{ligne 1 de } \tilde{Y}_i &\leftarrow \text{ligne 3 de } Y_i \\ \text{ligne 4 de } \tilde{Y}_i &\leftarrow \text{ligne 2 de } Y_i \\ \text{ligne 2 de } \tilde{Y}_i &\leftarrow \text{ligne 4 de } Y_i \end{aligned}$$

et donc on a dans ce cas

$$\tilde{Y}_1 = \begin{pmatrix} 1 \\ 0 \\ -1/5 \\ -1/5 \end{pmatrix} \text{ et } \tilde{Y}_2 = \begin{pmatrix} 0 \\ 1 \\ -2/5 \\ -2/5 \end{pmatrix}$$

et alors on en déduit que

$$\text{Ker } A = \text{Vect} \left(\left\{ \begin{pmatrix} 1 \\ 0 \\ -1/5 \\ -1/5 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -2/5 \\ -2/5 \end{pmatrix} \right\} \right)$$

On peut facilement vérifier que ce résultat est bien correct. En effet, les deux vecteurs ci-dessus forment

une famille libre et

$$A\tilde{Y}_1 = \begin{pmatrix} 1 & 2 & 2 & 3 \\ 1 & 2 & 3 & 2 \\ 2 & 4 & 5 & 5 \\ -1 & -2 & -1 & -4 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ -1/5 \\ -1/5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \text{ et } A\tilde{Y}_2 = \begin{pmatrix} 1 & 2 & 2 & 3 \\ 1 & 2 & 3 & 2 \\ 2 & 4 & 5 & 5 \\ -1 & -2 & -1 & -4 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ -2/5 \\ -2/5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Ces deux vecteurs sont donc bien dans $\text{Ker } A$. On sait de plus que $\dim \text{Ker } A = 2$ il est donc clair que $(\tilde{Y}_1, \tilde{Y}_2)$ est une base de $\text{Ker } A$ et alors $\text{Ker } A = \text{Vect}(\tilde{Y}_1, \tilde{Y}_2)$.

Remarque culturelle : On a montré que

$$\text{Ker } A = \text{Vect} \left(\left\{ P_\sigma \begin{pmatrix} -\tilde{B}'^{-1}\tilde{B}''E_1 \\ E_1 \end{pmatrix}, \dots, P_\sigma \begin{pmatrix} -\tilde{B}'^{-1}\tilde{B}''E_{n-r} \\ E_{n-r} \end{pmatrix} \right\} \right)$$

En fait, grâce à ce résultat, en posant pour tout $j \in \llbracket 1; n \rrbracket$, $e_j = (\delta_{i,j})_{i \in \llbracket 1; n \rrbracket}$ le j -ème vecteur de la base canonique de \mathbb{K}^n , on remarque que le projecteur

$$\pi : \begin{cases} \text{Ker } A & \longrightarrow \text{Vect}(e_{\sigma^{-1}(r+1)}, \dots, e_{\sigma^{-1}(n)}) \\ x_1e_1 + \dots + x_ne_n & \longmapsto x_{\sigma^{-1}(r+1)}e_{\sigma^{-1}(r+1)} + \dots + x_{\sigma^{-1}(n)}e_{\sigma^{-1}(n)} \end{cases}$$

est un isomorphisme. En effet, si on pose pour tout $i \in \llbracket 1; n-r \rrbracket$, $U_i = P_\sigma \begin{pmatrix} -\tilde{B}'^{-1}\tilde{B}''E_i \\ E_i \end{pmatrix}$, on peut facilement voir que pour tout $i \in \llbracket 1; n-r \rrbracket$,

$$\pi(U_i) = e_{\sigma^{-1}(r+i)}$$

et les deux familles (U_1, \dots, U_{n-r}) et $(e_{\sigma^{-1}(r+1)}, \dots, e_{\sigma^{-1}(n)})$ sont toutes les deux des bases de respectivement $\text{Ker } A$ et $\text{Vect}(e_{\sigma^{-1}(r+1)}, \dots, e_{\sigma^{-1}(n)})$ donc π est bien un isomorphisme.

Ceci signifie que tout élément de $\text{Ker } A$ peut être identifié d'une manière unique via ses coordonnées d'indices $\{\sigma^{-1}(r+1), \dots, \sigma^{-1}(n)\}$.

VI Comment résoudre $AX = B$ en pratique ?

On suppose toujours que $A \in \mathcal{M}_n(\mathbb{K})$ et $B \in \mathbb{K}^n$ et on pose $r = \text{rg } A$. Lorsque $r = n$, il s'agit d'un système de Cramer qu'on peut résoudre avec le pivot de Gauss par exemple. On sait d'après la proposition I.1 que l'ensemble des solutions \mathcal{S} de l'équation $AX = B$ s'écrit sous forme de $\mathcal{S} = X_0 + \mathcal{S}_0$ avec X_0 une solution de $AX = B$ et \mathcal{S}_0 l'ensemble des solutions de l'équation $AX = 0$, i.e. $\mathcal{S}_0 = \text{Ker } A$. Pour déterminer $\text{Ker } A$, il suffit d'appliquer ce qu'on vient de voir dans la section précédente. Il suffit donc de trouver une solution particulière X_0 du système. Nous ne détaillerons pas comment la trouver, mais il suffit de vérifier que $B \in \text{Im } A$ (si ce n'est pas le cas le système n'a pas de solution), d'éliminer $n-r$ lignes, fixer $n-r$ variables et résoudre un système de Cramer de taille r .

Correction de l'exercice VII.15. :

Posons $r = \text{rg } A$. On sait qu'il existe $(P, Q) \in \text{GL}_n(\mathbb{K}) \times \text{GL}_m(\mathbb{K})$ tels que

$$A = P \underbrace{\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 0 \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}}_{J_r} Q$$

où J_r a r coefficients égaux à 1 sur la diagonale. On a alors $A^T = Q^T J_r^T P^T = Q^T J_r P^T$ et alors $\text{rg } A^T = \text{rg}(Q^T J_r P^T) = \text{rg } J_r = r$.

Correction de l'exercice II.3. :

Supposons par l'absurde que $A \notin \text{GL}_n(\mathbb{C})$. Il existe alors $X = (x_1, \dots, x_n)^T \in \mathbb{C}^n$ tel que $AX = 0$. Considérons alors $i_0 \in \llbracket 1; n \rrbracket$ tel que $0 < |x_{i_0}| = \max_{1 \leq j \leq n} |x_j|$. Le coefficient de position i_0 du vecteur AX est égal à 0, c'est à dire

$$\sum_{j=1}^n a_{i_0,j} x_j = 0 \quad \text{i.e.} \quad a_{i_0,i_0} x_{i_0} = - \sum_{j=1, j \neq i_0}^n a_{i_0,j} x_j$$

et alors

$$|a_{i_0,i_0}| |x_{i_0}| = \left| \sum_{j=1, j \neq i_0}^n a_{i_0,j} x_j \right| \leq |x_{i_0}| \sum_{j=1, j \neq i_0}^n |a_{i_0,j}|$$

$|x_{i_0}|$ est strictement positif, on peut donc simplifier des deux côtés et obtenir

$$|a_{i_0,i_0}| \leq \sum_{j=1, j \neq i_0}^n |a_{i_0,j}|$$

ce qui est en contradiction avec les hypothèses.

Correction de l'exercice II.3. :

C'est une application directe du lemme d'Hadamard. En effet, si λ est une valeur propre de A , alors $A - \lambda I_n$ n'est pas inversible et donc il existe $i \in \llbracket 1; n \rrbracket$ tel que

$$|a_{i,i} - \lambda| \leq \sum_{\substack{j=1 \\ j \neq i}}^n |a_{i,j}| \quad \text{i.e.} \quad \lambda \in \bigcup_{i=1}^n B_f \left(a_{i,i}, \sum_{j=1, j \neq i}^n |a_{i,j}| \right)$$

Correction de l'exercice IV.2. :

1. On a

$$\det P_\sigma = \sum_{\gamma \in S_n} \varepsilon(\gamma) \prod_{i=1}^n [P_\sigma]_{\gamma(i),i} = \sum_{\gamma \in S_n} \varepsilon(\gamma) \underbrace{\prod_{i=1}^n \delta_{\gamma(i),\sigma(i)}}_{=0 \text{ lorsque } \gamma \neq \sigma} = \varepsilon(\sigma)$$

2. On a pour tout $i, j \in \llbracket 1; n \rrbracket$,

$$\begin{aligned} [P_\sigma P_{\sigma'}]_{i,j} &= \sum_{k=1}^n [P_\sigma]_{i,j} \times [P_{\sigma'}]_{k,j} = \sum_{k=1}^n \delta_{i,\sigma(k)} \delta_{k,\sigma'(j)} \\ &\stackrel{(1)}{=} \delta_{i,\sigma(\sigma^{-1}(i))} \delta_{\sigma^{-1}(i),\sigma'(j)} = \delta_{\sigma^{-1}(i),\sigma'(j)} \stackrel{(2)}{=} \delta_{i,\sigma \circ \sigma'(j)} = [P_{\sigma \circ \sigma'}]_{i,j} \end{aligned}$$

L'égalité (1) est vraie car le seul terme à priori non nul dans la somme $\sum_{k=1}^n \delta_{\sigma(i),k} \delta_{k,\sigma'(j)}$ est celui d'indice $k = \sigma^{-1}(i)$. L'égalité (2) est vraie car $\sigma^{-1}(i) = \sigma(j) \iff i = \sigma \circ \sigma'(j) = i$. On en déduit donc qu'on a bien $P_\sigma P_{\sigma'} = P_{\sigma \circ \sigma'}$. En particulier, on a

$$P_\sigma P_{\sigma^{-1}} = P_{\sigma \circ \sigma^{-1}} = P_{\text{Id}} = (\delta_{i,\text{Id}(j)})_{i,j \in \llbracket 1; n \rrbracket} = I$$

c'est dire que $P_\sigma^{-1} = P_{\sigma^{-1}}$.

3. Il suffit de considérer le morphisme $\psi : \begin{cases} S_n & \longrightarrow G \\ \sigma & \longmapsto P_\sigma \end{cases}$ et de montrer qu'il est bijectif.

4. On a pour tout $i, j \in \llbracket 1; n \rrbracket$

$$[AP_\sigma]_{i,j} = \sum_{k=1}^n [A]_{i,k} \times [P_\sigma]_{k,j} = \sum_{k=1}^n a_{i,k} \delta_{k,\sigma(j)} = a_{i,\sigma(j)}$$

Et donc en posant $A = (C_1 \ \dots \ C_n)$ où C_1, \dots, C_n sont les colonnes de A , on peut voir facilement que

$$AP_\sigma = (C_{\sigma(1)} \ \dots \ C_{\sigma(n)})$$

On en déduit donc que multiplier A à droite par P_σ revient à permuter les colonnes de A en appliquant σ aux indices.

On a encore une fois, pour tout $i, j \in \llbracket 1; n \rrbracket$,

$$[P_\sigma A]_{i,j} = \sum_{k=1}^n [P_\sigma]_{i,k} \times [A]_{k,j} = \sum_{k=1}^n \delta_{i,\sigma(k)} a_{k,j} \stackrel{(1)}{=} a_{\sigma^{-1}(i),j}$$

L'inégalité (1) est vraie car $\delta_{i,\sigma(k)}$ est non nul si et seulement si $i = \sigma(k)$, i.e. $k = \sigma^{-1}(i)$. On en déduit donc que multiplier A à gauche par P_σ revient à permuter les lignes de A en appliquant σ^{-1} aux indices.

On a enfin pour tout $i \in \llbracket 1; n \rrbracket$,

$$[P_\sigma X]_i = \sum_{k=1}^n [P_\sigma]_{i,k} \times x_k = \sum_{k=1}^n \delta_{i,\sigma(k)} x_k = x_{\sigma^{-1}(i)}$$

On en déduit donc que multiplier X à gauche par P_σ revient à permuter les coordonnées de X en appliquant σ^{-1} aux indices.



CHAPITRE 28

Réduction d'endomorphisme

Notations

Introduisons tout d'abord quelques notations. Soit \mathbb{K} un corps commutatif et E un \mathbb{K} -espace vectoriel de dimension $n \in \mathbb{N}^*$. Soit $u \in \mathcal{L}(E)$ et $A \in \mathcal{M}_n(\mathbb{K})$.

- Si β est une base de E alors $[u]_\beta$ est la matrice de $\mathcal{M}_n(\mathbb{K})$ dont les colonnes sont les coordonnées de l'image de chaque élément de β par u dans la base β .
- Pour toute base β de \mathbb{K}^n , on note $[A]_\beta = PAP^{-1}$ avec P la matrice dont les colonnes sont la représentation des éléments de β dans la base canonique.
- Pour toutes matrices $A, B \in \mathcal{M}_n(\mathbb{C})$, on écrit $A \simeq B$ s'il existe $P \in \mathrm{GL}_n(\mathbb{K})$ tel que $A = PBP^{-1}$.
- Si F et G sont deux \mathbb{K} -espaces vectoriels, on écrit $F \approx G$ s'ils sont isomorphes, i.e. il existe $\phi \in \mathcal{L}(F, G)$ un endomorphisme inversible tel que $\phi(F) = G$.
- On note $\mathrm{Com}(u) = \{v \in \mathcal{L}(E), v \circ u = u \circ v\}$.
- On note $\mathrm{Com}(A) = \{B \in \mathcal{M}_n(\mathbb{K}), AB = BA\}$.
- On note $\mathrm{VP}(u) = \{\lambda \in \mathbb{K}, \mathrm{Ker}(u - \lambda \mathrm{Id}) \neq \{0\}\}$.
- On note $\mathrm{VP}(A) = \{\lambda \in \mathbb{K}, \mathrm{Ker}(A - \lambda I) \neq \{0\}\}$.
- Pour tout $a \in \mathbb{N}^*$, on note $\mathcal{T}_a^+(\mathbb{K})$ l'ensemble des matrices triangulaires supérieures de taille a .
- Pour toute famille (x_1, \dots, x_r) de E (resp. \mathbb{K}^n) et toute base β de E (resp. \mathbb{K}^n), on note $[(x_1, \dots, x_r)]_\beta$ la matrice de $\mathcal{M}_{n,r}(\mathbb{K})$ dont les colonnes sont les représentations des vecteurs x_i dans la base β .
- Pour tout $\lambda_1, \dots, \lambda_n \in \mathbb{K}$, on note $\mathrm{diag}(\lambda_1, \dots, \lambda_n) = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$
- Pour tout $i, j \in \llbracket 1; n \rrbracket$, on note $E_{i,j} = (\delta_{i,k}\delta_{j,l})_{k,l \in \llbracket 1; n \rrbracket} \in \mathcal{M}_n(\mathbb{K})$.
- On note A^T la transposée de A .
- On note $\langle A \rangle = \{PAP^{-1}, P \in \mathrm{GL}_n(\mathbb{K})\}$.
- Pour tout polynôme $P \in \mathbb{K}[X]$, on note $\langle P \rangle = \{QP, Q \in \mathbb{K}[X]\}$.
- On note $\mathbb{K}[u] = \{P(u), P \in \mathbb{K}[X]\}$.
- On note $\mathbb{K}[A] = \{P(A), P \in \mathbb{K}[X]\}$.
- Pour tout $P \in \mathbb{K}[X]$, on note $Z(P)$ l'ensemble des racines de P .

Préambule : sommes directes et bases adaptées

Soit \mathbb{K} un corps commutatif et E un \mathbb{K} -espace vectoriel de dimension $n \in \mathbb{N}^*$. Soit $r \in \mathbb{N}^*$ et F_1, \dots, F_r des sous espaces vectoriel de E .

On considère l'application

$$j : \begin{cases} F_1 \times \cdots \times F_r & \longrightarrow E \\ (x_1, \dots, x_r) & \longmapsto x_1 + \cdots + x_r \end{cases}$$

Par définition, $\mathrm{Im} j = F_1 + \cdots + F_r$. Cette somme est dite directe lorsque j est injective.

Proposition .1.

Supposons que E est de dimension finie. On considère pour tout $k \in \llbracket 1; r \rrbracket$, $(e_{k,1}, \dots, e_{k,n_k})$ une base de F_k .

1. $F_1 \times \cdots \times F_r$ est un \mathbb{K} -espace vectoriel et $\dim F_1 \times \cdots \times F_r = \sum_{k=1}^r \dim F_k$.
2. Si les F_j sont en somme directe, alors $\dim \bigoplus_{k=1}^r F_k = \sum_{k=1}^r \dim F_k$
3. Si les F_j sont en somme directe, alors $(e_{1,1}, \dots, e_{1,n_1}, \dots, e_{r,1}, \dots, e_{r,n_r})$ est une base de $\bigoplus_{k=1}^r F_k$.

Preuve :

1. On considère la famille $\mathcal{B} = \{(0, \dots, 0, e_{k,l}, 0, \dots, 0), k \in \llbracket 1; r \rrbracket, l \in \llbracket 1; n_k \rrbracket\}$. \mathcal{B} est une base de $F_1 \times \cdots \times F_r$ et $|\mathcal{B}| = \sum_{k=1}^r n_k = \sum_{k=1}^r \dim F_k$. D'où le résultat.
2. j est un morphisme injectif, donc

$$\sum_{k=1}^r \dim F_k = \dim F_1 \times \cdots \times F_r = \dim j(F_1 \times \cdots \times F_r) = \dim \bigoplus_{k=1}^r F_k$$

3. Posons $\mathcal{B}' = (e_{1,1}, \dots, e_{1,n_1}, \dots, e_{r,1}, \dots, e_{r,n_r})$. On a

$$\begin{aligned} \text{Vect}(\mathcal{B}') &= \text{Vect}(e_{1,1}, \dots, e_{1,n_1}) + \cdots + \text{Vect}(e_{r,n_r}, \dots, e_{r,n_r}) \\ &= F_1 \oplus \cdots \oplus F_r \end{aligned}$$

Donc \mathcal{B}' est une famille génératrice (de $\bigoplus_{k=1}^r F_k$) de taille $n_1 + \cdots + n_r = \sum_{k=1}^r \dim F_k = \dim \bigoplus_{k=1}^r F_k$, et alors \mathcal{B}' est une base de $\bigoplus_{k=1}^r F_k$.

Objectif du chapitre : Pour une application linéaire $u \in \mathcal{L}(E)$ ou matrice $A \in \mathcal{M}_n(\mathbb{K})$ donnée, on souhaite trouver une base β ou une matrice $P \in \text{GL}_n(\mathbb{K})$ où la matrice de u (resp. $P^{-1}AP$) est simple

$$P^{-1}AP = [u]_\beta = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \text{ ou } P^{-1}AP = [u]_\beta = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

avec $\lambda_1, \dots, \lambda_r \in \mathbb{K}$. Ou alors si u est nilpotente,

$$P^{-1}AP = [u]_\beta = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}$$

Ou alors

$$P^{-1}AP = [u]_\beta = \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_k \end{pmatrix}$$

avec pour tout $k \in \llbracket 1; r \rrbracket$, J_k un bloc de Jordan, i.e.

$$J_k = \begin{pmatrix} a_k & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & a_k \end{pmatrix}$$

avec $a_k \in \mathbb{K}$. Ou alors sous forme de matrice compagnon

$$P^{-1}AP = [u]_\beta = \begin{pmatrix} 0 & & -a_0 \\ 1 & \ddots & \vdots \\ & \ddots & \ddots & \vdots \\ & & 1 & -a_{n-1} \end{pmatrix}$$

avec $a_0, \dots, a_{n-1} \in \mathbb{K}$.

I Stabilité

Dans cette partie, on considère u un endomorphisme de E .

Définition I.1.

Une sous-espace vectoriel F de E est stable par u si $u(F) \subset F$.

Proposition I.2.

Soit F et G deux sous-espaces vectoriels de E .

1. Si F et G sont stables par u , alors $F + G$ et $F \cap G$ le sont aussi.
2. Si F est de dimension finie, est stable par u et $F \cap \text{Ker } u = \{0\}$, alors $u(F) = F$.
3. u est une homothétie $\iff u$ laisse stable tout sous-espace de E

Preuve

1. Supposons que F et G sont stables par u et soient $x, y \in E$.
 - Supposons que $x \in F$ et $y \in G$. Montrons que $u(x+y) \in F+G$.

Par stabilité de F et G , on a $u(x) \in F$ et $u(y) \in G$ donc $u(x+y) = u(x) + u(y) \in F+G$, donc $F+G$ est stable par u .
 - Supposons que $x \in F \cap G$.

On a $x \in F$ et $x \in G$, donc $u(x) \in F$ et $u(x) \in G$ et alors $u(x) \in F \cap G$. On en déduit que $F \cap G$ est stable par u .
2. On considère l'application $\tilde{u} : \begin{cases} F & \longrightarrow F \\ x & \longmapsto u(x) \end{cases}$. On a $\text{Ker } \tilde{u} = \text{Ker } u \cap F$ et en utilisant le théorème du rang, on a

$$\dim \text{Ker } \tilde{u} + \text{rg } \tilde{u} = \dim F$$

donc

$$\dim \text{Ker } u \cap F + \dim u(F) = \dim F$$

et finalement

$$\dim u(F) = \dim F$$

De plus, $u(F) \subset F$, donc $u(F) = F$.

3. Montrons le résultat par double implication. Remarquons tout d'abord que si $E = \{0\}$, alors le résultat est évident. Supposons donc que $E \neq \{0\}$.

$\rightarrow (\Rightarrow)$ Le sens direct est une conséquence de la stabilité de F par multiplication par un scalaire.

$\rightarrow (\Leftarrow)$ Supposons que u laisse stable tout sous-espace de E .

Pour tout $x, y \in E \setminus \{0\}$, u laisse stable $\text{Vect}(x)$ et $\text{Vect}(y)$, donc il existe $\lambda_x, \lambda_y \in \mathbb{K}$ vérifiant

$$u(x) = \lambda_x x \text{ et } u(y) = \lambda_y y$$

u laisse aussi $\text{Vect}(x + y)$ stable, donc il existe λ_{x+y} vérifiant $u(x + y) = \lambda_{x+y}(x + y)$. On a alors

$$\lambda_{x+y}(x + y) = u(x + y) = u(x) + u(y) = \lambda_x x + \lambda_y y$$

et alors

$$(\lambda_{x+y} - \lambda_x)x + (\lambda_{x+y} - \lambda_y)y = 0$$

- Si (x, y) est libre, alors $\lambda_{x+y} - \lambda_x = 0$ et $\lambda_{x+y} - \lambda_y = 0$, et alors $\lambda_x = \lambda_{x+y} = \lambda_y$.
- Si (x, y) est liée, i.e. il existe $\lambda \in \mathbb{K}$ tel que $x = \lambda y$, alors

$$\lambda_y y = u(y) = \lambda u(x) = \lambda \lambda_x x = \lambda_x y$$

et donc, puisque $y \neq 0$, $\lambda_x = \lambda_y$.

On a alors $x \mapsto \lambda_x$ est constante sur $\mathbb{E} \setminus \{0\}$, il existe donc $\lambda \in \mathbb{K}$ tel que pour tout $x \in E \setminus \{0\}$, $u(x) = \lambda x$. Cette propriété est en particulier vraie pour $x = 0$, donc pour tout $x \in E$, $u(x) = \lambda x$, i.e. u est une homothétie.

Exemple : Les sous espaces $\{0\}$, $\text{Im } u^k$ et $\text{Ker } u^k$ avec $k \in \mathbb{N}$ sont stables par u .

Proposition I.3.

Soit v un endomorphisme de E . Si u et v commutent, alors v laisse $\text{Ker } u$ et $\text{Im } u$ stables. Plus généralement, $\forall P \in \mathbb{K}[X]$, $\text{Ker } P(u)$ et $\text{Im } P(u)$ sont stables par v .

Preuve : Supposons que u et v commutent.

\rightarrow Si $x \in \text{Ker } u$, alors $u(v(x)) = u \circ v(x) = v \circ u(x) = v(0) = 0$, donc $v(x) \in \text{ker } u$.

\rightarrow Si $y = u(x) \in \text{Im } u$ alors $v(y) = u(v(x))$ donc $v(y) \in \text{Im } u$.

\rightarrow Étant donné que u et v commutent, une récurrence simple permet de montrer que $\forall k \in \mathbb{N}$, u^k et v commutent également. Tout polynôme P en u est une combinaison linéaire des u^k qui commutent tous avec v , donc $P(u)$ et v commutent, et alors le point précédent nous permet d'affirmer que v laisse $\text{Ker } P(u)$ et $\text{Im } P(u)$ stables.

Remarque La réciproque est fausse en général. Prenons un contre-exemple. Soit (e_1, e_2, e_3) la base canonique de \mathbb{R}^3 . On définit u et v comme suit :

$$\begin{cases} u(e_1) = 0 \\ u(e_2) = e_3 \\ u(e_3) = e_3 \end{cases} \quad \text{et} \quad \begin{cases} v(e_1) = e_1 \\ v(e_2) = 0 \\ v(e_3) = e_3 \end{cases}$$

On peut facilement voir que v laisse stable $\text{Ker } u$ et $\text{Im } u$, mais

$$\begin{cases} u \circ v(e_2) = 0 \\ v \circ u(e_2) = e_3 \end{cases}$$

Proposition I.4.

Soit F un sous-espace vectoriel de E , β_1 une base de F et β_2 une base d'un supplémentaire de F . En posant $\beta = (\beta_1, \beta_2)$ la concaténation des deux bases et $p = \dim F = |\beta_1|$, pour tout $u \in \mathcal{L}(E)$, on a équivalence entre les propositions suivantes.

1. u laisse stable F .
2. $\exists (A, B, C) \in \mathcal{M}_p(\mathbb{K}) \times \mathcal{M}_{n-p}(\mathbb{K}) \times \mathcal{M}_{p, n-p}(\mathbb{K})$, $[u]_\beta = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$

Preuve

- $\rightarrow (1) \Rightarrow (2)$ Supposons que u laisse stable F . Pour tout $e \in \beta_1$, $u(e) \in F = \text{Vect}(\beta_1)$ car u stabilise F , donc les coefficients dans la famille β_2 de e sont nuls.
- $\rightarrow (2) \Rightarrow (1)$ Pour tout $e \in \beta_1$, $[u(e)]_\beta$ a des coefficients nuls dans les $|\beta_2|$ dernières coordonnées, donc $u(e) \in \text{Vect}(\beta_1) = F$ pour tout $e \in \beta_1$. Par combinaison linéaire, on peut conclure que $u(F) \subset F$.

Proposition I.5.

Soit $r \in \mathbb{N}^*$ et F_1, \dots, F_r des sous-espaces vectoriels de E non réduits à $\{0\}$ de dimensions respectives n_1, \dots, n_r . On suppose que $E = \bigoplus_{k=1}^r F_k$. Pour tout $j \in \llbracket 1; r \rrbracket$, on considère β_j une base de F_j . Soit $\beta = (\beta_1, \dots, \beta_r)$ la concaténation des β_j . On a alors pour tout $u \in \mathcal{L}(E)$, on a équivalence entre les deux propositions suivantes.

1. u laisse stable F_j pour tout j .

2. $\exists (A_1, \dots, A_r) \in \mathcal{M}_{n_1}(\mathbb{K}) \times \cdots \times \mathcal{M}_{n_r}(\mathbb{K})$, $[u]_\beta = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_r \end{pmatrix}$

Preuve

- $\rightarrow (1) \Rightarrow (2)$ Soit $k \in \llbracket 1; r \rrbracket$. Pour tout $e \in \beta_k$, $u(e) \in \text{Vect}(\beta_k)$, donc la sous-matrice de $[u]_\beta$ contenant des colonnes de rang entre $|\beta_1| + \cdots + |\beta_{k-1}| + 1$ et $|\beta_1| + \cdots + |\beta_k|$, i.e. la représentation de

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \\ A_k \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

l'image de la base β_k par u dans la base β s'écrit avec $A_k \in \mathcal{M}_{n_k}(\mathbb{K})$. On en déduit donc

directement que la matrice de u dans la base β s'écrit comme avec $(A_1, \dots, A_r) \in \mathcal{M}_{n_1}(\mathbb{K}) \times \cdots \times \mathcal{M}_{n_r}(\mathbb{K})$.

- $\rightarrow (2) \Rightarrow (1)$ De la même manière, pour tout $k \in \llbracket 1; r \rrbracket$, pour tout $e \in \beta_k$, étant donné la forme de la matrice, on voit que tous les coefficients de $u(e)$ dans $\beta \setminus \beta_k$ sont nuls, donc $u(e) \in \text{Vect}(F_k)$ et donc finalement $u(\text{Vect}(\beta_k)) \subset F_k$ i.e. $u(F_k) \subset F_k$.

II Éléments propres

Définition II.1.

Soit $u \in \mathcal{L}(E)$. Une vecteur $x \in E$ est appelé vecteur propre de u lorsque $x \neq 0$ et qu'il existe $\lambda \in \mathbb{K}$ tel que $u(x) = \lambda x$. Un tel scalaire λ est unique et est appelé valeur propre de u .

Proposition II.2.

Pour tout $\lambda \in \mathbb{K}$, on a l'équivalence suivante

$$\lambda \text{ valeur propre de } u \iff \text{Ker}(u - \lambda \text{Id}) \neq \{0\}$$

Preuve : La preuve de ce résultat ne présente pas de difficulté et est laissée comme exercice au lecteur.

Vocabulaire : Lorsque $u \in \mathcal{L}(E)$ et $\lambda \in \mathbb{K}$, $E_{\lambda,u} = \text{Ker}(u - \lambda \text{Id})$ est appelé espace propre de u associé à λ . Lorsqu'il n'y a pas ambiguïté sur l'endomorphisme associé à cet espace, on notera simplement $E_{\lambda,u} = E_\lambda$.

Proposition II.3.

Soit $u \in \mathcal{L}(E)$

1. Soit $x \in E \setminus \{0\}$. On a l'équivalence

$$x \text{ est un vecteur propre de } u \iff \text{La droite } \mathbb{K}x \text{ est stable par } u$$

2. Pour tout $x \in E$ l'application $\tilde{u} : \begin{cases} E_{\lambda,u} & \longrightarrow E_{\lambda,u} \\ x & \longmapsto \lambda x \end{cases}$ commute avec tout élément de $\mathcal{L}(E_{\lambda,u})$.

Preuve : Même chose pour ces deux propositions.

Proposition II.4.

Si E est de dimension finie non réduit à $\{0\}$ et que $\mathbb{K} = \mathbb{C}$, alors u possède au moins une valeur propre.

Preuve : Soit β une base de E . En posant $[u]_\beta = (a_{i,j})_{i,j \in \llbracket 1, n \rrbracket}$, on a

$$\lambda \text{ est une valeur propre de } u \iff \text{Ker}(u - \lambda \text{Id}) \neq \{0\}$$

$$\iff \det([u]_\beta - \lambda I) = 0$$

$$\iff \begin{vmatrix} a_{1,1} - \lambda & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} - \lambda & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n-1} & a_{n,n} - \lambda \end{vmatrix} = 0$$

L'application $\lambda \mapsto \det([u]_\beta - \lambda I)$ est donc une application polynomiale dans \mathbb{C} de degré n , elle admet donc au moins une racine λ , donc il existe au moins un $\lambda \in \mathbb{C}$ vérifiant $\text{Ker}(u - \lambda \text{Id}) \neq \{0\}$, i.e. λ est une valeur propre.

Exercice II.5.

Supposons que \mathbb{K} soit égal à \mathbb{R} ou \mathbb{C} . Soit $n \geq 2$. Existe-t-il un plan P de $\mathcal{L}(\mathbb{K}^n)$ tel que $P \setminus \{0\} \subset \text{GL}(\mathbb{K})$?

Notation : Pour tout $u, v \in \mathcal{L}(E)$, on note $[u, v] = u \circ v - v \circ u$.

Proposition II.6.

Soit $u, v \in \mathcal{L}(E)$ tel que $[u, v] = 0$. Si λ est une valeur propre de u , alors v laisse stable $E_{\lambda, u} = \text{Ker}(u - \lambda \text{Id})$.

Preuve : On a $[u, v] = 0$, donc $[u - \lambda \text{Id}, v] = 0$, i.e. $u - \lambda \text{Id}$ et v commutent, donc d'après la proposition I.3, v laisse stable $\text{Ker}(u - \lambda \text{Id})$.

Exercice II.7.

On dit qu'une partie L de $\mathcal{L}(\mathbb{C}^n)$ est irréductible lorsque les seuls sous-espaces vectoriels de E qui sont stables par tous les éléments de L sont $\{0\}$ et E . Soit L une partie irréductible de $\mathcal{L}(\mathbb{C}^n)$ et u un élément de $\mathcal{L}(\mathbb{C}^n)$ qui commute avec tous les éléments de L . Montrer que u est une homothétie.

Proposition II.8.

Supposons que E est un espace vectoriel muni de $\|\cdot\|$ et $u \in \mathcal{L}_c(E)$. Pour toute valeur propre λ de u , on a $|\lambda| \leq \||u|||$.

Preuve : Soit λ une valeur propre de u et x un vecteur propre pour λ , i.e. $u(x) = \lambda x$ et $x \neq 0$. On a alors

$$|\lambda| \|x\| = \|u(x)\| \leq \||u||| \times \|x\|$$

x est non nul, on peut donc simplifier par $\|x\|$ pour obtenir $|\lambda| \leq \||u|||$.

Remarque : Soit $u \in \mathcal{L}(E)$ et F un sous-espace vectoriel de E . Si F est stable par u , en considérant l'endomorphisme $v : \begin{cases} F & \longrightarrow F \\ x & \mapsto u(x) \end{cases}$, on a $\text{Ker}(v - \lambda \text{Id}) = F \cap \text{Ker}(u - \lambda \text{Id})$.

III Endomorphismes et matrices diagonalisables

Définition III.1.

On dit que $u \in \mathcal{L}(E)$ est diagonalisable lorsqu'il existe $r \in \mathbb{N}^*$ et $\lambda_1, \dots, \lambda_r \in \mathbb{K}$ tels que $E = E_{\lambda_1, u} + \dots + E_{\lambda_r, u}$.

Lemme III.2.

Soit $u \in \mathcal{L}(E)$, $p \in \mathbb{N}^*$, $\lambda_1, \dots, \lambda_p$ des valeurs propres deux à deux distinctes de u et $x_1, \dots, x_p \in E$ des vecteurs propres respectivement associés à $\lambda_1, \dots, \lambda_p$. La famille (x_1, \dots, x_p) est libre.

Preuve : Nous allons montrer ce lemme par récurrence sur p .

- Pour le cas $p = 1$, x_1 est un vecteur propre, il est donc non nul et alors la famille (x_1) est libre.
- Soit $p \in \mathbb{N}^*$. Supposons que la propriété est vraie pour p . Soit $\mu_1, \dots, \mu_{p+1} \in \mathbb{K}$ tels que

$$\mu_1 x_1 + \dots + \mu_{p+1} x_{p+1} = 0 \quad (1)$$

En appliquant u aux deux côtés, on obtient

$$\mu_1 \lambda_1 x_1 + \dots + \mu_{p+1} \lambda_{p+1} x_{p+1} = 0 \quad (2)$$

En faisant $(1) \times \lambda_{p+1} - (2)$, on obtient

$$\mu_1 (\lambda_{p+1} - \lambda_1) x_1 + \dots + \mu_p (\lambda_{p+1} - \lambda_p) x_p = 0$$

Par hypothèse de récurrence, on a que la famille (x_1, \dots, x_p) est libre, donc pour tout $k \in \llbracket 1; p \rrbracket$, $\mu_k (\lambda_{p+1} - \lambda_k) = 0$. $\lambda_1, \dots, \lambda_{p+1}$ sont deux à deux distinctes par hypothèse donc pour tout $k \in \llbracket 1; p \rrbracket$, $\mu_k = 0$ et alors (1) devient

$$\mu_{p+1} x_{p+1} = 0$$

ce qui finalement implique que pour tout $k \in \llbracket 1; p+1 \rrbracket$, $\mu_k = 0$ i.e. (x_1, \dots, x_{p+1}) est libre, d'où le résultat voulu.

Application : La famille $(f_\alpha)_{\alpha \in \mathbb{R}} = (x \mapsto x^\alpha)_{\alpha \in \mathbb{R}}$ est libre dans $\mathcal{C}^\infty(\mathbb{R}^*, \mathbb{R})$. En effet, en posant $u : f \mapsto (x \mapsto xf'(x))$, (f_α) est une famille de vecteurs propres associés à des valeurs propres deux à deux distinctes de u , elle est donc libre. On peut dire la même chose de la famille $(g_\beta)_{\beta \in \mathbb{C}}$, avec pour tout $\beta \in \mathbb{C}$, $g_\beta : x \mapsto e^{\beta x}$.

Proposition III.3.

On suppose que E est de dimension finie. Soit $u \in \mathcal{L}(E)$. Les propositions suivantes sont équivalentes

1. u est diagonalisable.
2. Il existe une base de E composée de vecteurs propres de u .
3. Il existe une base de E telle que $[u]_\beta$ est diagonale.
4. $\sum_{k=1}^p E_{\lambda_k, u} = E$, avec $\lambda_1, \dots, \lambda_p$ les valeurs propres de u .

Preuve

→ (1) ⇒ (2) Prenons $\lambda_1, \dots, \lambda_p$ comme dans la définition III.1. Quitte à éliminer les λ_i tels que $E_{\lambda_i, u} = \{0\}$, on peut supposer sans perte de généralité que $\forall i \in \llbracket 1; p \rrbracket E_{\lambda_i, u} \neq \{0\}$ et que les λ_i sont distincts. Le lemme III.2 nous permet de dire que toute famille de vecteurs $(x_1, \dots, x_p) \in E_{\lambda_1, u} \times \dots \times E_{\lambda_p, u}$ est libre et que donc la somme $E = \sum_{i=1}^p E_{\lambda_i, u}$ est directe.

Chacun de ces espaces étant de dimension finie (non nulle), on peut alors prendre, pour chaque i , une base $(b_i^1, \dots, b_i^{p_i})$ de E_i avec $p_i = \dim E_{\lambda_i, u}$. Il est clair que la concaténation de ces bases est une base de $E = \bigoplus_{i=1}^p E_{\lambda_i, u}$ et que chaque élément de cette dernière est un vecteur propre de u .

→ (2) ⇒ (3) Si (b_1, \dots, b_n) est une base de E formée de vecteurs propres de u , et que pour tout $i \in \llbracket 1; p \rrbracket$, b_i est associé à la valeur propre λ_i , alors la matrice de u dans cette base est la matrice diagonale $\text{diag}(\lambda_1, \dots, \lambda_n)$.

→ (3) ⇒ (4) Prenons une base $\beta = (\beta_1, \dots, \beta_n)$ qui rend $[u]_\beta$ diagonale. Il est alors clair que pour tout $i \in \llbracket 1; p \rrbracket$, il existe $\lambda_i \in \mathbb{K}$ tel que β_i est un vecteur propre de u , associé à λ_i (les λ_i ne sont pas

forcément distincts). On a alors en notant $\text{VP}(u)$ l'ensemble (fini) des valeurs propres de u

$$E = \text{Vect}(\beta_1, \dots, \beta_n) \subset \text{Vect}(E_{\lambda_1}, \dots, E_{\lambda_n}) = \sum_{i=1}^n E_{\lambda_i} \subset \sum_{\lambda \in \text{VP}(u)} E_{\lambda}$$

d'où le résultat.

→ (4) ⇒ (1) Direct.

Remarque 1 : Si u possède $n = \dim E$ valeurs propres différentes, alors u est diagonalisable et chaque espace propre est de dimension exactement une.

Ceci étant car, en notant $\lambda_1, \dots, \lambda_n$ ces n valeurs propres différentes, que

$$n \geq \dim \left(\sum_{i=1}^n E_{\lambda_i} \right) \stackrel{\text{lemme III.2}}{=} \dim \left(\bigoplus_{i=1}^n E_{\lambda_i} \right) = \sum_{i=1}^n \dim(E_{\lambda_i}) \geq n$$

On a alors $\dim \left(\bigoplus_{i=1}^n E_{\lambda_i} \right) = n = \dim E$, i.e. $E = \bigoplus_{i=1}^n E_{\lambda_i}$ et tous les $E_{\lambda_i, u}$ ne peuvent pas avoir une dimension strictement supérieure à 1 ou égale à 0, ils sont donc de dimension 1. On a donc bien les deux résultats voulus.

Remarque 2 : Lorsque u est diagonalisable, il est facile de retrouver son image et son noyau. En effet, considérons un base de vecteurs propres de u $\beta = (b_1, \dots, b_n)$ puis ordonnons la de manière à ce que les valeurs propres associées à b_1, \dots, b_p soient non nulles et celles associées à b_{p+1}, \dots, b_n soient nulles. Alors $\text{Im}(u) = \text{Vect}(b_1, \dots, b_p)$ et $\text{Ker}(u) = \text{Vect}(b_{p+1}, \dots, b_n)$.

Preuve

Une matrice diagonale à coefficients diagonaux tous non nuls dans \mathbb{K} est inversible. Ainsi, dans la base β , $[u]_{\beta}$ s'écrit :

$$\begin{pmatrix} A & 0_{\mathcal{M}_{p,n-p}(\mathbb{K})} \\ 0_{\mathcal{M}_{n-p,p}(\mathbb{K})} & 0_{\mathcal{M}_{n-p}(\mathbb{K})} \end{pmatrix}$$

Avec A une matrice diagonale à coefficients diagonaux non nuls. On en déduit donc que

$$\text{Ker}(u) = \left\{ a \in E, \exists v \in \mathbb{K}^{n-p}, [a]_{\beta} = \begin{pmatrix} 0_{\mathbb{K}^p} \\ v \end{pmatrix}, \right\} = \text{Vect}(e_{p+1}, \dots, e_n)$$

$$\text{Im}(u) = \left\{ a \in E, \exists v \in \mathbb{K}^p, [a]_{\beta} = \begin{pmatrix} v \\ 0_{\mathbb{K}^{n-p}} \end{pmatrix}, \right\} = \text{Vect}(e_1, \dots, e_p)$$

Proposition III.4.

Soit $u \in \mathcal{L}(E)$, $w \in GL(E)$ et $v = w \circ u \circ w^{-1}$

1. $\lambda \in \mathbb{K}$ est une valeur propre de u si et seulement si c'est une valeur propre de v et $E_{\lambda,v} = w(E_{\lambda,u})$.
2. u est diagonalisable si et seulement si v l'est.

1. Soit $\lambda \in \mathbb{K}$. On a

$$\begin{aligned} x \in E_{\lambda,v} &\iff w \circ u \circ w^{-1}(x) = \lambda x \\ &\iff u \circ w^{-1}(x) = \lambda w^{-1}(x) \\ &\iff w^{-1}(x) \in E_{\lambda,u} \iff x \in w(E_{\lambda,u}) \end{aligned}$$

D'où $E_{\lambda,v} = w(E_{\lambda,u})$ et donc

$$\lambda \in \text{VP}(v) \iff E_{\lambda,v} = w(E_{\lambda,u}) \neq \{0\} \underset{w \in GL(E)}{\iff} E_{\lambda,u} \neq \{0\} \iff \lambda \in \text{VP}(u)$$

2. Soit $\lambda_1, \dots, \lambda_r$ les valeurs propres de u et v . On a alors

$$\begin{aligned} u \text{ est diagonalisable} &\iff \sum_{i=1}^r E_{\lambda_i,u} = E \\ &\underset{w \in GL(E)}{\iff} \sum_{i=1}^r w(E_{\lambda_i,u}) = \sum_{i=1}^r E_{\lambda_i,v} = E \iff v \text{ est diagonalisable} \end{aligned}$$

Exercice III.5.

Soit $u \in \mathcal{L}(E)$ ayant n valeurs propres distinctes et v un endomorphisme de E qui commute avec u . Montrer que v est diagonalisable et que v est un polynôme en u .

Proposition III.6.

Soit $A \in \mathcal{M}_n(\mathbb{K})$ et $E = \mathbb{K}^n$. Les propriétés suivantes sont équivalentes :

1. $\exists P \in GL_n(\mathbb{K}), \exists \Delta \in D_n(\mathbb{K}), P^{-1}AP = \Delta$
2. $f_A : \begin{cases} \mathbb{K}^n & \longrightarrow \mathbb{K}^n \\ X & \longmapsto AX \end{cases}$ est diagonalisable.
3. Il existe $u \in \mathcal{L}(E)$ et β une base de E tels que u diagonalisable et $[u]_\beta = A$
4. Pour tout $u \in \mathcal{L}(E)$ et pour tout β base de E , on a l'implication

$$[u]_\beta = A \implies u \text{ est diagonalisable}$$

Preuve

- $\rightarrow (1) \Rightarrow (2)$ Soit β la base associée à la matrice P . Alors $[f_A]_\beta = P^{-1}AP = \Delta$ est diagonale.
 $\rightarrow (2) \Rightarrow (3)$ Soit $\beta = (e_1, \dots, e_n)$ une base de E et considérons l'application

$$u : \begin{cases} E & \longrightarrow E \\ \sum_{i=1}^n x_i e_i & \longmapsto \sum_{i=1}^n y_i e_i \end{cases}$$

où $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = f_A(X)$ avec $X = (x_1, \dots, x_n)^T$. Une vérification rapide nous permet de voir que $[u]_\beta = A$.

De plus, en considérant $((f_{1,i})_{i \in \llbracket 1;n \rrbracket}, \dots, (f_{n,i})_{i \in \llbracket 1;n \rrbracket})$ une base de vecteurs propres de f_A , il est facile de voir que la famille (f_1, \dots, f_n) telle que pour tout $k \in \llbracket 1;n \rrbracket$, $f_k = f_{k,1}e_1 + \dots + f_{k,n}e_n$ est une base de vecteurs propres de u , ce qui nous permet d'affirmer que u est diagonalisable.

- $\rightarrow (3) \Rightarrow (1)$ Soit $u \in \mathcal{L}(E)$ et β une base tel que $[u]_\beta = A$. Soit γ une base de diagonalisation de u et P la matrice de passage de γ à β . On a alors

$$[u]_\gamma = P[u]_\beta P^{-1} = P^{-1}AP$$

On a de plus, pour tout $i \in \llbracket 1;n \rrbracket$, si e est le i -ème vecteur de la base canonique de $\mathcal{M}_n(\mathbb{K})$ et b_i est le i -ème vecteur de la base γ , alors il existe $\lambda_i \in \mathbb{K}$ tel que $u(b_i) = \lambda_i b_i$, i.e., en passant aux

matrices dans la base γ , $[u]_\gamma e_i = \lambda e_i$, donc il existe une matrice diagonale Δ telle que $[u]_\gamma = \Delta$. On en déduit donc finalement que $A = P^{-1}\Delta P$.

$\rightarrow (4) \Leftrightarrow (1)$ Laissé comme exercice au lecteur.

Vocabulaire : Lorsque A vérifie l'une de ces propriétés, on dit que A est diagonalisable.

IV Action des polynômes

1. Rappels

L'algèbre des polynomes $\mathbb{K}[X]$ agit naturellement sur $\mathcal{L}(E)$. Plus exactement, si $P = \sum_0^p a_k X^k$ et $u \in \mathcal{L}(E)$ alors on définit

$$\phi_u : \begin{cases} \mathbb{K}[X] & \longrightarrow \mathcal{L}(E) \\ P & \longmapsto P(u) = \sum_{k=0}^p a_k u^k \end{cases}$$

ϕ_u est alors un morphisme d'algèbre unitaire. En particulier, $I_u := \text{Ker}(\phi_u)$ est un idéal.

Rappel IV.1.

Soit $(\mathcal{A}, +, \cdot)$ un anneau commutatif. Un sous ensemble I de \mathcal{A} est appelé idéal lorsque

- $\rightarrow (I, +)$ est un sous groupe de $(\mathcal{A}, +)$.
- \rightarrow Pour tout $x \in \mathcal{A}$ et $i \in I$, $ix \in I$.

I est dit principal lorsqu'il est engendré par un seul élément i.e. il existe $x \in \mathcal{A}$ tel que $I = \langle x \rangle := x\mathcal{A}$.

Un anneau commutatif \mathcal{A} est dit principal si tout idéal de \mathcal{A} est principal.

On notera en particulier que $\mathbb{K}[X]$ est principal lorsque \mathbb{K} est un corps.

Si ce dernier est non trivial, chose toujours vraie en dimension finie, alors il est engendré par un unique polynome unitaire μ_u , appelé polynome minimal de u . Autrement dit si $P \in \mathbb{K}[X]$ et $P(u) = 0$, alors $P \in I_u$, c'est à dire qu'il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = Q(X)\mu_u(X)$, i.e. $\mu_u | P$.

$\mathbb{K}[X]$ agit similairement sur les matrices carrées et commute avec les automorphismes intérieurs (i.e. les automorphismes de la forme $M \mapsto PMP^{-1}$ avec $P \in \text{GL}_n(\mathbb{K})$) de conjugaison i.e. pour tout $P \in \text{GL}_n(\mathbb{K})$ et $Q \in \mathbb{K}[X]$, $Q(PAP^{-1}) = PQ(A)P^{-1}$.

Vocabulaire : Un élément de I_u , i.e. un polynôme P tel que $P(u) = 0_{\mathcal{L}(E)}$ est appelé un polynôme annulateur de u .

Proposition IV.2.

Soit x un vecteur propre de u de valeur propre associée λ . Les propositions suivantes sont vraies.

1. $\forall P \in \mathbb{K}[X], P(u)(x) = P(\lambda)x$
2. Si $P \in I_u$ alors $P(\lambda) = 0$
3. Soit $\lambda \in \mathbb{K}$. Alors $\mu_u(\lambda) = 0 \iff \lambda$ valeur propre de u .

En particulier, lorsque $\mathbb{K} = \mathbb{C}$, il existe $(l_\lambda)_{\lambda \in \text{VP}(u)} \in \mathbb{N}^{*\text{VP}(u)}$ tel que

$$\mu_u(X) = \prod_{\lambda \in \text{VP}(u)} (X - \lambda)^{l_\lambda}$$

Preuve :

CPGE
paradise

1. On peut montrer par une récurrence rapide que $\forall k \geq 0 u^k(x) = \lambda^k x$ (avec par convention $0^0 = 1$).
Ainsi, si $P(X) = \sum_{k=0}^d a_k X^k$, alors $P(u)(x) = \sum_{k=0}^d a_k \cdot u^k(x) = \sum_{k=0}^d a_k \cdot \lambda^k x = P(\lambda)x$.
2. On sait que $0 = P(u)(x) = P(\lambda)x$ et donc $P(\lambda) = 0$ car $x \neq 0$.
3. Soit $\lambda \in \mathbb{K}$
 - $\rightarrow (\Leftarrow)$ Il suffit d'appliquer le point (2) pour $P = \mu_u$.
 - $\rightarrow (\Rightarrow)$ $\mu_u(\lambda) = 0$, on peut donc écrire $\mu_u(X) = (X - \lambda)Q(X)$. On a alors

$$0 = \mu_u(u) = (u - \lambda \text{Id}) \circ Q(u)$$

Si λ n'est pas une valeur propre de u , la proposition II.2 nous permet d'affirmer que $u - \lambda \text{Id}$ est inversible et que donc $Q(u) = 0$, ce qui contredit la minimalité de μ_u . Donc λ est bien une valeur propre de u .

Exemple : Soit p un projecteur différent de 0 et Id . On a $\mu_p(X) = X^2 - X$.

Exercice IV.3.

Soit $u \in \mathcal{L}(E)$ tel que $u \circ u = \text{Id}$ et $u \neq \pm \text{Id}$. Montrer que $\mu_u = X^2 - 1$.

2. Décomposition des noyaux

Proposition (Lemme de décomposition des noyaux) IV.4.

Soit P_1, \dots, P_r des éléments de $\mathbb{K}[X]$, deux à deux premiers entre eux et $u \in \mathcal{L}(E)$. On a $\text{Ker } P_1 \dots P_r(u) = \bigoplus_{i=1}^r \text{Ker } P_i(u)$. En particulier, en considérant le cas où $P_i(X) = X - \lambda_i$ avec pour tout i , λ_i une valeur propre de u , on retrouve que les espaces propres sont en somme directe.

Preuve : Montrons le résultat pour $r = 2$.

Soit P et Q deux polynômes premiers entre eux et soit $x \in \text{Ker } P(u) \cap \text{Ker } Q(u)$.

P et Q sont premiers entre eux et donc par Bezout, on dispose de $A, B \in \mathbb{K}[X]$ tel que $AP + BQ = 1$. On a alors $x = AP(u)(x) + BQ(u)(x) = 0 + 0 = 0$ et alors $\text{Ker } P(u) \cap \text{Ker } Q(u) = \{0\}$. $\text{Ker } P(u)$ et $\text{Ker } Q(u)$ sont donc bien en somme directe.

Montrons à présent que $\text{Ker } PQ(u) = \text{Ker } P(u) \oplus \text{Ker } Q(u)$.

$\rightarrow (\supset)$ Si $x \in \text{Ker } P(u) \oplus \text{Ker } Q(u)$, alors en posant $x = x_{\text{Ker } P(u)} + x_{\text{Ker } Q(u)}$ on retrouve

$$PQ(u)(x) = Q(u) \circ P(u) \left(x_{\text{Ker } P(u)} \right) + P(u) \circ Q(u) \left(x_{\text{Ker } Q(u)} \right) = 0$$

$\rightarrow (\subset)$ Soit $x \in \text{Ker } PQ(u)$. La relation obtenue via Bezout nous permet d'écrire

$$x = \underbrace{AP(u)(x)}_{\in \text{Ker } Q(u)} + \underbrace{BQ(u)(x)}_{\in \text{Ker } P(u)}$$

Enfin, pour généraliser pour $r \geq 2$, on peut le faire simplement de la manière suivante. Soit $P_1, \dots, P_r \in \mathbb{K}[X]$ premiers entre eux. On a

$$\text{Ker } P_1 \dots P_r(u) = \text{Ker } P_1(u) \oplus \text{Ker } P_2 \dots P_r(u) = \dots = \bigoplus_{i=1}^r \text{Ker } P_i(u)$$

Proposition IV.5.

Soit $u \in \mathcal{L}(E)$ avec $\dim E < +\infty$. Les propriétés suivantes sont équivalentes

1. u est diagonalisable.
2. u est annulé par un polynôme scindé à racines simples (dans \mathbb{K})
3. μ_u est scindé à racines simples.

Bien entendu, on possède un théorème similaire pour les matrices.

Proposition IV.6.

Soit $A \in \mathcal{M}_n(\mathbb{K})$. Les propriétés suivantes sont équivalentes :

1. A est diagonalisable.
2. A est annulé par un polynôme scindé à racines simples (dans \mathbb{K}).
3. μ_A est scindé à racines simples.

$\rightarrow (1) \Rightarrow (2)$ A est diagonalisable, il existe donc $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ tel que A est semblable à $D = \text{diag}(\lambda_1, \dots, \lambda_n)$. Notons $\delta_1, \dots, \delta_r$ tous les scalaires λ_i en enlevant les doublons et considérons le polynôme scindé à racines simples $P(x) = \prod_{i=1}^r (X - \delta_i)$. On peut facilement vérifier que

$$P(D) = \text{diag}(P(\lambda_1), \dots, P(\lambda_n)) = 0$$

$\rightarrow (2) \Rightarrow (3)$ Soit P un polynôme scindé à racines simples annulant A . On sait que $\mu_A | P$ ($P \neq 0$ et μ_A non constant), donc μ_A est bien scindé à racines simples.

$\rightarrow (3) \Rightarrow (1)$ Écrivons $\mu_A = \prod_{i=1}^r (X - \lambda_i)$ avec les λ_i distincts. On a alors d'après le lemme de décomposition des noyaux

$$E = \text{Ker } \mu_u(u) = \bigoplus_{i=1}^r \text{Ker}(u - \lambda_i \text{Id})$$

Considérons pour tout i , β_i une base de $\text{Ker}(u - \lambda_i \text{Id})$ puis posons $\beta = (\beta_1, \dots, \beta_r)$ la concaténation de ces bases. β est une base de E . On a alors $[A]_\beta = \begin{pmatrix} \lambda_1 I_{l_1} & & \\ & \ddots & \\ & & \lambda_r I_{l_r} \end{pmatrix}$ et donc A est bien diagonalisable.

Exemple : Soit $A \in \mathcal{M}_n(\mathbb{C})$ tel que $A^m = I_n$ alors A est diagonalisable étant donné que

$$X^m - 1 = \prod_{\omega \in U_m} (X - \omega)$$

est un polynôme annulateur de u scindé à racines simples sur \mathbb{C} .

En pratique, pour des corps algébriquement clos tel que \mathbb{C} , tout polynôme est scindé, donc dire qu'un polynôme P non constant est scindé à racines simples est équivalent à ce que $P \wedge P' = 1$ ou à ne pas avoir de racines multiples i.e. ne pas avoir de racine commune à P et P' . Dans l'exemple précédent, si $m \geq 2$, alors $Z(mX^{m-1}) = \{0\}$ et 0 n'est pas racine de X^{m-1} . De même

$$X^m - 1 \wedge mX^{m-1} = (X^m - 1) \wedge X^{m-1} = (X^m - 1 - X \times X^{m-1}) \wedge X^{m-1} = 1$$

Finalement, la notion de diagonalisabilité passe aux sous-espaces. Plus exactement :

Proposition IV.7.

Soit $u \in \mathcal{L}(E)$ diagonalisable et F un sous espace vectoriel de E . Si u stabilise F (i.e. $u(F) \subset F$) alors $v := u|_F^F$ est diagonalisable.

Preuve : Soit P un polynôme scindé à racines simples tel que $P(u) = 0$. On a alors $P(v) = 0$, v est annulé par un polynôme scindé à racine simple, c'est donc un endomorphisme diagonalisable.

Remarque : Pour les endomorphismes diagonalisables, les espaces stables et $\text{Com}(u) = \{v \in \mathcal{L}(E), v \circ u = u \circ v\}$ sont faciles à caractériser. On peut voir cela à partir des deux exercices ci-dessous.

Exercice IV.8.

Soit $u \in \mathcal{L}(E)$ diagonalisable de valeurs propres $\lambda_1, \dots, \lambda_s$ distinctes. Montrer que les propositions suivantes sont équivalentes

1. $F \subset E$ est un sous-espace vectoriel de E stable par u .
2. $F = \bigoplus_{i=1}^s F \cap E_{\lambda_i, u}$.
3. Il existe une famille $(F_i)_{i \in \llbracket 1; s \rrbracket}$ de sous-espaces vectoriels de E telle que pour tout $i \in \llbracket 1; s \rrbracket$ $F_i \subset E_{\lambda_i, u}$ et $F = \bigoplus_{i=1}^s F_i$.

Exercice IV.9.

Soit $u \in \mathcal{L}(E)$ diagonalisable de valeurs propres $\lambda_1, \dots, \lambda_s$ distinctes et soit β une base de E telle que $[u]_\beta = \begin{pmatrix} \lambda_1 I_{l_1} & & 0 \\ & \ddots & \\ 0 & & \lambda_s I_{l_s} \end{pmatrix}$, avec $(l_1, \dots, l_s) \in \llbracket 1; n \rrbracket$ tel que $l_1 + \dots + l_s = n$.

Montrer que

$$\text{Com}(u) = \left\{ v \in \mathcal{L}(E), \exists (A_1, \dots, A_s) \in \mathcal{M}_{l_1}(\mathbb{K}) \times \cdots \times \mathcal{M}_{l_s}(\mathbb{K}), [v]_\beta = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_s \end{pmatrix} \right\}$$

En déduire une autre solution de l'exercice III.5.

3. Compléments : projecteurs spectraux et codiagonalisation

Proposition IV.10.

Soit $u \in \mathcal{L}(E)$ diagonalisable de valeurs propres $\lambda_1, \dots, \lambda_r$ distinctes. Les propositions suivantes sont vraies.

1. $\mu_u = \prod_{i=1}^r (X - \lambda_i)$
2. Soit (L_i) les interpolateurs de Lagrange des (λ_i) , i.e. pour tout i , L_i est l'unique polynôme de degré $r - 1$ tel que pour tout $k \neq i$ $L_i(\lambda_k) = 0$ et $L_i(\lambda_i) = 1$. On a $L_1 + \dots + L_r = 1$ et $\forall i \neq j$, $\mu_u|L_i L_j$.
3. En posant $p_i = L_i(u)$. Alors p_i est le projecteur sur $E_{\lambda_i, u}$ parallèlement à $\bigoplus_{j \neq i} E_{\lambda_j, u}$.

1. La proposition IV.5 donne le fait que μ_u est scindé à racines simples car u est diagonalisable. Ainsi, il existe $\delta_1, \dots, \delta_r \in K$ deux à deux distincts tels que $\mu_u = \prod_{i=1}^s (X - \lambda_i)$ où les λ_i sont distincts. De plus, d'après la proposition IV.2

$$\forall \lambda \in \mathbb{K}, \mu_u(\lambda) = 0 \iff \lambda \in \text{VP}(u)$$

et donc finalement $\mu_u = \prod_{i=1}^r (X - \lambda_i)$

2. Posons $P = L_1 + \dots + L_r - 1$. Alors pour tout $i \in \llbracket 1; r \rrbracket$ $P(\lambda_i) = 1 - 1 = 0$. Ainsi, étant donné que $\mu_u(X) = \prod_{i=1}^s (X - \lambda_i)$, $\mu_u|P$ et $\deg P \leq r - 1$ et alors $P = 0$ i.e. $L_1 + \dots + L_r = 1$. Finalement, pour tous $i \neq j$ et tout $k \in \llbracket 1; r \rrbracket$, $L_i L_j(\lambda_k) = 0$ et donc pour tous $i \neq j$ et tout $k \in \llbracket 1; r \rrbracket$, $(X - \lambda_k)|L_i L_j$ i.e. $\mu_u|L_i L_j$ si $i \neq j$.
3. Soit $j \in \llbracket 1; r \rrbracket$ et $x \in E_{\lambda_j, u}$. On a pour tout $i \in \llbracket 1; r \rrbracket$, $L_i(u)(x) = L_i(\lambda_j)x = \delta_{i,j}x$. En considérant pour tout $i \in \llbracket 1; r \rrbracket$, β_i une base de $E_{\lambda_i, u}$, on voit que pour tout $j \in \llbracket 1; r \rrbracket$, pour tout $i \in \llbracket 1; r \rrbracket$ et $e \in \beta_j$, $L_i(u)(e) = e$ si $i = j$ et 0 sinon. On a aussi clairement $L_i(u) \circ L_i(u) = L_i(u)$, d'où le résultat.

Exercice IV.11.

Soit $S \subset \mathcal{L}(E)$ un ensemble non vide d'endomorphismes diagonalisables de E . Montrer que les éléments de S sont codiagonalisables (c'est à dire que leurs matrices sont toutes diagonales dans une même base) si et seulement si ils commutent tous deux à deux, i.e.

$$\forall (u, v) \in S^2, u \circ v = v \circ u$$

Exercice IV.12.

Soit \mathbb{K} un corps de caractéristique différente de 2 et $m, n \geq 1$. Montrer que s'il existe $\varphi : \text{GL}_m(\mathbb{K}) \rightarrow \text{GL}_n(\mathbb{K})$ morphisme de groupes injectif alors $m \leq n$. En particulier, si $\text{GL}_m(\mathbb{K})$ et $\text{GL}_n(\mathbb{K})$ sont isomorphes alors $m = n$.

Exercice IV.13.

Dans cet exercice, on suppose que $\mathbb{K} = \mathbb{C}$. Soit $u \in \mathcal{L}(E)$ tel que u^2 soit diagonalisable. Montrer que u est diagonalisable si et seulement si $\text{Ker } u = \text{Ker } u^2$.

V Polynome caractéristique

1. Généralités

Soit E un espace vectoriel de dimension finie $n \geq 1$ et $u \in \mathcal{L}(E)$.

Proposition V.1.

1. Soit $\lambda \in \mathbb{K}$. λ est une valeur propre de u si et seulement si $\det(u - \lambda \text{Id}) = 0$
2. Si A et B sont deux matrices de $\mathcal{M}_n(\mathbb{K})$ semblables, alors $\det(A - XI_n) = \det(B - XI_n)$. En particulier, la quantité $\det([u]_\beta - XI_n)$ est indépendante de la base β . On appelle alors polynôme caractéristique de u le polynôme

$$\chi_u(X) = \det(XI_n - [u]_\beta) = (-1)^n \det([u]_\beta - XI_n)$$

Preuve :

1. $\lambda \in \text{VP}(u) \iff \text{Ker}(u - \lambda \text{Id}) \neq \{0\} \underset{\text{dimension finie}}{\iff} u - \lambda \text{Id} \notin \text{GL}(E) \iff \det(u - \lambda \text{Id}) = 0$
2. $\det(PAP^{-1} - X \text{Id}) = \det(P(A - \lambda \text{Id})P^{-1}) = \det(P) \det(P^{-1}) \det(A - X \text{Id}) = \det(A - X \text{Id})$

Remarque : le point 1 se reformule de la manière suivante

$$\lambda \in \mathbb{K} \text{ est une valeur propre de } u \iff \chi_u(\lambda) = 0$$

En particulier, lorsque $\mathbb{K} = \mathbb{C}$, $\chi_u(X) = \prod_{\delta \in \text{VP}(u)} (X - \delta)^{l_\delta}$ où $\forall \delta \in \text{VP}(u)$, $l_\delta \geq 1$.

Attention : χ_u peut avoir des racines non contenues dans \mathbb{K} . En effet, si on considère une matrice de rotation d'angle $\frac{\pi}{2}$, $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, on a $\chi_M(X) = X^2 + 1$. Ce polynôme admet deux racines complexes mais aucune racine réelle.

Astuce utile : Un calcul explicite nous permet d'affirmer que

$$\det(XI_n - A) = X^n - \text{tr}(A)X^{n-1} + \cdots + (-1)^n \det A$$

En particulier, il est bon de retenir les formules suivantes

- Lorsque $n = 2$, $\chi_A(X) = X^2 - \text{Tr}(A)X + \det A$
- Lorsque $n = 3$, $\chi_A(X) = X^3 - \text{Tr}(A)X^2 + C_2(A)X - \det A$
où $C_2(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} + \begin{vmatrix} a_{12} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix}$ lorsque $A = (a_{i,j})_{i,j \in \llbracket 1;3 \rrbracket}$.

Notation : Pour tout $u \in \mathcal{L}(E)$, on désigne par $\text{Spec}_{\mathbb{K}}(u)$ la liste non ordonnée des valeurs propres de u qui sont contenues dans \mathbb{K} en prenant compte de leurs multiplicité dans χ_u , c'est à dire que $\text{Spec}_{\mathbb{K}}(u)$ peut être vu comme un ensemble mais contrairement à un ensemble usuel, un élément peut être compté plus d'une fois et contrairement aux k -uplets l'ordre n'est pas pris en compte. Par exemple, lorsque $\text{Spec}_{\mathbb{K}}(u)$ contient deux fois 1 et une fois 2, nous noterons $\text{Spec}_{\mathbb{K}}(u) = [1, 1, 2]$.

Parfois, par abus de notation, on pourra voir $\text{Spec}_{\mathbb{K}}(u)$ comme un ensemble normal aussi.

Exemple : Si $A = \text{diag}(\lambda_1, \dots, \lambda_n)$ (pas forcément distincts) alors $\chi_A = \prod_1^n (X - \lambda_i)$ et $\text{Spec}_{\mathbb{K}}(A) = [\lambda_1, \dots, \lambda_n]$.

Attention : En général, $\text{Spec}_{\mathbb{R}}(u) \subsetneq \text{Spec}_{\mathbb{C}}(u)$.

Proposition V.2.

Lorsque $\mathbb{K} = \mathbb{C}$, pour tout $A \in \mathcal{M}_n(\mathbb{K})$, si $\text{Spec}_{\mathbb{C}}(A) = [\lambda_1, \dots, \lambda_n]$ alors $\text{Tr}(A) = \lambda_1 + \dots + \lambda_n$ et $\det A = \lambda_1 \dots \lambda_n$.

Preuve : Soit $A \in \mathcal{M}_n(\mathbb{K})$. On a

$$\chi_A(X) = \det(XI_n - A) = \prod_{i=1}^n (X - \lambda_i) = X^n - \text{Tr}(A)X^{n-1} + \dots + (-1)^n \det(A)$$

En identifiant les coefficients de l'avant dernier terme et du dernier terme, on trouve bien que $\text{Tr}(A) = \lambda_1 + \dots + \lambda_n$ et $\det A = \lambda_1 \dots \lambda_n$.

Exemples :

- Si $A = (a_{i,j})_{i,j \in \llbracket 1; n \rrbracket}$ est une matrice triangulaire supérieure (resp. inférieure) alors

$$\chi_A(X) = \prod_{i=1}^n (X - a_{ii})$$

- Soit $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{K}[X]$ et $C_P = \begin{pmatrix} 0 & & -a_0 \\ 1 & \ddots & \vdots \\ \ddots & 0 & -a_{n-2} \\ & 1 & -a_{n-1} \end{pmatrix} \in \mathcal{M}_n(\mathbb{K})$.

On a $\chi_{C_P} = P$. On appelle C_P la matrice compagnon de P .

La preuve (classique) de ces deux points se fait par récurrence en développant suivant la première colonne.

Exercice V.3.

Soit $A \in \mathcal{M}_n(\mathbb{K})$. En utilisant la base $(E_{k,l})_{k,j \in \llbracket 1; n \rrbracket} = ((\delta_{i,k}\delta_{j,l})_{i,j \in \llbracket 1; n \rrbracket})$, trouver le polynôme caractéristique de

$$\phi_A : \begin{cases} \mathcal{M}_n(\mathbb{K}) & \longrightarrow \mathcal{M}_n(\mathbb{K}) \\ X & \longmapsto AX \end{cases}$$

Proposition V.4.

Soit F un sous-espace vectoriel de E stable par u . Posons $v = u|_F^F$. Montrer que $\chi_v|\chi_u$.

Preuve : Considérons β_1 une base de F qu'on complète en une base $\beta = (\beta_1, \beta_2)$ de E . On a alors

$$[X \text{ Id} - u]_{\beta} = \begin{pmatrix} [X \text{ Id} - v]_{\beta_1} & * \\ 0 & X \text{ Id} - B \end{pmatrix}$$

où $B \in \mathcal{M}_{|\beta_2|}(\mathbb{K})$. On a alors $\chi_u(X) = \chi_v(X)\chi_B(X)$ (on rappelle que le déterminant d'une matrice triangulaire supérieure par bloc est le produit des déterminants des blocs diagonaux). Ceci donne bien le résultat voulu.

2. Caractérisation des endomorphismes diagonalisables

Dans cette sous-partie, nous allons présenter des moyens de dire si un endomorphisme est diagonalisable ou non.

Définition V.5.

Soit $u \in \mathcal{L}(E)$ et $\lambda \in \text{Spec}_{\mathbb{K}}(u)$.

1. La multiplicité algébrique de λ est sa multiplicité en tant que racine de χ_u , notée $\alpha_u(\lambda)$.
2. La multiplicité géométrique de λ est $\beta_u(\lambda) := \dim E_{\lambda,u}$

S'il n'y a pas d'ambiguïté sur l'endomorphisme u , on pourra les noter $\alpha(\lambda)$ (ou α_λ) et $\beta(\lambda)$ (ou β_λ) respectivement.

Proposition V.6.

Soit $u \in \mathcal{L}(E)$. Les propositions suivantes sont vraies.

1. Pour toute valeur propre λ de u , $\alpha_u(\lambda) \geq \beta_u(\lambda)$.
2. u est diagonalisable $\iff \chi_u$ scindé et $\forall \lambda \in \text{Spec}_{\mathbb{K}}(u)$, $\alpha_u(\lambda) = \beta_u(\lambda)$

Preuve :

1. $F = \text{Ker}(u - \lambda \text{Id})$ est stable par u . Considérons $v = u|_F^F$. $\chi_v = (X - \lambda \text{Id})^{\beta(\lambda)}|\chi_u$ d'où $\beta_\lambda \leq \alpha_\lambda$.

2. Soit $u \in \mathcal{L}(E)$

$\rightarrow (\Rightarrow)$ Soit β une base de E et $\lambda_1, \dots, \lambda_r$ deux à deux distincts tels que $[u]_\beta = \begin{pmatrix} \lambda_1 I_{l_1} & & \\ & \ddots & \\ & & \lambda_r I_{l_r} \end{pmatrix}$

avec $\lambda_1, \dots, \lambda_r \in \mathbb{N}^*$. On a alors

$$\begin{aligned} \chi_u(X) &= \det(XI_n - [u]_\beta) = \det \begin{pmatrix} (X - \lambda_1)I_{l_1} & & \\ & \ddots & \\ & & (X - \lambda_n)I_{l_r} \end{pmatrix} \\ &= \prod_{i=1}^r (X - \lambda_i)^{l_i} \end{aligned}$$

De là, on voit bien que χ_u est scindé et pour tout $i \in \llbracket 1; r \rrbracket$, $l_i = \alpha_u(\lambda_i) = \beta_u(\lambda_i)$.

$\rightarrow (\Leftarrow)$ On a

$$n = \sum_{\lambda \in \text{VP}(u)} \alpha_u(\lambda) = \sum_{\lambda \in \text{VP}(u)} \beta_u(\lambda) = \dim \left(\bigoplus_{\lambda \in \text{VP}(u)} E_{\lambda,u} \right)$$

En déduit donc que $E = \bigoplus_{\lambda \in \text{VP}(u)} E_{\lambda,u}$, i.e. u est diagonalisable.

Remarque : Soit $A \in \mathcal{M}_n(\mathbb{K})$. Si χ_A possède n racines distinctes dans \mathbb{K} alors

$\rightarrow A$ est diagonalisable dans $\mathcal{M}_n(\mathbb{K})$.

$\rightarrow \chi_A$ est scindé à racines simples.

$\rightarrow \forall \lambda \in \text{Spec}_{\mathbb{K}}(A)$, $\alpha_\lambda = \beta_\lambda = 1$

Remarque : En général, Pour deux matrices $A, B \in \mathcal{M}_n(\mathbb{K})$, $\chi_A = \chi_B$ n'implique pas forcément que A est semblable à B . Toutefois, si A et B sont toutes les deux diagonalisables alors l'implication devient vraie. Ceci car, dans ce cas,

$$\text{Spec}_{\mathbb{K}}(A) = \text{Spec}_{\mathbb{K}}(B) = [\lambda_1, \dots, \lambda_n]$$

donc A et B sont toutes deux semblables à $\text{diag}(\lambda_1, \dots, \lambda_n)$, A et B sont donc semblables par transitivité de la relation d'équivalence matricielle. Notons aussi que le fait d'avoir la diagonalisabilité pour uniquement

une seule d'elles ne suffit pas. En effet, pour le voir, il suffit de prendre $A = 0$ et B une matrice nilpotente non nulle quelconque (par exemple strictement triangulaire supérieure non nulle), ces deux matrices admettent X^n comme polynôme caractéristique mais ne sont clairement pas équivalentes.

Le théorème suivant est l'un des plus utile en algèbre linéaire

Théorème (Cayley-Hamilton) V.7.

Pour tout $A \in \mathcal{M}_n(\mathbb{K})$, $\chi_A(A) = 0$.

Remarque : Le théorème ci-dessus est équivalent à dire que pour tout $A \in \mathcal{M}_n(\mathbb{K})$, $\mu_A | \chi_A$.

Preuve : Plusieurs démonstrations sont possibles, on rencontrera notamment plusieurs dans ce cours. On présentera ici une basée sur le changement de corps. On considérera dans cette démonstration que $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} et on posera $\mathbb{L} := \mathbb{C}$. Noter que cette démonstration est généralisable à d'autres corps si on connaît un peu de théorie d'extension de corps (c.f. section Bonus sur l'existence d'une clôture algébrique qui est en particulier un surcorps qui scinde tout polynôme).

Remarquons d'abord que χ_A est indépendant du corps de référence. On peut donc sans souci travailler dans $M_n(\mathbb{L})$ et montrer que dans \mathbb{L} , $\chi_A(A) = 0$. Montrons cela dans $M_n(\mathbb{L})$.

Dans \mathbb{L} , $\mu_{A,\mathbb{L}}$ (le polynôme minimal de u dans $\mathbb{L}[X]$) et χ_A sont scindés et leurs racines sont exactement les mêmes (il s'agit des valeurs propres de A dans \mathbb{L}). Notons alors $\lambda_1, \dots, \lambda_s$ les valeurs propres distinctes de A . On a alors

$$\mu_{A,\mathbb{L}} = \prod_{i=1}^s (X - \lambda_i)^{\gamma_i} \text{ et } \chi_A = \prod_{i=1}^s (X - \lambda_i)^{\alpha_i}$$

Il suffit maintenant de montrer que $\forall i \gamma_i \leq \alpha_i$, car une fois cela fait, on aurait $\mu_{A,\mathbb{L}} | \chi_A$ et donc $\chi_A(A) = 0$. Par symétrie des rôles des γ_i , il suffit de montrer que $\gamma_1 \leq \alpha_1$. Soit $u \in \mathcal{L}(\mathbb{L}^n)$ l'endomorphisme associé à A dans la base canonique. De même, E désignera désormais \mathbb{L}^n . Posons

$$\begin{aligned} F &= \text{Ker}(u - \lambda_1 \text{Id})^{\gamma_1} & H &= \bigoplus_{i=2}^s \text{Ker}(u - \lambda_i \text{Id})^{\gamma_i} \\ d &= \dim(F) & v &= u \Big|_F \end{aligned}$$

Remarquons que v est bien défini car F est stable par u . Soit β_1 une base de F et β_2 une base de H . $\beta = (\beta_1, \beta_2)$ est une base de E et

$$[u]_\beta = \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$$

Soit μ_B et μ_C les polynômes minimaux de B et C respectivement. Par souci de clareté, nous procéderons point par point.

- v est annulé par $(X - \lambda_1)^{\gamma_1}$, donc $\mu_B | (X - \lambda_1)^{\gamma_1}$, i.e. il existe $p \in \llbracket 1; \gamma_1 \rrbracket$ tel que $\mu_B = (X - \lambda_1)^p$.
- De même, $\prod_{i=2}^s (X - \lambda_i)^{\gamma_i}$ annule C , donc $\mu_C \Big| \prod_{i=2}^s (X - \lambda_i)^{\gamma_i}$.
- De plus, on a pour tout $P \in \mathbb{L}[X]$, P annule u si et seulement si P annule B et C , i.e. $P \in \langle \mu_B \rangle \cap \langle \mu_C \rangle = \langle \mu_B \vee \mu_C \rangle$. Le polynôme unitaire de plus petit degré vérifiant cette propriété est $\mu_C \vee \mu_B$, donc

$$\prod_{i=1}^s (X - \lambda_i)^{\gamma_i} = \mu_u = \mu_C \vee \mu_B = \mu_B \mu_C = (X - \lambda_1)^p \mu_C$$

On a alors $(X - \lambda_1)^{\gamma_1} | (X - \lambda_1)^p \mu_C$ et $\mu_C \wedge (X - \lambda_1)^{\gamma_1} = 1$, donc $(X - \lambda_1)^{\gamma_1} | (X - \lambda_1)^p$, donc $\gamma_1 \leq p$ (et aussi $\gamma_1 \geq p$), donc $\gamma_1 = p$, et alors $\mu_B = (X - \lambda_1)^{\gamma_1}$.

- La matrice $N = B - \lambda_1 \text{Id}$ est nilpotente d'indice de nilpotence γ_1 . En particulier, on dispose de $X \in \mathbb{L}^d$ tel que $N^{\gamma_1-1} X \neq 0$. Ainsi, $\gamma_1 \leq d$ car $(X, NX, \dots, N^{\gamma_1-1} X)$ est libre et ne peut donc

pas contenir plus de d éléments (pour le montrer, il suffit de considérer une combinaison linéaire de cette famille non triviale et d'appliquer un nombre suffisant de fois N).

- La seule valeur propre de N est 0 car si $\lambda \neq 0$ est une valeur propre de N et X un vecteur propre associé, $0 = N^{\gamma_1}X = \lambda^{\gamma_1}X$ ce qui est absurde. De plus, χ_N est de degré d , unitaire scindé dans \mathbb{L} et admet uniquement 0 comme racine donc $\chi_N(X) = X^d$.
- Le point précédent nous permet d'écrire

$$\chi_B(X) = \det(XI - B) = \det((X - \lambda_1)I - N) = \chi_N(X - \lambda_1) = (X - \lambda_1)^d$$

- Pour conclure, on a

$$(X - \lambda_1)^d = \chi_B(X)|\chi_A(X) = \prod_{i=1}^s (X - \lambda_i)^{\alpha_i}$$

et alors $d \leq \alpha_1$ et finalement $\gamma_1 \leq d \leq \alpha_1$, ce qui est bien le résultat recherché.

Corollaire V.8.

Soit $u \in \mathcal{L}(E)$. Les propositions suivantes sont vraies.

1. $\deg(\mu_u) \leq n$
2. Les facteurs irréductibles de μ_u et χ_u sont exactement les mêmes à puissance près.
3. $\chi_u|\mu_u^n$ et $Z_{\mathbb{K}}(\mu_u) = Z_{\mathbb{K}}(\chi_u) = \text{Spec}_{\mathbb{K}}(u)$.

Remarque 1 : Dans le cas particulier où $\mathbb{K} = \mathbb{C}$, le point (2) est équivalent à dire

$$\chi_u(X) = \prod_{i=1}^r (X - \lambda_i)^{\alpha_i} \text{ et } \mu_u(X) = \prod_{i=1}^r (X - \lambda_i)^{\gamma_i}$$

où λ_i distincts et pour tout $i \in \llbracket 1; r \rrbracket$, $1 \leq \gamma_i \leq \alpha_i$.

Remarque 2 : Ce résultat est vrai même pour \mathbb{K} égal à un corps quelconque, pas forcément égal à \mathbb{R} ou \mathbb{C} (vois partie bonus).

Applications :

- Soit $A \in \mathcal{M}_2(\mathbb{K})$. Si $\text{Tr}(A) = 0$, alors A^2 est une homothétie. En effet, $0 = \chi_A(A) = A^2 - \text{Tr}(A)A + \det(A)I_2 = A^2 + \det(A)I_2$ et alors $A^2 = -\det(A)I_2$.
- Soit $A, B \in \mathcal{M}_n(\mathbb{Z})$ tel que $\det A \wedge \det B = 1$. Alors $\exists U, V \in \mathcal{M}_n(\mathbb{Z})$ tel que $UA + VB = I_n$.
En effet, $\chi_A(A) = 0$ nous donne que

$$A^n + (\text{Tr } A)A^{n-1} + \cdots + c_1A + (-1)^n \det A \cdot I_n = 0$$

i.e.

$$\det A \cdot I_n = A \times \underbrace{(-1)^{n+1}(A^{n-1} + (\text{Tr } A)A^{n-2} + \cdots + c_1I_n)}_{U \in \mathcal{M}_n(\mathbb{Z})}$$

De la même manière, il existe $V \in \mathcal{M}_n(\mathbb{Z})$ polynôme en B tel que $\det B \cdot I_n = VB$ et finalement d'après Bezout, on dispose de $a, b \in \mathbb{Z}$ tel que $a \cdot \det A + b \cdot \det B = 1$ ce qui permet de dire, en multipliant par I_n des deux côtés que $(aU)A + (bV)B = I_n$

Dans ce qui suit, on aura besoin du lemme suivant, qui est souvent assez utile.

Lemme V.9.

Soit $u \in \mathcal{L}(E)$, $\lambda \in \mathbb{K}$ et $k \geq 2$, on a

$$\text{Ker}(u - \lambda \text{Id})^k = \text{Ker}(u - \lambda \text{Id}) \iff \text{Ker}(u - \lambda \text{Id})^2 = \text{Ker}(u - \lambda \text{Id})$$

Preuve

$\rightarrow (\Leftarrow)$ Soit $k \geq 2$ et $x \in E$, on a

$$\begin{aligned} (u - \lambda \text{Id})^k(x) = 0 &\implies (u - \lambda \text{Id})^2 \circ (u - \lambda \text{Id})^{k-2}(x) = 0 \\ &\implies (u - \lambda \text{Id}) \circ (A - \lambda \text{Id})^{k-2}(x) = 0 \\ &\implies (u - \lambda \text{Id})^{k-1}(x) = 0 \end{aligned}$$

En itérant ce procédé $k - 1$ fois, on obtient que

$$(u - \lambda \text{Id})^k(x) = 0 \implies (u - \lambda \text{Id})^{k-1}(x) = 0 \implies \dots \implies (u - \lambda \text{Id})(x) = 0$$

On en déduit donc que $\text{Ker}(u - \lambda \text{Id})^k \subset \text{Ker}(u - \lambda \text{Id})$, i.e. $\text{Ker}(u - \lambda \text{Id})^k = \text{Ker}(u - \lambda \text{Id})$.

$\rightarrow (\Rightarrow)$ On a clairement

$$\text{Ker}(u - \lambda \text{Id}) \subset \text{Ker}(u - \lambda \text{Id})^2 \subset \dots \subset \text{Ker}(u - \lambda \text{Id})^k$$

Le fait que $\text{Ker}(u - \lambda \text{Id})^k = \text{Ker}(u - \lambda \text{Id})$ implique que toutes ces inclusions sont des égalités, et en particulier que $\text{Ker}(u - \lambda \text{Id}) = \text{Ker}(u - \lambda \text{Id})^2$.

Exercice V.10.

Soit $A \in \mathcal{M}_n(\mathbb{K})$ avec χ_A scindé. Montrer que

$$A \text{ est diagonalisable} \iff \forall \lambda \in \text{Spec}_{\mathbb{K}}(A), \dim \text{Ker}(A - \lambda I_n) = \dim \text{Ker}(A - \lambda I_n)^2$$

VI Trigonalisation

1. Généralités

Soit E un \mathbb{K} -espace vectoriel de dimension finie $n \in \mathbb{N}^*$.

Définition VI.1.

On dit que $u \in \mathcal{L}(E)$ est trigonalisable s'il existe β base de E tel que $[u]_{\beta}$ est triangulaire supérieure.

Remarque : Soit $\beta = (e_1, \dots, e_n)$ est une base de E . $[u]_{\beta}$ est triangulaire supérieure si et seulement si u stabilise le drapeau associé à β i.e. $\forall k \in \llbracket 1; n \rrbracket$, $u(Vect(e_1, \dots, e_k)) \subset Vect(e_1, \dots, e_k)$

Définition VI.2.

On dit que $A \in \mathcal{M}_n(\mathbb{K})$ est trigonalisable s'il existe $P \in \text{GL}_n(\mathbb{K})$ tel que $P^{-1}AP$ soit triangulaire supérieure.

Remarque : Soit $A \in \mathcal{M}_n(\mathbb{K})$. Lorsque A est triangulaire supérieure, notons $A = \begin{pmatrix} a_{11} & * & \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}$, on a $\text{Spec}_{\mathbb{K}}(A) = [a_{11}, \dots, a_{nn}]$. La preuve de ce résultat est laissée comme exercice au lecteur.

Proposition VI.3.

Soit $A \in \mathcal{M}_n(\mathbb{K})$ et $u \in \mathcal{L}(E)$.

1. A est trigonalisable $\iff f_A : X \mapsto AX$ est trigonalisable
2. u est trigonalisable \iff Il existe β une base de E tel que $[u]_\beta$ est trigonalisable \iff pour tout base β de E , $[u]_\beta$ est trigonalisable.

3. Soit $A = \begin{pmatrix} a_{11} & * & \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}$ et $B = \begin{pmatrix} b_{11} & * & \\ & \ddots & \\ 0 & & b_{nn} \end{pmatrix}$ Si A et B sont semblables, alors (a_{11}, \dots, a_{nn}) et (b_{11}, \dots, b_{nn}) sont égaux à permutation près, soit, avec nos notations, $[a_{11}, \dots, a_{nn}] = [b_{11}, \dots, b_{nn}] (= \text{Spec}_{\mathbb{K}}(A) = \text{Spec}_{\mathbb{K}}(B))$.

Preuve : La démonstration est facile est laissée au lecteur (elle est très similaire à celle sur la diagonalisabilité).

Proposition VI.4.

Soit $u \in \mathcal{L}(E)$. Les propriétés suivantes sont équivalentes

1. u est trigonalisable
2. χ_u est scindé
3. μ_u est scindé
4. $\exists P \in \mathbb{K}[X] \setminus \{0\}$, $P(u) = 0$ et P est scindé

En particulier, sur un corps algébriquement clos tel que \mathbb{C} , tout endomorphisme est trigonalisable

Preuve

$\rightarrow (1) \Rightarrow (2)$ Si u est trigonalisable donc on dispose de β base de E tel que $[u]_\beta = \begin{pmatrix} \lambda_1 & * & \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ et alors

$$\chi_u(X) = \det([X \text{ Id} - u]_\beta) = \det \begin{pmatrix} X - \lambda_1 & * & \\ & \ddots & \\ 0 & & X - \lambda_n \end{pmatrix} = \prod_{i=1}^n (X - \lambda_i)$$

χ_u est donc bien scindé.

- $\rightarrow (2) \Rightarrow (3) \quad \mu_u | \chi_u$
- , donc
- μ_u
- est aussi scindé.
-
- $\rightarrow (3) \Rightarrow (4)$
- Il suffit de prendre
- $P = \mu_u$
- .
-
- $\rightarrow (4) \Rightarrow (1)$
- Procédons par récurrence forte sur
- n
- , la dimension de
- E
- .
- Le cas $n = 1$ est évident.
 - Soit $n \geq 2$. Supposons que pour tout $k \in \llbracket 1; n \rrbracket$, la propriété soit vraie. $\mu_u | P$, donc μ_u est aussi scindé. μ_u admet donc une racine λ . Considérons $F = \text{Ker}(u - \lambda \text{ Id}) \neq \{0\}$ et β_1 une base de

F qu'on complète en une base $\beta = (\beta_1, \beta_2)$ de E . On a alors

$$[u]_\beta = \begin{pmatrix} \lambda \text{Id} & * \\ 0 & B \end{pmatrix} \text{ et donc } 0 = [P(u)]_\beta = \begin{pmatrix} P(\lambda) \text{Id} & * \\ 0 & P(B) \end{pmatrix}$$

Donc $P(B) = 0$. $B \in \mathcal{M}_l(\mathbb{K})$ (avec $1 \leq n - 1$) est annulé par un polynôme scindé, on peut donc appliquer l'hypothèse de récurrence et dire que B est trigonalisable. Il existe donc $Q \in \text{GL}_l(\mathbb{K})$ tel que $T := QBQ^{-1}$ soit triangulaire supérieure. Finalement,

$$[u]_\beta = \begin{pmatrix} \lambda \text{Id} & * \\ 0 & B \end{pmatrix} \simeq \begin{pmatrix} \text{Id} & 0 \\ 0 & Q \end{pmatrix} \begin{pmatrix} \lambda \text{Id} & * \\ 0 & B \end{pmatrix} \begin{pmatrix} \text{Id} & 0 \\ 0 & Q^{-1} \end{pmatrix} = \begin{pmatrix} \lambda \text{Id} & * \\ 0 & T \end{pmatrix}$$

cette matrice est triangulaire supérieure, donc u est trigonalisable.

Applications :

1. Soit $u \in \mathcal{L}(E)$. Les propriétés suivantes sont équivalentes
 - u est nilpotente.
 - Il existe une base β de E telle que $[u]_\beta$ est strictement triangulaire supérieure.
 - $\chi_u = X^n$

Pour montrer cela, il suffit de remarquer que le seul facteur irréductible de X^d est X .

2. Soit $A \in \mathcal{M}_n(\mathbb{C})$ et $\mathbb{P} \in K[X]$.

$$\text{Spec}_{\mathbb{C}}(A) = [\lambda_1, \dots, \lambda_n] \implies \text{Spec}_{\mathbb{C}}(P(A)) = [P(\lambda_1), \dots, P(\lambda_n)]$$

Cette propriété se démontre aisément en trigonalisant la matrice A et en utilisant le fait que le spectre d'une matrice triangulaire est égal aux coefficients diagonaux de cette matrice.

Exercice VI.5.

Soit $u \in \mathcal{L}(\mathbb{C}^n)$. Montrer que les propriétés suivantes sont équivalentes.

1. u est nilpotent
2. $\forall k \in \llbracket 1; n \rrbracket$, $\text{Tr}(u^k) = 0$
3. $\forall P \in \mathbb{K}[X]$, $\text{Tr}(P(u)) = nP(0)$

Exercice VI.6.

Supposons que $\mathbb{K} = \mathbb{C}$.

1. Trouver toutes les classes de similitudes des matrices suivant les valeurs de μ_A et χ_A pour $A \in \mathcal{M}_n(\mathbb{C})$ lorsque $n = 2$ et $n = 3$.
2. En déduire que pour tout $A, B \in \mathcal{M}_n(\mathbb{C})$,
 - Pour $n = 2$, $\mu_A = \mu_B \iff A \simeq B$.
 - Pour $n = 3$, $(\mu_A = \mu_B \text{ et } \chi_A = \chi_B) \iff A \simeq B$.
3. Trouver un contre-exemple des propriétés précédentes dans $n = 4$.

Exercice VI.7.

Soit $S \subset M_n(\mathbb{K})$ un sous-ensemble non vide de matrices trigonalisables qui commutent deux à deux. Montrer qu'il existe $P \in GL_n(\mathbb{K})$ telle que pour tout $A \in S$, PAP^{-1} est triangulaire supérieure.

2. Décomposition de Jordan-Dunford

Proposition VI.8.

Soit $u \in \mathcal{L}(E)$. Supposons que χ_u soit scindé, i.e. qu'on peut écrire $\mu_u(X) = \prod_{i=1}^r (X - \lambda_i)^{\gamma_i}$ et $\chi_u(X) = \prod_{i=1}^r (X - \lambda_i)^{\alpha_i}$ avec les λ_i distincts. posons $F_{\lambda_i} = \text{Ker}(u - \lambda_i \text{Id})^{\gamma_i} = \text{Ker}(u - \lambda_i \text{Id})^{\alpha_i}$. Les propriétés suivantes sont vraies.

1. F_{λ_i} est stable par u et est de dimension α_i .
2. $E = \bigoplus_{i=1}^r F_{\lambda_i}$
3. $u|_{F_{\lambda_i}}^{F_{\lambda_i}} = \lambda_i \text{Id}_{F_{\lambda_i}} + N_{\lambda_i}$ où $N_{\lambda_i} \in \mathcal{L}(F_{\lambda_i})$ est nilpotent.

Vocabulaire : On appelle F_{λ_i} l'espace caractéristique de u associé à λ_i .

En considérant pour tout i, β_i une base de F_{λ_i} où $[u|_{F_{\lambda_i}}]_{\beta_i}$ est triangulaire supérieure et β la concaténation de ces bases (qui est une base de E), on obtient que

$$[u]_{\beta} = \begin{pmatrix} A_{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & A_{\lambda_r} \end{pmatrix} \text{ où } A_{\lambda_i} = \begin{pmatrix} \lambda_i & & * \\ & \ddots & \\ 0 & & \lambda_i \end{pmatrix} \in \mathcal{M}_{\alpha_i}(\mathbb{K})$$

Remarquons lorsque χ_u est scindé que $\forall i \in \llbracket 1; r \rrbracket$, $F_{\lambda_i, u} = E_{\lambda_i, u}$ si et seulement si u est diagonalisable. Ceci étant vrai car

$$\begin{aligned} F_{\lambda_i, u} = E_{\lambda_i, u} &\iff \text{Ker}(u - \lambda \text{Id}) = \text{Ker}((u - \lambda \text{Id})^{\alpha_i}) \\ &\iff \text{Ker}(u - \lambda \text{Id}) = \text{Ker}((u - \lambda \text{Id})^2) \iff u \text{ est diagonalisable} \end{aligned}$$

Le cas $\alpha_i = 1$ est facile et peut être traité séparément par le lecteur. La dernière équivalence est vraie d'après l'exercice V.10. et l'avant dernière d'après le lemme V.9.

Rassemblons maintenant tous les blocs diagonaux en une seule matrice D et de même pour ceux nilpotents (la partie strictement triangulaire supérieure) en N . En considérant $\delta, \nu \in \mathcal{L}(E)$ tel que

$$[\delta]_{\beta} = D = \begin{pmatrix} \lambda_1 \cdot I_{\alpha_1} & & 0 \\ & \ddots & \\ 0 & & \lambda_r \cdot I_{\alpha_r} \end{pmatrix} \text{ et } [\nu]_{\beta} = N = \begin{pmatrix} N_{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & N_{\lambda_r} \end{pmatrix}$$

on obtient la décomposition suivante, appelée décomposition de Dunford.

Proposition (Décomposition de Dunford) VI.9.

Soit $u \in \mathcal{L}(E)$ tel que χ_u soit scindé. Il existe un unique couple d'endomorphismes $(\delta, \nu) \in \mathcal{L}(E)^2$ telle que

- $u = \delta + \nu$
- δ est diagonalisable et ν est nilpotente.
- δ et ν commutent.

De plus, δ et ν sont polynomiales en u i.e. il existe $P, Q \in \mathbb{K}[X]$ tels que $\delta = P(u)$ et $\nu = Q(u)$.

Preuve : L'existence a déjà été établie avant, il reste à montrer le caractère polynomial et l'unicité. Remarquons d'abord que $\delta \in \mathbb{K}[u] \iff \nu \in \mathbb{K}[u]$. Il suffit donc de le montrer pour δ ou ν , disons δ . Reprenons les notations de la proposition, ainsi que celles considérées juste avant. Remarquons que $\delta = \sum_1^r \lambda_i \pi_i$ où π_i est la projection sur $F_{\lambda_i, u}$ parallèlement à $\bigoplus_{j \neq i} F_{\lambda_j, u}$ et donc il suffit de vérifier que $\pi_i \in \mathbb{K}[u]$ pour tout i . Par symétrie des rôles des π_i , il suffit de le montrer par exemple pour $i = 1$. Posons

$$\begin{aligned} P_1 &= \prod_{j=2}^r (X - \lambda_j)^{\alpha_j}, \quad \lambda = P(\lambda_1) \neq 0, \quad P_2 = P_1 - \lambda \\ P_3 &= (P_2)^n, \quad P_4 = P_3 - (-\lambda)^n, \quad P_5 = \frac{-1}{(-\lambda)^n} P_5 \end{aligned}$$

Pour voir que ces polynômes sont naturels à considérer, il suffit de voir la succession d'égalités ci-dessous.

$$[P_1(u)]_\beta = \begin{pmatrix} \lambda \text{Id} + N & & 0 \\ & 0 & \\ & & \ddots & \\ 0 & & & 0 \end{pmatrix} \text{ donc } [P_2(u)]_\beta = \begin{pmatrix} N & & & 0 \\ -\lambda \text{Id} & & & \\ & \ddots & & \\ 0 & & -\lambda \text{Id} & \end{pmatrix}$$

et donc

$$[P_3(u)]_\beta = \begin{pmatrix} N^n = 0 & & 0 & \\ & (-\lambda)^n \text{Id} & & \\ & & \ddots & \\ 0 & & & (-\lambda)^n \text{Id} \end{pmatrix} \text{ ainsi } [P_4(u)]_\beta = \begin{pmatrix} -(-\lambda)^n \text{Id} & & & 0 \\ 0 & & & \\ & \ddots & & \\ 0 & & & 0 \end{pmatrix}$$

finalement

$$[P_5(u)]_\beta = \begin{pmatrix} \text{Id} & & 0 \\ & 0 & \\ & & \ddots & \\ 0 & & & 0 \end{pmatrix} = [\pi_1]_\beta$$

Ce qui nous donne bien le résultat voulu.

Montrons enfin l'unicité. Considérons (δ', ν') vérifiant les mêmes propriétés que (δ, ν) . On a

$$u = \delta + \nu = \delta' + \nu' \text{ i.e. } \delta - \delta' = \nu - \nu'$$

ν et ν' commutent car $\nu \in \mathbb{K}[u]$ et ν' commute avec δ' et alors avec $\delta' + \nu' = u$. En posant $v = \delta - \delta' = \nu - \nu'$, on obtient

$$v^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} \nu^k \nu'^{2n-k}$$

sachant que $\forall k \in \llbracket 1; 2n \rrbracket$, soit $k \geq n$ soit $2n - k \geq n$ (on rappelle que l'indice de nilpotence de ν et ν' est forcément inférieur à n), tous les termes de cette somme sont nuls. Ainsi, les seules valeurs propres de v dans \mathbb{C} sont 0, mais v est diagonalisable car il est égal à la somme de δ et δ' qui sont diagonalisables et commutent entre eux car δ est dans $\mathbb{K}[u]$ et δ' commute avec ν' et donc avec $\delta' + \nu' = u$ et sont donc codiagonalisables. On en déduit donc directement que $v = 0$, i.e. $(\delta, \nu) = (\delta', \nu')$, d'où l'unicité de δ et ν .

Exercice VI.10.

Résoudre les équations suivantes.

$$1. X^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 9 \end{pmatrix} \text{ dans } \mathcal{M}_3(\mathbb{R}).$$

$$2. X^2 = \begin{pmatrix} a^2 & 1 \\ 0 & a^2 \end{pmatrix} \text{ dans } \mathcal{M}_2(\mathbb{C}) \text{ avec } a \in \mathbb{C}.$$

$$3. X^2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ dans } \mathcal{M}_3(\mathbb{R}).$$

Exercice VI.11.

Soit $u \in \mathcal{L}(\mathbb{C}^n)$. On considère l'application

$$\phi_u : \begin{cases} \mathcal{L}(\mathbb{C}^n) & \longrightarrow \mathcal{L}(\mathbb{C}^n) \\ v & \longmapsto u \circ v - v \circ u \end{cases}$$

Montrer que u est diagonalisable si et seulement si ϕ_u est diagonalisable.

Exercice VI.12.

Soit $u \in \mathrm{GL}_n(\mathbb{C})$. Montrer que u admet une racine, i.e. qu'il existe $v \in \mathrm{GL}_n(\mathbb{C})$, $v^2 = u$.

Proposition (Décomposition de Jordan 1) VI.13.

Soit $v \in \mathcal{L}(E)$ nilpotent. Il existe une base β de E tel que

$$[v]_\beta = \begin{pmatrix} J_{l_1} & & 0 \\ & \ddots & \\ 0 & & J_{l_s} \end{pmatrix} \text{ où } \forall k \in \llbracket 1; s \rrbracket, J_k = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix} \in \mathcal{M}_k(\mathbb{K})$$

avec $l_1, \dots, l_s \in \llbracket 1; n \rrbracket$ et $l_1 + \dots + l_s = n$.

Preuve : Soit $u \in \mathcal{L}(E)$ nilpotent, il est clair qu'il existe $p \geq 1$ tel que $\mu_u = X^p$ pour un certain $p \geq 1$ (en effet, u est annulé par X^l pour l assez grand, donc $\mu_u | X^l$).

Montrons le résultat par récurrence forte sur la dimension n de E .

→ Le cas $n = 1$ est évident.

→ Soit $n \geq 2$ tel que $\dim E = n$. Supposons que la propriété soit vraie pour tout $k \in \llbracket 1; n \rrbracket$. Soit $x_1 \in E \setminus \{0\}$ tel que $u^{p-1}(x_1) \neq 0$. En posant $F_{x_1} = \mathrm{Vect}(x_1, \dots, u^{p-1}(x_1))$ (remarquons que cette

famille est libre, c'est donc une base de F_{x_1}), on voit que F_{x_1} est stable et

$$\left[u \right]_{F_{x_1}}^{F_{x_1}} = J_p$$

Notre intuition est de trouver un supplémentaire de F_{x_1} stable par u et lui appliquer l'hypothèse de récurrence. Voici comment nous allons procéder

- La famille $(x_1, u(x_1), \dots, u^{p-1}(x_1))$ est libre, on peut donc considérer $\phi : E \rightarrow \mathbb{K}$ une forme linéaire telle que $\varphi(u^{p-1}(x_1)) = 1$ et pour tout $k \in \llbracket 0; p-2 \rrbracket$, $\phi(u^k(x_1)) = 0$.
- À partir de ϕ on construit l'application linéaire suivante

$$\varphi : \begin{cases} E & \longrightarrow \mathbb{K}^p \\ y & \longmapsto (\phi(u^{p-1}(y)), \dots, \phi(u(y)), \phi(y)) \end{cases}$$

et on pose $F = \text{Ker } \varphi$.

- F est stable par u . En effet, on a pour tout $y \in E$

$$\begin{aligned} \varphi(y) = 0 &\implies \forall k \in \llbracket 0; p-1 \rrbracket, u^k(y) = 0 \\ &\implies \forall k \in \llbracket 0; p-1 \rrbracket, u^k(u(y)) = 0 \text{ (car } u^p = 0\text{)} \\ &\implies u(y) \in F \end{aligned}$$

- φ est surjective. En effet, pour tout $k \in \llbracket 0; p-1 \rrbracket$, $\varphi(u^k(x_1)) = (\delta_{ik})_{i \in \llbracket 0; p-1 \rrbracket}$ donc pour tout $(a_0, \dots, a_{p-1}) \in \mathbb{K}^p$

$$\varphi(a_0 u^0(x_1) + \dots + a_{p-1} u^{p-1}(x_1)) = (a_0, \dots, a_{p-1})$$

- $F \cap F_{x_1} = \{0\}$. En effet, pour tout $y \in F_{x_1}$, en posant $y = y := \sum_0^{p-1} a_k u^k(x_1)$, on a

$$\varphi(y) = 0 \implies 0 = \varphi \left(\sum_0^{p-1} a_k u^k(x_1) \right) = (a_0, \dots, a_{p-1}) \implies y = 0$$

donc F et F_{x_1} sont en somme directe et par la formule du rang $\dim F = \dim \text{Ker } \varphi = \dim E - \dim \text{Im } \varphi = n - p$, et alors $\dim F_{x_1} + \dim F = n = \dim E$. F et F_{x_1} sont donc supplémentaires.

- Pour finir, on voit que $w = u \Big|_F^F$ est aussi nilpotente, on peut donc appliquer l'hypothèse de récurrence à w sur F ce qui nous donne bien le résultat voulu.

Remarques :

- Lorsqu'on ajoute la condition $l_1 \geq \dots \geq l_s \geq 1$, cette décomposition est unique, i.e. s'il existe une autre base β' de E , où n est de la même forme avec $m_1 \geq \dots \geq m_r \geq 1$ les tailles respectives de ses blocs $(J_k)_{k \in \llbracket 1; r \rrbracket}$, alors $r = s$ et $\forall i \in \llbracket 1; s \rrbracket$, $l_i = m_i$.

Pour s'en convaincre, notons

$$\forall i \in \mathbb{N}^* \quad F(i) = |\{k \in \llbracket 1; s \rrbracket, l_k = i\}| \text{ et } G(i) = |\{k \in \llbracket 1; r \rrbracket, m_k = i\}|$$

Il est aisément vérifier que

$$\forall r \in \mathbb{N}^* \quad \forall k \in \mathbb{N} \quad \dim \text{Ker}(J_r^k) = \min(k, r)$$

Ceci permet donc d'affirmer que

$$\forall k \in \mathbb{N}^* \quad \dim \text{Ker}(u^k) = \sum_1^\infty F(i) \min(k, i) = \sum_1^\infty G(i) \min(k, i)$$

Ainsi, $F = G$ (Il suffit de considérer par absurdité le 1-er indice $i \in \mathbb{N}^*$ où $F(i) \neq G(i)$ pour tomber sur un矛盾). et donc on a notre unicité.

- Remarquons que le bloc associé au sous espace F_{x_1} a la plus grande taille des blocs. En effet la taille du bloc correspond à la dimension de ce sous espace, $\dim F_{x_1} = p$ et la dimension de tout espace défini de la même manière (en itérant u sur un élément de E) est de dimension au plus p .

Proposition (Décomposition de Jordan 2) VI.14.

Soit $u \in \mathcal{L}(E)$ tel que χ_u est scindé dans \mathbb{K} . Notons $\lambda_1, \dots, \lambda_r$ les valeurs propres distinctes (comptées sans multiplicité) de u . Il existe une base β de E telle que

$$[u]_\beta = \begin{pmatrix} \lambda_1 \cdot I_{l_1^i} + A_1 & 0 & & \\ & \ddots & & \\ 0 & & \lambda_r \cdot I_{l_{s_i}^i} + A_r & \end{pmatrix} \text{ avec } A_i = \begin{pmatrix} J_{l_1^i} & & 0 \\ & \ddots & \\ 0 & & J_{l_{s_i}^i} \end{pmatrix}$$

où pour tout $i \in \llbracket 1; r \rrbracket$, $s_i \in \mathbb{N}^*$ et $l_1^i \geq \dots \geq l_{s_i}^i \geq 1$. De plus, cette écriture est unique à permutation des blocs $\lambda_i I_{l_{s_i}^i} + A_i$ près.

On appelle cette décomposition réduction de Jordan de u .

Remarque : Certains auteurs n'exigent pas les inégalités sur les tailles des blocs dans la réduction de Jordan. Cela ne change que la partie unicité de ce théorème.

Exercice VI.15.

Soit $A \in \mathcal{M}_n(\mathbb{C})$. Montrer que $\dim \text{Com}(A) \geq n$.

VII Endomorphismes cycliques

Cette partie hors programme est assez classique. En effet, elle revient dans un nombre considérable d'exercices d'oraux et de sujets d'écrits, voir par exemple Centrale Math 1 2019, où l'intégralité du sujet portait sur les endomorphismes cycliques. Les élèves (dont ceux des MP* de Louis-le-Grand) ayant vu cette notion étaient très avantagés par rapport aux autres cette année là.

Soit E un \mathbb{K} -espace vectoriel de dimension finie $n \geq 1$.

Définition VII.1.

Soit $u \in \mathcal{L}(E)$ et $x \in E \setminus \{0\}$. On appelle espace cyclique engendré par x pour u le sous-espace vectoriel défini par

$$F_{x,u} = \text{Vect}\{u^k(x), k \in \mathbb{N}\}$$

On le notera aussi F_x lorsqu'il n'y a pas d'ambiguïté sur u .

Proposition VII.2.

Soit $u \in \mathcal{L}(E)$ et $x \in E \setminus \{0\}$. Les propositions suivantes sont vraies.

1. $F_{x,u}$ est le plus petit sous-espace vectoriel de E stable par u contenant x .
2. Soit $p = \max\{k \in \mathbb{N}^*, (x, u(x), \dots, u^{k-1}(x)) \text{ est libre}\}$. $\beta = (x, \dots, u^{p-1}(x))$ est une base de $F_{x,u}$.
3. Il existe $P \in \mathbb{K}[X]$ unitaire tel que $\left[u\Big|_{F_{x,u}}\right]_\beta = C_P$ la matrice compagnon associée à P .
4. P est le générateur normalisé de $\mathcal{H}_{u,x} = \{Q \in \mathbb{K}[X], Q(u)(x) = 0\}$, i.e. P est l'unique polynôme unitaire tel que $\mathcal{H}_{u,x} = \langle P \rangle := P \cdot \mathbb{K}[X]$. On appellera P le polynôme minimal (de u) en x et on le notera $\mu_{x,u}$ ou μ_x s'il n'y a pas d'ambiguïté sur u . De plus, $\mu_{x,u} | \mu_u$.

Preuve

1. Clair (il suffit de l'écrire).
2. β est libre par définition. Montrons par récurrence forte que $\forall l \in \mathbb{N} \ u^l(x) \in \text{Vect}(\beta)$.
 - La propriété est évidente pour $l \in \llbracket 0; p-1 \rrbracket$.
 - Soit $l \geq 1$. Supposons que la propriété soit vraie pour tout $k \in \llbracket 0; l-1 \rrbracket$. Si $l \leq p$, la propriété est vraie. Supposons donc que $l > p$. Par définition, $(x, \dots, u^l(x))$ est lié, il existe donc $m \in \llbracket 0; l \rrbracket$ et $(\lambda_0, \dots, \lambda_m) \in \mathbb{K}^n \setminus \{(0, \dots, 0)\}$ tels que

$$u^m(x) = \sum_0^{m-1} \lambda_k u^k(x)$$

On a donc, par hypothèse de récurrence

$$u^l(x) = u^{l-m} \left(\sum_0^{m-1} \lambda_k u^k(x) \right) = \sum_0^{m-1} \lambda_k \underbrace{u^{k+l-m}(x)}_{\in \text{Vect}(\beta)} \in \text{Vect}(\beta)$$

ce qui est bien le résultat voulu.

3. β est libre mais $(\beta, u^p(x))$ ne l'est pas, il existe donc $\lambda_0, \dots, \lambda_{p-1} \in \mathbb{K}$ tels que $u^p(x) = \sum_0^{p-1} \lambda_k u^k(x)$
En Posant $P := X^p - \sum_{k=0}^{p-1} \lambda_k X^k$, il est aisément vérifiable que $\left[u\Big|_{F_{x,u}}\right]_\beta = C_P$.
4. Remarquons que le polynôme P retrouvé au point (3) est unitaire, de degré p et annule u en x . Remarquons de plus que $(x, \dots, u^{p-1}(x))$ est libre i.e. tout élément $Q \in \mathcal{H}_{u,x}$ non nul doit être de degré supérieur à p . En particulier, si Q est le générateur unitaire de $\mathcal{H}_{u,x}$ (existe car $\mathcal{H}_{u,x}$ est un idéal non trivial), alors $Q|P$ et Q et P unitaires (non nuls) et $\deg(P) = p \leq \deg(Q)$ d'où $P = Q$ et donc $\mathcal{H}_{u,x} = \langle P \rangle$.

Définition VII.3.

On dit que u est cyclique lorsqu'il existe $x \in E \setminus \{0\}$ tel que $F_x = E$ i.e. il existe $x \in E$ tel que $(x, \dots, u^{n-1}(x))$ est libre.

Proposition VII.4.

Soit u cyclique et $x \in E \setminus \{0\}$ tel que $F_x = E$. Alors $\mu_x = \mu_u = \chi_u$

Preuve : Les trois polynômes sont tous unitaires et $\mu_x|\mu_u|\chi_u$ et donc il suffit de montrer que $\deg(\mu_x) \geq n$, ce qui est vrai car $(x, u(x), \dots, u^{n-1}(x))$ est libre et donc aucun polynôme de degré $n - 1$ ou moins ne peut annuler u .

Remarquons qu'en prenant u quelconque, $x \in E \setminus \{0\}$ et en considérant $v = u|_{F_x}^{F_x}$, on obtient que $\mu_{u,x} = \mu_{v,x} = \chi_v$ et donc, en particulier, $\deg(\mu_x) = \dim(F_x)$.

Exercice VII.5.

Soit $u \in \mathcal{L}(E)$. On admettra qu'il existe $x \in E - \{0\}$ tel que $\mu_{x,u} = \mu_u$ (démontré dans un exercice ultérieur)

1. Montrer que $\mu_u = \chi_u$ si et seulement si u est cyclique.
2. Supposons que u est cyclique. Montrer que $\text{Com}(u) = \mathbb{K}[u] = \{P(u), P \in \mathbb{K}[X]\}$ et en déduire que $\dim \text{Com}(u) = n$.
3. On ne suppose plus que u est cyclique. Déduire de la question précédente que $\dim \text{Com}(u) \geq n$
4. Montrer que $\mu_u = \chi_u$ si et seulement si $\text{Com}(u) = \mathbb{K}[u]$.

Exercice VII.6.

Soit $u \in \mathcal{L}(E)$. Montrer que χ_u est irréductible si et seulement si les seuls sous-espaces vectoriels stables par u sont $\{0\}$ et E .

Au passage remarquer que, dans ce cas, tout élément non nul est cyclique pour u .

Exercice VII.7.

Soit $A \in \mathcal{M}_n(\mathbb{C})$.

1. Montrer que la dimension de chaque espace propre est égale à 1 si A est semblable à une matrice compagnon.
2. En déduire que si A est diagonalisable, alors A est cyclique si et seulement si A possède n valeurs propres distinctes.

Exercice VII.8.

Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré n et de racines (dans \mathbb{C} , possiblement avec répétition) $\lambda_1, \dots, \lambda_n$

1. Montrer que $\forall k \geq 1, \lambda_1^k, \dots, \lambda_n^k$ sont les racines d'un polynôme unitaire de $\mathbb{Z}[X]$ de degré n .
2. En déduire que si $|\lambda_1| = \dots = |\lambda_n| = 1$ alors les λ_j sont des racines de l'unité.

Exercice VII.9.

Dans cet exercice, on notera $\forall P \in \mathbb{K}[X]$ et $x \in E$, $P \cdot x = P(u)(x)$ et $\mu_0 = 1$.

1. Soit $x \in E \setminus \{0\}$. Supposons qu'il existe $P, Q \in \mathbb{K}[X]$ unitaires tels que $\mu_x = PQ$ et posons $y = Q \cdot x$. Vérifier que $\mu_y = P$.
2. Soit $x, y \in E$ non nuls tels que $\mu_x \wedge \mu_y = 1$. Montrer que $\mu_{x+y} = \mu_x \mu_y$.
3. On ne suppose plus que $\mu_x \wedge \mu_y = 1$. Montrer que qu'il existe $z \neq 0$ tel que $\mu_z = \mu_x \vee \mu_y$.
4. Montrer qu'il existe $a \neq 0$ tel que pour tout $x \neq 0$, $\mu_x | \mu_a$. En déduire que $\mu_a = \mu_u$, le polynôme minimal de u .

Application : en utilisant le résultat de la dernière question, on peut démontrer le théorème de Cayley-Hamilton. En effet, considérons $u \in \mathcal{L}(E)$ et $x \in E \setminus \{0\}$ tel que $\mu_x = \mu_u$. F_x étant stable, $\mu_u = \mu_x = \chi_v|_{\chi_u}$ où $v = u|_{F_x}$. On en déduit donc directement que $\chi_u(u) = 0$.

Une autre manière similaire de démontrer Cayley Hamilton sans le résultat de la dernière question est de voir que pour tout $x \in E \setminus \{0\}$, F_x étant stable, $\mu_x = \chi_v|_{\chi_u}$ où $v = u|_{F_x}$. On a alors pour tout $x \in E \setminus \{0\}$, $\chi_u(u)(x) = 0$, i.e. $\chi_u(u) = 0$.

VIII Réduction et topologie

1. Normes, valeurs propres

On suppose dans cette partie que $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} .

Rappel VIII.1.

On suppose que $E = \mathcal{M}_n(\mathbb{K})$. Soit $\|\cdot\|$ une norme sur \mathbb{K}^n . On peut définir une norme sur E , appelée norme d'opérateur, par

$$\|A\| = \sup_{\|X\|=1} \|AX\| = \sup_{\|X\|\leq 1} \|AX\| = \sup_{X \in E \setminus \{0\}} \frac{\|AX\|}{\|X\|}$$

Remarque : cette norme vérifie les propriétés suivantes

- $\|I_n\| = 1$.
- $\forall A, B \in \mathcal{M}_n(\mathbb{K})$, $\|AB\| \leq \|A\| \times \|B\|$
- $\forall A \in \mathcal{M}_n(\mathbb{K})$, $\sup_{\lambda \in \text{Spec}_{\mathbb{K}}(A)} |\lambda| \leq \|A\|$

Proposition VIII.2.

Soit $A = (a_{ij})_{i,j \in [\![1;n]\!]} \in \mathcal{M}_n(\mathbb{K})$. On a $\text{VP}(A) \subset \bigcup_{k=1}^n B_f \left(a_{kk}, \sum_{j=1, j \neq k}^n |a_{kj}| \right)$.

Preuve : Posons $H = \bigcup_{k=1}^n B_f \left(a_{kk}, \sum_{j=1}^n |a_{kj}| \right)$. Soit $\lambda \notin H$, alors

$$\forall k \in [\![1;n]\!], |\lambda - a_{kk}| > \sum_{j=1, j \neq k}^n |a_{kj}|$$

D'après Hadamard (voir le chapitre des systèmes linéaires), ceci est équivalent à dire que la matrice $A - \lambda I$ est inversible et que donc λ n'est pas une valeur propre de A . On en déduit donc bien que $\text{VP}(A) \subset H$.

Application : En utilisant ce résultat, on peut redémontrer le résultat sur les racines d'un polynôme vu au chapitre 1. En effet, considérons $P \in \mathbb{K}[X]$ et soit $A = C_P$. On a bien entendu

$$P(X) = \chi_A(X) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_1X + \alpha_0$$

On a donc, en utilisant le résultat ci-dessus

$$Z(P) = \text{Spec}_{\mathbb{K}}(A) \subset \bigcup_{k=0}^{n-2} B_f(0, 1 + |\alpha_k|) \cup B_f(\alpha_{n-1}, 1)$$

i.e. pour toute racine λ de P , on a l'inégalité

$$|\lambda| \leq 1 + \max_{k \in \llbracket 0; n-1 \rrbracket} |\alpha_k|$$

Exercice VIII.3.

Soit F un fermé de \mathbb{C} . Montrer que $\tilde{F} = \{A \in \mathcal{M}_n(\mathbb{C}), \text{Spec}_{\mathbb{C}}(A) \subset F\}$ est fermé dans $\mathcal{M}_n(\mathbb{C})$.

Application : $\mathcal{M}_n(\mathbb{R})$ est fermé dans $\mathcal{M}_n(\mathbb{C})$, donc en appliquant le résultat de cet exercice, on a que $\{A \in \mathcal{M}_n(\mathbb{C}), \text{Spec}_{\mathbb{C}}(A) \subset \mathbb{R}\}$ est fermé dans $\mathcal{M}_n(\mathbb{C})$. De plus, on a

$$\begin{aligned} \{A \in \mathcal{M}_n(\mathbb{R}), A \text{ est trigonalisable}\} &= \{A \in \mathcal{M}_n(\mathbb{R}), \chi_A \text{ est scindé}\} \\ &\quad \uparrow \\ &\quad \text{proposition VI.4} \\ &= \{A \in \mathcal{M}_n(\mathbb{C}), \text{Spec}_{\mathbb{C}}(A) \subset \mathbb{R}\} \cap \mathcal{M}_n(\mathbb{R}) \end{aligned}$$

On en déduit donc que l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$ trigonalisables s'écrit sous forme d'une intersection de deux fermés, c'est donc un fermé dans $\mathcal{M}_n(\mathbb{R})$ et $\mathcal{M}_n(\mathbb{C})$.

2. Diagonalisation à ε près

Proposition VIII.4.

Soit $A \in \mathcal{M}_n(\mathbb{C})$ et $\lambda_1, \dots, \lambda_n$ les coefficients diagonaux d'une trigonalisation de A . Pour tout $\varepsilon > 0$, il existe $P \in \mathcal{M}_n(\mathbb{C})$ tel que $P^{-1}AP = \begin{pmatrix} \lambda_1 & & b_{ij} \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ avec $\forall i \neq j |b_{ij}| \leq \varepsilon$.

Preuve : Soit $\beta = (b_1, \dots, b_n)$ une base de trigonalisation de A dans $\mathcal{M}_n(\mathbb{C})$ i.e. une base telle que

$$A_{\beta} = QAQ^{-1} = \begin{pmatrix} \lambda_1 & & a_{ij} \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

avec Q la matrice de la base β . Soit $p > 0$, posons $\beta_p = \left(b_1, \frac{b_2}{p}, \dots, \frac{b_n}{p^n}\right)$. β_p est aussi une base de $\mathcal{M}_n(\mathbb{C})$.

La matrice de A dans cette base s'écrit

$$V_p Q A Q^{-1} V_p^{-1} = \begin{pmatrix} \lambda_1 & & \frac{a_{ij}}{p^{|i-j|}} \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

avec $V_p = \text{Diag}\left(1, \frac{1}{p}, \dots, \frac{1}{p^{n-1}}\right)$. Il suffit ensuite de prendre p assez grand pour qu'on ait pour tout $i \neq j$, $\frac{|a_{i,j}|}{p} \leq \varepsilon$.

Exercice VIII.5.

Soit $A \in \mathcal{M}_n(\mathbb{C})$ tel que $\text{Spec}(A) \subset B(0, 1)$. Montrer que $A^p \xrightarrow[p \rightarrow +\infty]{} 0$.

Remarque : La propriété connue $\|A^p\|^{1/p} \xrightarrow[p \rightarrow \infty]{} \rho(A) = \sup\{|\lambda|, \lambda \in \text{Spec}_{\mathbb{C}}(A)\}$ dans \mathbb{C} permet de rapidement en conclure aussi.

Exercice VIII.6.

Soit $A \in \mathcal{M}_n(\mathbb{Z})$ tel que $\text{Spec}_{\mathbb{C}}(A) \subset B(0, 1)$. Montrer que A est nilpotente

3. Densité des matrices diagonalisables

Proposition VIII.7.

$\Omega = \{A \in \mathcal{M}_n(\mathbb{C}), A \text{ possède } n \text{ valeurs propres distinctes}\}$ est dense dans $\mathcal{M}_n(\mathbb{C})$.

Preuve

Soit β une base de \mathbb{C}^n tel que $[A]_{\beta} = PAP^{-1} = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ avec $P \in \text{GL}_n(\mathbb{K})$. Considérons alors (A_p) la suite de matrices vérifiant

$$\forall p \in \mathbb{N}, A_p = A + P^{-1} \begin{pmatrix} \frac{1}{p+1} & & 0 \\ & \ddots & \\ 0 & & \frac{1}{p+n} \end{pmatrix} P$$

On a alors

$$\forall p \in \mathbb{N}, [A_p]_{\beta} = [A]_{\beta} + \begin{pmatrix} \frac{1}{p+1} & & 0 \\ & \ddots & \\ 0 & & \frac{1}{p+n} \end{pmatrix}$$

On remarque que On a $\text{Spec}_{\mathbb{C}}(A) = [\lambda_1, \dots, \lambda_n]$. A partir de là, il y a deux moyens de conclure.

Méthode 1 : Considérons le polynôme non nul

$$P(X) = \prod_{i \neq j} (X+i)(X+j) \left(\lambda_i + \frac{1}{X+i} - \lambda_j - \frac{1}{X+j} \right) = \prod_{i \neq j} ((X+i)(X+j)(\lambda_i - \lambda_j) + j - i)$$

Il est clair que si A_p n'admet pas n valeurs propres distinctes alors $P(p) = 0$. P n'a qu'un nombre fini de racines et donc à partir d'un certain rang A_p admet toujours n valeurs propres distinctes. Finalement

$$A_p = A + P^{-1} \underbrace{\begin{pmatrix} \frac{1}{p+1} & & 0 \\ & \ddots & \\ 0 & & \frac{1}{p+n} \end{pmatrix}}_{\xrightarrow[p \rightarrow +\infty]{} 0} P \xrightarrow[p \rightarrow +\infty]{} A$$

d'où le résultat recherché.

Méthode 2 : Posons $\delta = \frac{1}{2} \min\{|\lambda_i - \lambda_j|, i \neq j \text{ et } \lambda_i \neq \lambda_j\} > 0$ et soit $k \in \mathbb{N}^*$ tel que $\frac{1}{k} < \delta$. Supposons par l'absurde qu'il existe deux termes diagonaux de $[A_p]_\beta$ égaux, il existe donc $i \neq j$ tel que $\lambda_i + \frac{1}{k+i} = \lambda_j + \frac{1}{k+j}$. Deux cas se présentent

$$\rightarrow \lambda_i = \lambda_j \text{ et donc } 0 = |\lambda_i - \lambda_j| = \left| \frac{1}{i+k} - \frac{1}{j+k} \right| \neq 0 \text{ ce qui est absurde.}$$

$$\rightarrow \lambda_i \neq \lambda_j \text{ et donc } \delta < |\lambda_i - \lambda_j| = \left| \frac{1}{i+k} - \frac{1}{j+k} \right| = \frac{|i-j|}{(k+i)(k+j)} \leq \frac{1}{k} < \delta \text{ ce qui est absurde.}$$

En déduit donc que pour tout $p \geq k$, A_p admet n valeurs propres distinctes, et $A_p \xrightarrow[p \rightarrow +\infty]{} A$, d'où le résultat voulu.

Conséquence : D'après la question 1 de l'exercice VII.4, pour tout $u \in \mathcal{L}(E)$, $\chi_u = \mu_u$ implique que u est cyclique. Or si u admet n valeurs propres deux à deux différentes, $\chi_u = \mu_u$ et donc u est cyclique. L'ensemble des endomorphismes ayant n valeurs propres deux à deux différentes (qui est dense) est inclus dans l'ensemble des endomorphismes cycliques. On en déduit donc que l'ensemble des les endomorphismes cycliques est dense dans $\mathcal{M}_n(\mathbb{C})$.

Application : On peut utiliser ce résultat pour redémontrer le théorème de Cayley-Hamilton.

Soit $A \in \mathcal{M}_n(\mathbb{C})$ et (A_p) une suite de matrices dont chacune possède n valeurs propres distinctes (et donc, a fortiori, est diagonalisable) tel que $A_p \xrightarrow[p \rightarrow +\infty]{} A$.

Lorsque $D \in \mathcal{M}_n(\mathbb{C})$ est diagonale, il est aisément d'établir que $\chi_D(D) = 0$. Idem pour le cas où D est diagonalisable. Ainsi, par continuité de $(A, B) \mapsto \chi_A(B)$ (l'image de (A, B) est une matrice dont les coordonnées sont produit et somme des coefficients de A et B)

$$\chi_A(A) = \lim_{p \rightarrow \infty} \chi_{A_p}(A_p) = \lim_{p \rightarrow \infty} 0 = 0$$

Remarque : On peut également montrer que Ω est ouvert. En effet

$$A \in \Omega \iff \chi_A \wedge \chi'_A = 1 \iff \det \chi'_A(A) \neq 0$$

$h : A \mapsto \det(\chi'_A(A))$ est continue et \mathbb{K}^* est ouvert, donc $\Omega = h^{-1}(\mathbb{K}^*)$ est ouvert.

Exercice VIII.8.

Soit $A \in \mathcal{M}_n(\mathbb{C})$, montrer que

$$A \text{ est diagonalisable} \iff \{P^{-1}AP, P \in \mathrm{GL}_n(\mathbb{C})\} \text{ est fermé}$$

4. Valeurs propres "pures"**Définition VIII.9.**

$\lambda \in \mathrm{Spec}_{\mathbb{K}}(A)$ est dite pure lorsque

$$E_{\lambda,u} = \mathrm{Ker}(A - \lambda I_n) = \mathrm{Ker}(A - \lambda I_n)^{\alpha_{\lambda}} = F_{\lambda,u}$$

ou alors d'une manière équivalente $\mathrm{Ker}(A - \lambda I_n) = \mathrm{Ker}(A - \lambda I_n)^2$.

Remarque : Cette propriété est aussi équivalente au fait que la composante nilpotente dans la décomposition de Dunford associée à l'espace caractéristique de λ est nulle (i.e. u est simplement une homothétie sur cet espace).

Exercice VIII.10.

Soit λ une valeur propre de $A \in \mathcal{M}_n(\mathbb{C})$ et $\|\cdot\|$ une norme sur \mathbb{C}^n . Montrer que si $|\lambda| = |||A|||$, avec $||| \cdot |||$ la norme d'opérateur associée à $\|\cdot\|$, alors λ est pure.

Application : Si $u \in \mathcal{M}_n(\mathbb{C})$ est une isométrie pour $\|\cdot\|$ alors u est diagonalisable. En effet, $\forall \lambda \in \mathrm{Spec}_{\mathbb{C}}(u)$, $|\lambda| = |||u||| = 1$ et donc $E_{\lambda,u} = F_{\lambda,u}$.

Correction de l'exercice II.5. :

→ Lorsque $\mathbb{K} = \mathbb{R}$, un tel plan existe.

En effet, le plan suivant privé de 0 est inclus dans $GL_2(\mathbb{R})$

$$P = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, (a, b) \in \mathbb{R}^2 \right\}$$

→ Lorsque $\mathbb{K} = \mathbb{C}$, il n'existe pas de tel plan.

En effet, supposons qu'il existe un plan P vérifiant ces conditions et soit (u, v) une base de P et $\lambda \in \mathbb{C}$. On a alors

$$u - \lambda v \in GL_n(\mathbb{C}) \iff \det(u - \lambda v) \neq 0 \underset{v \in GL_n(\mathbb{C})}{\iff} \det(uv^{-1} - \lambda id) \neq 0$$

Ce qui ne peut pas être vrai pour tout $\lambda \in \mathbb{C}$ car uv^{-1} admet une valeur propre dans \mathbb{C} .

Correction de l'exercice II.7. :

Soit λ une valeur propre de u . $u - \lambda \text{Id}$ commute avec tous les éléments de L et donc $F = \text{Ker}(u - \lambda id) \neq \{0\}$ est stable par tous les éléments L . L étant irréductible, on a $F = E$ et $u = \lambda \text{Id}$.

Correction de l'exercice III.5. :

Soit $\beta = (b_1, \dots, b_n)$ une base telle que $[u]_\beta = \text{diag}(\lambda_1, \dots, \lambda_n)$ où les λ_i sont les n valeurs propres distinctes de u . v commute avec u et donc pour tout $i \in \llbracket 1; n \rrbracket$, $\text{Ker}(u - \lambda_i id) = \text{Vect}(b_i)$ est stable par v et donc pour tout $i \in \llbracket 1; n \rrbracket$, il existe $\mu_i \in \mathbb{K}$ tel que $v(b_i) = \mu_i b_i$ et donc finalement $[v]_\beta = \text{diag}(\mu_1, \dots, \mu_n)$. On en déduit directement que v est diagonalisable.

En considérant un polynôme interpolateur $P \in \mathbb{K}[X]$ tel que $\forall i \in \llbracket 1; n \rrbracket$, $P(\lambda_i) = \mu_i$ (chose possible vu que les λ_i sont distincts), on voit que

$$[P(u)]_\beta = \text{diag}(P(\lambda_1), \dots, P(\lambda_n)) = \text{diag}(\mu_1, \dots, \mu_n) = [v]_\beta$$

d'où le résultat.

Correction de l'exercice IV.3. :

$X^2 - 1$ est un polynôme annulateur de u , donc $\mu_u | X^2 - 1$. μ_u n'est pas constant, il y a donc 2 possibilités

→ $\mu_u = X - 1$ ou $\mu_u = X + 1$, ce qui est impossible car $u \neq \pm \text{Id}$.

→ $\mu_u(X) = X^2 - 1$ est la seule possibilité qui reste, d'où la résultat voulu.

Correction de l'exercice IV.8. :

→ (1) ⇒ (2) Considérons $v = u \Big|_F^F$ (bien défini car F stable par u). $P(X) = \prod_{i=1}^s (X - \lambda_i)$ annule v , on a donc par le lemme de décomposition des noyaux

$$F = \text{Ker}(P(v)) = \bigoplus_{i=1}^s \text{Ker}(v - \lambda_i \text{Id}) = \bigoplus_{i=1}^s F \cap \text{Ker}(u - \lambda_i \text{Id}) = \bigoplus_{i=1}^s F \cap E_{\lambda_i, u}$$

→ (2) ⇒ (3) Il suffit de prendre pour tout $i \in \llbracket 1; s \rrbracket$, $F_i = F \cap E_{\lambda_i, u}$.

→ (3) ⇒ (1) Chaque F_i est stable par u , donc F , qui est égal à la somme directe des F_i , est également stable par u .

Correction de l'exercice IV.9. :

Méthode 1 :

→ Soit $v \in \text{Com}(u)$. Posons

$$[v]_\beta = \begin{pmatrix} A_{1,1} & \dots & A_{1,s} \\ \vdots & \ddots & \vdots \\ A_{s,1} & \dots & A_{s,s} \end{pmatrix}$$

avec pour tout $i, j \in \llbracket 1; s \rrbracket$, $A_{i,j} \in \mathcal{M}_{l_i, l_j}(\mathbb{K})$. On a alors

$$\begin{pmatrix} \lambda_1 A_{1,1} & \dots & \lambda_1 A_{1,s} \\ \vdots & \ddots & \vdots \\ \lambda_s A_{s,1} & \dots & \lambda_s A_{s,s} \end{pmatrix} = [u]_\beta \times [v]_\beta = [u \circ v]_\beta = [v \circ u]_\beta = [v]_\beta \times [u]_\beta = \begin{pmatrix} \lambda_1 A_{1,1} & \dots & \lambda_s A_{1,s} \\ \vdots & \ddots & \vdots \\ \lambda_1 A_{s,1} & \dots & \lambda_s A_{s,s} \end{pmatrix}$$

On a alors $(\lambda_i A_{i,j})_{i,j \in \llbracket 1; s \rrbracket} = (\lambda_j A_{i,j})_{i,j \in \llbracket 1; s \rrbracket}$, i.e. pour tout $i \neq j$,

$$\lambda_i A_{i,j} = \lambda_j A_{i,j}$$

ce qui implique que $A_{i,j} = 0$ car les λ_i sont deux à deux distincts. v s'écrit donc bien dans la base β sous la forme

$$v = \begin{pmatrix} A_{1,1} & & 0 \\ & \ddots & \\ 0 & & A_{s,s} \end{pmatrix}$$

→ Réciproquement, si on suppose que v s'écrit comme ci-dessus, alors

$$[v \circ u]_\beta = [v]_\beta \times [u]_\beta = \begin{pmatrix} \lambda_1 A_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_s A_s \end{pmatrix} = [u]_\beta \times [v]_\beta = [u \circ v]_\beta$$

donc $v \in \text{Com}(u)$.

Méthode 2 :

- Notons S l'ensemble de droite. Il est alors clair que $S \subset \text{Com}(u)$ (pour s'en convaincre, voir le dernier point de la méthode 1).
- Réciproquement, soit $v \in \text{Com}(u)$. Pour tout $i \in \llbracket 1; s \rrbracket$, $E_{\lambda_i, u}$ est stable par v . La proposition I.5 nous permet d'affirmer que dans la base β , v s'écrit bien de la manière voulue.

Une autre solution de l'exercice III.5 consiste à utiliser ce résultat pour $s = n$ et $l_i = 1$ pour tout $i \in \llbracket 1; s \rrbracket$.

Remarque : une conséquence de ce résultat est que $\dim(\text{Com}(u)) = \sum_{i=1}^s l_i^2 \geq n$ avec égalité si et seulement si $n = s$ et pour tout $i \in \llbracket 1; s \rrbracket$, $l_i = 1$. L'inégalité $\dim_{\mathbb{C}}(\text{Com}(u)) \geq n$ est en fait toujours vraie même sans diagonalisabilité lorsque $u \in \mathcal{L}(\mathbb{C}^n)$. On le prouvera dans un exercice ultérieur.

Correction de l'exercice IV.11. :

- (\Leftarrow) Dans une base β où les matrices de tous les endomorphismes de S sont de matrice diagonale, toutes ces matrices commutent ce qui nous donne bien le résultat voulu.
- (\Rightarrow) Procédons par récurrence forte sur la dimension n de E .
 - Le cas $n = 1$ est évident car dans ce cas tous les endomorphismes de E commutent et sont diagonaux.
 - Soit $n \geq 1$. Supposons que la propriété est vraie pour tout $k \in \llbracket 1; n \rrbracket$. Le cas où tous les éléments de S sont des homothéties est évident, on suppose donc que ce n'est pas le cas. On

dispose donc de $u \in S$, $s \geq 2$ et $\lambda_1, \dots, \lambda_s$ ses valeurs propres comptées sans multiplicité. Tout élément $v \in S$ commute avec u , donc pour tout $i \in \llbracket 1; s \rrbracket$, $E_{\lambda_i, u}$ est stable par tout élément de S . En posant $F = \bigoplus_{i=2}^s E_{\lambda_i, u}$, on voit clairement que F est stable par tout élément de S . Considérons les deux ensembles

$$S_1 = \left\{ v \Big|_{E_{\lambda_1, u}}^{E_{\lambda_1, u}}, v \in S \right\} \text{ et } S_2 = \left\{ v \Big|_F^F, v \in S \right\}$$

On peut appliquer l'hypothèse de récurrence à $E_{\lambda_1, u}$ pour S_1 et à F pour S_2 . Il existe une base β_1 (resp. β_2) de $E_{\lambda_1, u}$ (resp. F) dans laquelle les matrices de tous les éléments de S_1 (resp. S_2) sont diagonales. On en déduit donc que les matrices de tous les éléments de S dans la base $\beta = (\beta_1, \beta_2)$ sont diagonales, ce qui est bien le résultat recherché.

Correction de l'exercice IV.12. :

Considérons l'ensemble

$$S = \{\text{diag}(\varepsilon_1, \dots, \varepsilon_m), (\varepsilon_1, \dots, \varepsilon_m) \in \{-1, 1\}^m\}$$

S est clairement un sous-groupe de $\text{GL}_m(\mathbb{K})$ de cardinal 2^m (car $\text{car } \mathbb{K} \neq 2$).

Posons $S' := \varphi(S)$. φ est injective, donc S' est un sous-groupe de $\text{GL}_n(\mathbb{K})$ de cardinal 2^m .

Remarquons que pour tout $A \in S$, $A^2 = I_m$ donc pour tout $A' \in S'$, il existe $A \in S$ tel que $A' = \varphi(A)$ et donc $A'^2 = \varphi(A)^2 = I_n$. $X^2 - 1$ annule donc tout élément de S' et est scindé à racines simples dans \mathbb{K} (car $\text{car } \mathbb{K} \neq 2$) et donc chaque élément de S' est diagonalisable. De plus, les éléments de S commutent entre eux, donc ceux de S' aussi.

Ainsi, en utilisant l'exercice précédent, on dispose d'une base β de $M_n(\mathbb{K})$ où la matrice de tout élément de S' est diagonale. Par construction, le carré de chacune de ces matrices est égal à l'identité, ce qui impose que $[S']_\beta = \{[v]_\beta, v \in S'\} \subset \{\text{diag}(\varepsilon_1, \dots, \varepsilon_n), (\varepsilon_1, \dots, \varepsilon_n) \in \{-1, 1\}^n\}$. On a alors

$$2^m = |S'| = |[S']_\beta| \leq 2^n$$

i.e. $m \leq n$.

Correction de l'exercice IV.13. :

→ (\Rightarrow) Supposons que u^2 et u soient diagonalisables. Il existe une base β et une matrice diagonale $D \in \mathcal{M}_n(\mathbb{C})$ telle que $[u]_\beta = D$. De plus $\text{rg } D = \text{rg } D^2$ (il s'agit du nombre de coefficients non nuls sur la diagonale) et donc $\text{rg } u = \text{rg } u^2$. La formule du rang nous donne donc $\dim \text{Ker } u = \dim \text{Ker } u^2$. En combinant ce résultat avec le fait que $\text{Ker } u \subset \text{Ker } u^2$, on obtient $\text{Ker } u = \text{Ker } u^2$.

→ (\Leftarrow) Deux cas se présentent

- u est inversible (i.e. $\text{Ker } u^2 = \text{Ker } u = \{0\}$).

Considérons $\lambda_1, \dots, \lambda_s$ les valeurs propres comptées sans multiplicité non nulles de u^2 et $\alpha_1, -\alpha_1, \dots, \alpha_s, -\alpha_s$ leurs racines complexes distinctes respectives. Le polynôme $P(X) = \prod_{i=1}^s (X - \lambda_i)$ annule u^2 et donc le polynôme

$$P(X^2) = \prod_{i=1}^s (X^2 - \lambda_i) = \prod_{i=1}^s (X - \alpha_i)(X + \alpha_i)$$

scindé à racines simples annule u , donc u est diagonalisable.

- u n'est pas inversible, donc u^2 non plus.

Reprendons les notations du point précédent et considérons que $\lambda_1 = 0$. Le polynôme

$$P(X^2) = X^2 \prod_{i=2}^s (X - \alpha_i)(X + \alpha_i)$$

annule u , et donc par le lemme des noyaux

$$\begin{aligned} E = \text{Ker } P(u^2) &= \text{Ker } u^2 \oplus \bigoplus_{i=2}^s (\text{Ker}(u - \alpha_i \text{Id}) \oplus \text{Ker}(u + \alpha_i \text{Id})) \\ &= \text{Ker } u \oplus \bigoplus_{i=2}^s (\text{Ker}(u - \alpha_i \text{Id}) \oplus \text{Ker}(u + \alpha_i \text{Id})) \end{aligned}$$

On en déduit que E est somme directe d'espaces propres de u , i.e. u est diagonalisable.

Correction de l'exercice V.3. :

Posons $A = (a_{i,j})_{i,j \in \llbracket 1; n \rrbracket}$. Pour calculer le polynôme caractéristique de ϕ_A , nous allons calculer sa matrice dans la base

$$\mathcal{B} = (E_{1,1}, \dots, E_{1,n}, \dots, E_{n,1}, \dots, E_{n,n})$$

et posons pour tout $i \in \llbracket 1; n \rrbracket$, $\mathcal{B}_i = (E_{i,j})_{j \in \llbracket 1; n \rrbracket}$ et remarquons que $\mathcal{B} = (\mathcal{B}_1, \dots, \mathcal{B}_n)$.

Soit $i \in \llbracket 1; n \rrbracket$. On a pour tout $j \in \llbracket 1; n \rrbracket$, $\phi_A(E_{i,j})$ est égal à une matrice de coefficients nuls partout, sauf à la ligne i où se trouve la ligne j de la matrice A . On a donc

$$\phi_A(E_{i,j}) = a_{j,1}E_{i,1} + \dots + a_{j,n}E_{i,n} \in \text{Vect } \mathcal{B}_i$$

On en déduit que pour tout $i \in \llbracket 1; n \rrbracket$, $\text{Vect } \mathcal{B}_i$ est stable par ϕ_A . Il existe donc des matrices $B_1, \dots, B_n \in \mathcal{M}_n(\mathbb{C})$ telles que

$$[\phi_A]_{\mathcal{B}} = \begin{pmatrix} B_1 & & 0 \\ & \ddots & \\ 0 & & B_n \end{pmatrix}$$

Soit $k \in \llbracket 1; n \rrbracket$. Pour tout $i, j \in \llbracket 1; n \rrbracket$, le coefficient de position i, j de B_k est égal à le coefficient de $E_{k,i}$ dans la décomposition de $\phi_A(E_{k,j})$ dans la base \mathcal{B}_k , qui est égal à $a_{j,i}$. On en déduit donc que pour tout $k \in \llbracket 1; n \rrbracket$, $B_k = A^T$ et alors

$$\chi_{\phi_A}(X) = \det(XI_{n^2} - [\phi_A]_{\mathcal{B}}) = \det \begin{pmatrix} XI_n - A^T & & 0 \\ & \ddots & \\ 0 & & XI_n - A^T \end{pmatrix} = \det (XI_n - A^T)^n = \chi_A(X)^n$$

Correction de l'exercice V.10. :

→ (⇒) Supposons que A soit diagonalisable. Il existe donc $P \in \text{GL}_n(\mathbb{K})$ et D une matrice diagonale $D \in \mathcal{M}_n(\mathbb{K})$ telle que $PAP^{-1} = D$. On en déduit donc que pour tout $\lambda \in \text{VP}(A)$

$$\text{rg}(A - \lambda \text{Id})^2 = \text{rg } P(A - \lambda \text{Id})^2 P^{-1} = \text{rg}(D - \lambda \text{Id})^2$$

$\text{rg}(D - \lambda \text{Id})^2$ est égal au nombre de coefficients diagonaux non nuls dans $(D - \lambda \text{Id})^2$. Ce nombre est le même que le nombre de coefficients non nuls dans la matrice diagonale $D - \lambda \text{Id}$ (les deux matrices sont diagonales). On a alors

$$\text{rg}(A - \lambda I)^2 = \text{rg}(A - \lambda I)$$

et finalement par la formule du rang

$$\dim \text{Ker}(A - \lambda I)^2 = \dim \text{Ker}(A - \lambda I)$$

$\rightarrow (\Leftarrow)$ Supposons que χ_A est scindé et que pour tout $\lambda \in \text{VP}(A)$,

$$\dim \text{Ker}(A - \lambda \text{Id}) = \dim \text{Ker}(A - \lambda \text{Id})^2$$

Soit $\lambda \in \text{VP}(A)$. On a $\text{Ker}(A - \lambda \text{Id}) \subset \text{Ker}(A - \lambda \text{Id})^2$, et ces deux sous espaces sont de même dimension, donc $\text{Ker}(A - \lambda \text{Id}) = \text{Ker}(A - \lambda \text{Id})^2$. nous allons montrer que pour tout $k \in \mathbb{N}^*$, $\text{Ker}(A - \lambda \text{Id}) = \text{Ker}(A - \lambda \text{Id})^k$. Soit $k \geq 2$ et $X \in \mathbb{K}^n$, on a

$$\begin{aligned} (A - \lambda \text{Id})^k X = 0 &\implies (A - \lambda \text{Id})^2(A - \lambda \text{Id})^{k-2}X = 0 \\ &\implies (A - \lambda \text{Id})(A - \lambda \text{Id})^{k-2}X = 0 \\ &\implies (A - \lambda \text{Id})^{k-1}X = 0 \end{aligned}$$

En itérant ce procédé $k - 1$ fois, on obtient que

$$(A - \lambda \text{Id})^k X = 0 \implies (A - \lambda \text{Id})^{k-1}X = 0 \implies \dots \implies (A - \lambda \text{Id})X = 0$$

On en déduit donc que $\text{Ker}(A - \lambda \text{Id})^k \subset \text{Ker}(A - \lambda \text{Id})$, i.e. $\text{Ker}(A - \lambda \text{Id})^k = \text{Ker}(A - \lambda \text{Id})$.

Remarquons que ce raisonnement peut aussi être fait par récurrence.

χ_A est scindé, on peut donc écrire

$$\chi_A(X) = \prod_{i=1}^s (X - \lambda_i)^{\alpha_i}$$

où $\lambda_1, \dots, \lambda_s \in \mathbb{K}$ sont les valeurs propres de A . On a donc par le lemme des noyaux

$$\mathbb{K}^n = \text{Ker } \chi_A(A) = \bigoplus_{i=1}^s \text{Ker}(A - \lambda_i \text{Id})^{\alpha_i} = \bigoplus_{i=1}^s \text{Ker}(A - \lambda_i \text{Id})$$

\mathbb{K}^n est donc somme directe des espaces propres de A i.e. A est diagonalisable.

Correction de l'exercice VI.5. :

- $\rightarrow (1) \Rightarrow (2)$ Supposons que u est nilpotent. Pour tout $k \geq 1$, la seule valeur propre de u^k dans \mathbb{C} est 0 et $\text{Tr}(u^k)$ est égal à la somme des valeurs propres de u^k , et donc pour tout $k \in \llbracket 1; n \rrbracket$, $\text{Tr}(u^k) = 0$.
- $\rightarrow (2) \Rightarrow (1)$ Supposons que pour tout $k \in \llbracket 1; n \rrbracket$, $\text{Tr}(u^k) = 0$. Soit $\lambda_1, \dots, \lambda_s$ les coefficients diagonaux sans répétition et sans coefficients nuls de la matrice trigonalisée de u et soit $n_1, \dots, n_s \in \llbracket 1; n \rrbracket$ le nombre respectifs d'occurrences de $\lambda_1, \dots, \lambda_s$ dans cette diagonale. supposons que $s \geq 1$. La condition $\text{Tr}(u^k) = 0$ pour tout $k \in \llbracket 1; s \rrbracket$ donne

$$\begin{cases} n_1\lambda_1 + \dots + n_s\lambda_s &= 0 \\ n_1\lambda_1^2 + \dots + n_s\lambda_s^2 &= 0 \\ \vdots \\ n_1\lambda_1^s + \dots + n_s\lambda_s^s &= 0 \end{cases}$$

i.e.

$$\begin{pmatrix} \lambda_1 & \dots & \lambda_s \\ \lambda_1^2 & \dots & \lambda_s^2 \\ \vdots & \ddots & \vdots \\ \lambda_1^s & \dots & \lambda_s^s \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_s \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

En posant $M = \begin{pmatrix} \lambda_1 & \dots & \lambda_s \\ \lambda_1^2 & \dots & \lambda_s^2 \\ \vdots & \ddots & \vdots \\ \lambda_1^s & \dots & \lambda_s^s \end{pmatrix}$, on voit que

$$\det M = \lambda_1 \dots \lambda_s \det \begin{pmatrix} 1 & \dots & 1 \\ \lambda_1 & \dots & \lambda_s \\ \vdots & \ddots & \vdots \\ \lambda_1^{s-1} & \dots & \lambda_s^{s-1} \end{pmatrix} = \lambda_1 \dots \lambda_s \det V(\lambda_1, \dots, \lambda_s)^T$$

$$= \lambda_1 \dots \lambda_s \prod_{i,j \in \llbracket 1; n \rrbracket, i \neq j} (\lambda_i - \lambda_j) \neq 0$$

où $V(\lambda_1, \dots, \lambda_s)$ est la matrice de Vandermonde associée à $\lambda_1, \dots, \lambda_s$. Ce dernier nombre est non nul car les λ_i sont tous non nuls et distincts. La formule de ce déterminant est assez classique, nous ne le démontrerons donc pas (une récurrence suffit pour le faire).

M est donc inversible et alors $n_1 = \dots = n_s = 0$, ce qui est absurde. On a alors $s = 1$, i.e. les coefficients diagonaux de la matrice trigonalisée de u sont donc tous égaux à 0.

→ (2) ⇒ (3) Supposons que (2) est vérifiée. u est alors nilpotente et le coefficient de nilpotence de u est inférieur à n , donc pour tout $k \in \mathbb{N}^*$, $\text{Tr}(u^k) = 0$. Soit $m \in \mathbb{N}$ et $P(X) = \sum_{i=0}^m a_i X^i \in \mathbb{K}[X]$. On a

$$\text{Tr}(P(u)) = \sum_{i=0}^m a_i \text{Tr}(u^i) = a_0 \text{Tr}(\text{Id}) = nP(0)$$

→ (3) ⇒ (2) Supposons que (3) est vérifiée, on a alors pour tout $k \in \mathbb{N}^*$, en posant $P(X) = X^k$,

$$\text{Tr}(u^k) = \text{Tr}(P(u)) = nP(0) = 0$$

Correction de l'exercice VI.6. :

Dans cet exercice, on suppose que $\mathbb{K} = \mathbb{C}$.

1. Faisons une discussion des cas pour $n = 2$ puis $n = 3$.

→ Pour $n = 2$

- Si $\deg \mu_A = 1$, alors il existe $\lambda \in \mathbb{K}$, tel que $\mu_A(X) = X - \lambda$, et donc $A = \lambda I$.
- Si $\deg \mu_A = 2$, alors il y a deux possibilités.
 - ▷ Il existe $\lambda, \delta \in \mathbb{K}$ différents tels que $\chi_A(X) = \mu_A(X) = (X - \lambda)(X - \delta)$. χ_A est scindé à racines simples, donc A est diagonalisable et $A \simeq \text{diag}(\lambda, \delta)$.
 - ▷ Il existe $\lambda \in K$ tel que $\chi_A(X) = \mu_A(X) = (X - \lambda)^2$. En trigonalisant, on voit que $A \simeq \begin{pmatrix} \lambda & a \\ 0 & \lambda \end{pmatrix}$ dans une base $\beta = (b_1, b_2)$. De plus $a \neq 0$, car sinon on aurait $\mu_A(X) = X - \lambda$. Enfin, on voit qu'en regardant la matrice A dans la base (ab_1, b_2) , $A \simeq \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$.

On en déduit donc que les classes de similitudes de $\mathcal{M}_2(\mathbb{K})$ sont

$$\mathcal{C}_2 = \left\{ \left\langle \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \right\rangle, \lambda \in \mathbb{K} \right\} \cup \left\{ \left\langle \begin{pmatrix} \lambda & 0 \\ 0 & \delta \end{pmatrix} \right\rangle, \lambda, \delta \in \mathbb{K} \right\}$$

→ Pour $n = 3$

- S'il existe $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{K}$ distincts tels que $\chi_A(X) = (X - \lambda_1)(X - \lambda_2)(X - \lambda_3)$, alors A est diagonalisable, $\mu_A = \chi_A$ et $A \simeq \text{diag}(\lambda_1, \lambda_2, \lambda_3)$.
- S'il existe $\lambda, \delta \in \mathbb{K}$ différents tels que $\chi_A(X) = (X - \lambda)^2(X - \delta)$, alors deux cas se présentent.
 - ▷ Si $\mu_A(X) = (X - \lambda)(X - \delta)$, alors A est diagonalisable et $A \simeq \text{diag}(\lambda, \lambda, \delta)$.
 - ▷ Si $\mu_A = \chi_A$, alors on a

$$\mathbb{K}^n = \text{Ker}(A - \lambda I)^2 \oplus \text{Ker}(A - \delta I)$$

Il existe donc une base où $A \simeq \begin{pmatrix} B & 0 \\ 0 & \delta \end{pmatrix}$ où $B \in \mathcal{M}_2(\mathbb{K})$ est la matrice de la corestriction de A à $\text{Ker}(A - \delta \text{Id})^2$. On a $\mu_B(X) = (X - \lambda)^2$, donc d'après la discussion pour $n = 2$,

$$B \simeq \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \text{ et finalement } A \simeq \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \delta \end{pmatrix}$$

- S'il existe $\delta \in \mathbb{K}$ tel que $\chi_A(X) = (X - \lambda)^3$
 - ▷ Si $\mu_A(X) = X - \lambda$, alors $A \simeq \lambda I$.
 - ▷ Si $\mu_A(X) = (X - \lambda)^2$ alors on peut écrire $A = \lambda I + N$ avec N nilpotente d'indice de nilpotence égal à 2. Soit $X \in \mathbb{K}^3$ tel que $NX \neq 0$. la famille (NX, X) est libre (raisonnement déjà fait avant). Complétons cette famille en une base $\beta = (NX, X, Y)$ avec $Y \in \mathbb{K}^n$. On a alors, dans cette base

$$[N]_\beta = \begin{pmatrix} 0 & 1 & a \\ 0 & 0 & b \\ 0 & 0 & c \end{pmatrix}$$

avec $a, b, c \in \mathbb{K}$. c est une valeur propre de N , donc on a nécessairement $c = 0$. De plus, on a

$$0 = N^2Y = N(NY) = N(aNX + bX) = bNX$$

donc $b = 0$. Enfin, en regardant N dans la base $\beta' = (NX, X, Y - aX)$, on voit que

$$[N]_{\beta'} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ et donc finalement } A \simeq \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$$

▷ Si $\mu_A(X) = \chi_A(X) = (X - \lambda)^3$, alors on peut écrire $A = \lambda I + N$ avec N d'ordre de nilpotence égal à 3. En prenant donc $X \in \mathbb{K}^3$ tel que $N^2X \neq 0$, on voit que $\beta = (N^2X, NX, X)$ est une base de \mathbb{K}^3 et dans cette base

$$[N]_\beta = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \text{ et donc finalement } A \simeq \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}$$

On en déduit donc que les classes de similitude dans $\mathcal{M}_3(\mathbb{K})$ sont

$$\mathcal{C}_3 = \left\{ \left\langle \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix} \right\rangle, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{K} \right\} \cup \left\{ \left\langle \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \delta \end{pmatrix} \right\rangle, \lambda, \delta \in \mathbb{K} \right\} \cup \left\{ \left\langle \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix} \right\rangle, \lambda \in \mathbb{K} \right\}$$

2. Il suffit de revoir la discussion ci-dessus pour répondre à la question.

3. On peut trouver le contre-exemple suivant pour $n = 4$

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

En effet, $\mu_A = \mu_B = X^2$ et $\chi_A = \chi_B = X^4$ mais $A \not\sim B$ car $\text{rg}(A) = 1$ et $\text{rg}(B) = 2$.

Correction de l'exercice VI.7. :

Procédons par récurrence forte sur la dimension n de E .

- Le cas $n = 1$ est évident car dans ce cas tous les endomorphismes de E commutent et sont triangulaires supérieurs dans toute base.
- Soit $n \geq 1$. Supposons que la propriété est vraie pour tout $k \in \llbracket 1; n \rrbracket$.

Soit $u \in S$ non homothétie (le cas $S \subset \mathbb{K} \cdot \text{Id}$ étant trivial) et soit λ_1 une de ses valeurs propres.

Posons β_1 une base de $E_{\lambda_1, u}$, de dimension $a < n$, qui est stable par tout élément de S . Prenons maintenant F un supplémentaire quelconque de $E_{\lambda_1, u}$ dans E de dimension b et de base β_2 . Tous les éléments de S sont triangulaires supérieurs par blocs dans $\beta = (\beta_1, \beta_2)$. En particulier, pour tout $u \in S$, il existe $(A_u, B_u, C_u) \in \mathcal{M}_a(\mathbb{K}) \times \mathcal{M}_{a \times b}(\mathbb{K}) \times \mathcal{M}_b(\mathbb{K})$ tels que

$$[u]_\beta = \begin{pmatrix} A_u & B_u \\ 0 & C_u \end{pmatrix}$$

On considère alors les deux ensembles

$$S_1 = \{A_v, v \in S\} \text{ et } S_2 = \{C_s, v \in S\}$$

On peut appliquer l'hypothèse de récurrence à S_1 et S_2 (les matrices commutent toujours et sont toujours trigonalisables et de plus $1 \leq a \leq n - 1$ et $1 \leq b \leq n - 1$). Il existe donc une matrice inversible $P \in \text{GL}_a(\mathbb{K})$ (resp. $Q \in GL_b(\mathbb{K})$) telle que pour tout $s \in S$, $P^{-1}A_sP \in \mathcal{T}_a^+(\mathbb{K})$ (resp. $Q^{-1}C_sQ \in \mathcal{T}_b^+(\mathbb{K})$). Finalement, pour la base γ correspondante au changement de base (depuis β) induit par

$$R = \begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix}$$

Il est clair que $[u]_\gamma = R^{-1}[u]_\beta R$ est triangulaire supérieure pour tout $u \in S$, ce qui est bien le résultat voulu.

Correction de l'exercice VI.10. :

$$1. X^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 9 \end{pmatrix} \text{ dans } \mathcal{M}_3(\mathbb{R})$$

Soit X une solution de l'équation. X^2 et X commutent, donc X laisse stable les espaces propres de X^2 , i.e. X laisse stable $\text{Vect}(e_1), \text{Vect}(e_2), \text{Vect}(e_3)$ avec (e_1, e_2, e_3) la base canonique de \mathbb{R}^3 . On en déduit donc que X est diagonale, i.e. il existe $\alpha, \beta, \gamma \in \mathbb{R}$ tels que

$$X = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$$

en réinjectant dans l'équation, on voit qu'on a nécessairement $(\alpha^2, \beta^2, \gamma^2) = (1, 4, 9)$ et donc $(\alpha, \beta, \gamma) = (\pm 1, \pm 2, \pm 3)$. Réciproquement, une matrice de cette forme vérifie bien l'équation, donc

l'ensemble des solutions est bien

$$S = \left\{ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}, (\alpha, \beta, \gamma) \in \{1, -1\} \times \{2, -2\} \times \{3, -3\} \right\}$$

2. $X^2 = \begin{pmatrix} a^2 & 1 \\ 0 & a^2 \end{pmatrix}$ dans $\mathcal{M}_2(\mathbb{C})$ avec $a \in \mathbb{C}$

Soit X une solution de l'équation. $\text{Vect}(e_1)$ est un espace propre de X^2 . De plus X et X^2 commutent, donc X laisse stable $\text{Vect}(e_1)$. Il existe donc $\alpha, \beta, \gamma \in \mathbb{C}$ tels que

$$X = \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}$$

On a alors

$$\begin{pmatrix} \alpha^2 & \alpha\beta + \gamma\beta \\ 0 & \gamma^2 \end{pmatrix} = X^2 = \begin{pmatrix} a^2 & 1 \\ 0 & a^2 \end{pmatrix}$$

En utilisant cette inégalité, on voit que $a \neq 0$, car sinon $\alpha = \gamma = \beta = 0$ et alors $X = 0$. En elevant les cas où l'égalité est fausse, on obtient que $(\alpha, \beta, \gamma) \in \left\{ \left(a, \frac{1}{2a}, a \right), \left(-a, -\frac{1}{2a}, -a \right) \right\}$. Réciproquement, en réinjectant ces deux matrices possibles dans l'équation, on voit que elles sont bien solutions. On en déduit que l'ensemble des solutions est bien

$$S = \left\{ \begin{pmatrix} a & \frac{1}{2a} \\ 0 & a \end{pmatrix}, \begin{pmatrix} -a & -\frac{1}{2a} \\ 0 & -a \end{pmatrix} \right\}$$

3. $X^2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ dans $\mathcal{M}_3(\mathbb{R})$

Soit X une solution de l'équation. Posons $\beta = (e_3, e_1, e_2)$ une permutation de la base canonique et regardons la matrice X dans cette base. Posons $Y = [X]_\beta$. On a

$$Y^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Y commute avec Y^2 et laisse donc ses espaces propres stables, donc Y laisse stable $\text{Vect}((1, 0, 0)^T, (0, 1, 0)^T)$. Il existe donc $x, y, z, t, c, d, e \in \mathbb{R}$ tels que

$$Y = \begin{pmatrix} x & y & c \\ z & t & d \\ 0 & 0 & e \end{pmatrix}$$

En posant $A = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$, on voit que $A^2 = I$, donc A est inversible. On a alors

$$\begin{pmatrix} A^2 & (A + eI) \times \begin{pmatrix} c \\ d \end{pmatrix} \\ 0 & e^2 \end{pmatrix} = Y^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Donc

$$A^2 = I \quad (A + eI) \times \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad e^2 = 1$$

La suite de l'exercice est laissée au lecteur : il suffit d'évaluer les différents cas possible pour trouver

toutes les solutions de l'équation.

Correction de l'exercice VI.11. :

→ (⇒) Supposons que u est diagonalisable. Soit $\beta = (e_1, \dots, e_n)$ une base de diagonalisation de u . Il existe donc $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ tels que $[u]_\beta = D = \text{diag}(\lambda_1, \dots, \lambda_n)$. Pour tout $i, j \in \llbracket 1; n \rrbracket$, on considère $v_{i,j} \in \mathcal{L}(E)$ définie par

$$\forall k \in \llbracket 1; n \rrbracket, v_{i,j}(e_k) = \begin{cases} e_i & \text{si } k = j \\ 0 & \text{sinon} \end{cases}$$

On a alors, pour tout $i, j \in \llbracket 1; n \rrbracket$,

$$\begin{aligned} [\phi_u(v_{i,j})]_\beta &= [u \circ v_{i,j} - v_{i,j} \circ u]_\beta \\ &= DE_{i,j} - E_{i,j}D \\ &= (\lambda_i - \lambda_j)E_{i,j} = [(\lambda_i - \lambda_j)v_{i,j}]_\beta \end{aligned}$$

On en déduit donc que $(v_{i,j})_{i,j \in \llbracket 1; n \rrbracket}$ est une base de vecteurs propres de ϕ_u , donc ϕ_u est diagonalisable.

→ (⇐) Supposons que ϕ_u est diagonalisable. Utilisons la décomposition de Dunford. Sois $\delta, \nu \in \mathcal{L}(E)$ tels que δ est diagonalisable, ν est nilpotent et $u = \delta + \nu$. δ et ν commutent, donc il est facile de vérifier que ϕ_δ et ϕ_ν aussi. De plus, d'après le point précédent, ϕ_δ est diagonalisable et pour tout $p \in \mathbb{N}$ et $v \in \mathcal{L}(E)$,

$$\phi_\nu^p(v) = \sum_{k=0}^p \binom{p}{k} (-1)^{p-k} \nu^k \circ v \circ \nu^{p-k}$$

Donc ϕ_ν est nilpotent. ϕ_u est diagonalisable, donc par unicité de la décomposition de Dunford, $\phi_\nu = 0$, i.e. $\nu = 0$ et donc u est diagonalisable.

Correction de l'exercice VI.12. :

En décomposant sur chaque espace caractérisique (proposition VI.8), on sait que E s'écrit sous forme de somme directe de sous espaces (espaces caractéristiques) F_1, \dots, F_s stables par u et où pour tout i , il existe ν_i nilpotent et $\lambda_i \in \mathbb{K}^*$ tels que

$$u\Big|_{F_i}^{F_i} = \lambda_i \text{Id} + \nu_i$$

Il suffit donc de montrer ce résultat à l'application linéaire ci-dessus. Nous allons nous inspirer du développement limité en 0 de $x \mapsto \sqrt{1+x}$. On a

$$\sqrt{1+x} = 1 + \frac{x}{2} + \dots + (-1)^{n-1} \frac{(2n)!}{2^{2n}(n!)^2} x^n + o(x^n) = P_n(x) + o(x^n)$$

On a alors

$$P_n(x)^2 = 1 + x + \underbrace{o(x^n)}_{Q(x)}$$

où Q est un polynôme de terme de plus petit degré égal à au moins n . On peut donc écrire $Q(X) = X^n R(X)$ avec $R \in \mathbb{K}[X]$. On a alors, si α_i est une racine de λ_i , alors

$$\left(\alpha_i P_n \left(\frac{1}{\lambda_i} \nu_i \right) \right)^2 = \lambda_i \text{Id} + \nu_i + \frac{1}{\lambda_i^{n-1}} \nu_i^n R \left(\frac{1}{\lambda_i} \nu_i \right) = \lambda_i \text{Id} + \nu_i$$

et donc $\alpha_i P_n \left(\frac{1}{\lambda_i} \nu_i \right)$ est une racine de $\lambda_i \text{Id} + \nu_i$, d'où le résultat voulu.

Correction de l'exercice VI.15. :

Soit $A \in \mathcal{M}_n(\mathbb{C})$. En utilisant la décomposition de Jordan, on sait qu'il existe une base β , $\lambda_1, \dots, \lambda_r \in \mathbb{C}$ non nécessairement distincts et $s_1, \dots, s_r \in \llbracket 1; n \rrbracket$ tels que $s_1 + \dots + s_r = n$ et

$$[A]_\beta = \begin{pmatrix} \lambda_1 \cdot I_{s_1} + J_{s_1} & & 0 \\ & \ddots & \\ 0 & & \lambda_r \cdot I_{s_r} + J_{s_r} \end{pmatrix}$$

Pour tout $i \in \llbracket 1; r \rrbracket$, on considère l'application linéaire injective $\phi_i : \mathcal{M}_{s_i}(\mathbb{C}) \rightarrow \mathcal{M}_n(\mathbb{C})$ définie par

$$\forall B \in \mathcal{M}_{s_i}(\mathbb{C}), \phi_i(B) = \begin{pmatrix} 0_{\mathcal{M}_{s_1}(\mathbb{C})} & & & & & \\ & \ddots & & & & 0 \\ & & 0_{\mathcal{M}_{s_{i-1}}(\mathbb{C})} & & & \\ & & & B & & \\ & & & & 0_{\mathcal{M}_{s_{i+1}}(\mathbb{C})} & \\ 0 & & & & & \ddots \\ & & & & & 0_{\mathcal{M}_{s_r}(\mathbb{C})} \end{pmatrix}$$

On a alors

$$\text{Com}(A) \approx \text{Com}([A]_\beta) \supset \bigoplus_{i=1}^r \phi_i(\text{Com}(\lambda_i I_{s_i} + J_{s_i})) = \bigoplus_{i=1}^r \phi_i(\text{Com}(J_{s_i}))$$

Il suffit de montrer que pour tout $s \in \llbracket 1; n \rrbracket$, $\dim \text{Com}(J_s) \geq s$ car une fois cela fait, on aurait

$$\dim \text{Com}(A) = \dim \text{Com}([A]_\beta) \geq \sum_{i=1}^r \dim \text{Com}(J_{s_i}) \geq s_1 + \dots + s_r = n$$

Soit $s \in \llbracket 1; n \rrbracket$. En posant $X = (1, 0, \dots, 0)^T \in \mathbb{K}^s$, on a

$$J_s^{s-1}X = (0, \dots, 0, 1)^T \neq 0$$

donc l'indice de nilpotence de J_s est égal à s , i.e. $\mu_{J_s}(X) = X^s$. En utilisant ce résultat, il est aisément de montrer que $\dim \mathbb{K}[J_s] = s$ ($(I, J_s, \dots, J_s^{s-1})$ est une base de cet espace). Enfin, puisque $\mathbb{K}[J_s] \subset \text{Com}(J_s)$, on a

$$\dim \text{Com}(J_s) \geq \dim \mathbb{K}[J_s] = s$$

d'où le résultat voulu.

Correction de l'exercice VII.5. :

1. Soit $u \in \mathcal{L}(E)$.

$\rightarrow (\Leftarrow)$ Supposons que u est cyclique. Il existe donc $x_0 \in E$ tel que $(x_0, u(x_0), \dots, u^{n-1}(x_0))$ est une base de E et alors $\deg \mu_u \geq n$ (car tout polynôme de degré inférieur ou égal à $n-1$ ne peut pas annuler u). De plus, $\mu_u | \chi_u$, $\deg \chi_u = n$ et les deux polynômes sont unitaires, ce qui nous permet d'affirmer que $\chi_u = \mu_u$.

$\rightarrow (\Rightarrow)$ Soit $x_0 \in E$ tel que $\mu_{x_0, u} = \mu_u$ (existe d'après l'énoncé). On a alors $\chi_u = \mu_u = \mu_{x_0, u}$, donc $\deg \mu_{x_0, u} = \deg \chi_u = n$. On a alors pour tout $\lambda_0, \dots, \lambda_{n-1} \in \mathbb{K}^n$,

$$\lambda_0 x_0 + \lambda_1 u(x_0) + \dots + \lambda_{n-1} u^{n-1}(x_0) = 0 \implies \lambda_0 = \dots = \lambda_{n-1} = 0$$

car sinon x_0 serait annulé en u par un polynôme de degré strictement inférieur à n . On en déduit donc que $(x_0, u(x_0), \dots, u^{n-1}(x_0))$ est une base de E , i.e. u est cyclique. On aurait aussi pu conclure en utilisant la proposition VII.4 (la remarque en dessous en particulier).

2. Supposons que $u \in \mathcal{L}(E)$ est cyclique. Montrons par double inclusion que $\text{Com}(u) = \mathbb{K}[u]$.

- (\supseteq) Cette inclusion est évidente car tout polynôme en u commute avec u .
 → (\subseteq) Soit $v \in \text{Com}(u)$ et x_0 tel que $\beta = (x_0, u(x_0), \dots, u^{n-1}(x_0))$ est une base de E . Ecrivons la décomposition de $v(x_0)$ dans la base β

$$v(x_0) = a_0 x_0 + a_1 u(x_1) + \cdots + a_{n-1} u^{n-1}(x_0)$$

et considérons l'application linéaire w définie par

$$w = v - \sum_{k=0}^{n-1} a_k u^k$$

w commute avec u et $w(x_0) = 0$. De plus, on a pour tout $k \in \llbracket 1; n-1 \rrbracket$,

$$w(u^k(x_0)) = w \circ u^k(x_0) = u^k(w(x_0)) = 0$$

w est nul sur la base β , donc $w = 0$ et donc $v \in \mathbb{K}[u]$ et alors $\text{Com}(u) = \mathbb{K}[u]$. De plus, $(\text{Id}, u, \dots, u^{n-1})$ est une base de $\mathbb{K}[u]$ (pour le montrer, il suffit d'effectuer la division euclidienne de tout polynôme de $\mathbb{K}[X]$ en u par μ_u) et donc

$$\dim \text{Com}(u) = \dim \mathbb{K}[u] = n$$

3. Déjà fait à l'exercice VI.15.

4. Soit $u \in \mathcal{L}(E)$. Procédons par double implication.

→ (\Rightarrow) Si $\chi_u = \mu_u$, alors d'après la question 1, u est cyclique et donc d'après la question 2, $\text{Com}(u) = \mathbb{K}[u]$.

→ (\Leftarrow) Si $\text{Com}(u) = \mathbb{K}[u]$, alors

$$\deg \mu_u = \dim \mathbb{K}[u] = \dim \text{Com}(u) \geq n$$

La dernière inégalité est vraie d'après la question précédente. On a de plus $\mu_u | \chi_u$ et ces deux polynômes sont unitaires de même degré, donc $\chi_u = \mu_u$.

Correction de l'exercice VII.6. :

L'énoncé est équivalent à

χ_u non irréductible \iff il existe un sous-espace vectoriel de E non trivial stable par u

→ (\Rightarrow) Supposons que χ_u n'est pas irréductible. Soit P un terme irréductible de la décomposition en facteurs irréductibles de χ_u tel que $\deg P \in \llbracket 1; n-1 \rrbracket$. D'après le corollaire V.8, on sait que $P | \mu_u$. Soit $x \in \text{Ker } P \setminus \{0\} \neq \emptyset$. $F_{x,u}$ est stable par u et

$$1 \leq \dim F_{x,u} = \deg \mu_{x,u} \stackrel{(*)}{\leq} \deg P \leq n-1$$

\uparrow
Proposition VII.2

L'inégalité (*) est vraie d'après la proposition VII.4. $F_{x,u}$ est donc un sous-espace vectoriel de E non trivial stable par u .

→ (\Leftarrow) Soit F un sous-espace vectoriel de E non trivial stable par u et posons $v = u|_F^F$. On a alors $\chi_v | \chi_u$ et $\deg \chi_v \in \llbracket 1; n-1 \rrbracket$.

Correction de l'exercice VII.7. :

1. Soit $A \in \mathcal{M}_n(\mathbb{C})$. Supposons que A est semblable à une matrice compagnon. Il existe donc une base β de \mathbb{K}^n et $a_0, \dots, a_{n-1} \in \mathbb{C}$ tels que

$$[A]_\beta = \begin{pmatrix} 0 & & -a_0 \\ 1 & \ddots & \vdots \\ \ddots & \ddots & \vdots \\ & 1 & -a_{n-1} \end{pmatrix}$$

On a alors pour tout $\lambda \in \mathbb{C}$,

$$[A - \lambda \text{Id}]_\beta = \begin{pmatrix} -\lambda & & -a_0 \\ 1 & \ddots & \vdots \\ \ddots & -\lambda & \vdots \\ & 1 & -a_{n-1} - \lambda \end{pmatrix}$$

Le sous bloc de $[A - \lambda \text{Id}]_\beta$ regroupant les colonnes de position 1 à $n-1$ est égal à

$$B = \begin{pmatrix} -\lambda & & 0 \\ 1 & \ddots & \\ \ddots & -\lambda & \\ & & 1 \end{pmatrix}$$

Les colonnes de B sont libres, donc $\text{rg}(A - \lambda \text{Id}) \geq n-1$, i.e. par la formule du rang $\dim \text{Ker}(A - \lambda \text{Id}) \leq 1$. En particulier, lorsque λ est une valeur propre de A , $\dim \text{Ker}(A - \lambda \text{Id}) = 1$.

2. Procédons par double implication. Soit $A \in \mathcal{M}_n(\mathbb{C})$ diagonalisable.

$\rightarrow (\Rightarrow)$ Si A est cyclique, alors A est semblable à une matrice compagnon et donc d'après la question précédente, tous les espaces propres de A sont de dimension 1, i.e. toutes les valeurs propres de A sont de multiplicité 1, il y en a donc n .

$\rightarrow (\Leftarrow)$ Supposons que A admet n valeurs propres deux à deux distinctes. Soit $\beta = (e_1, \dots, e_n)$ une base de diagonalisation de A . Il existe $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ deux à deux distincts tels que

$$[A]_\beta = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

Soit $x = e_1 + \dots + e_n$. On a pour tout $k \in \mathbb{N}$,

$$u^k(x) = \lambda_1^k e_1 + \dots + \lambda_n^k e_n$$

On a alors

$$[(x, u(x), \dots, u^{n-1}(x))]_\beta = \begin{pmatrix} 1 & \lambda_1 & \dots & \lambda_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_n & \dots & \lambda_n^{n-1} \end{pmatrix}$$

Cette matrice est une matrice de Vandermonde associée aux $\lambda_1, \dots, \lambda_n$ qui sont deux à deux distincts, elle est donc inversible. La famille $(x, u(x), \dots, u^{n-1}(x))$ est donc libre et alors c'est une base de \mathbb{K}^n . Finalement, A est cyclique i.e. semblable à une matrice compagnon.

Correction de l'exercice VII.8. :

1. Considérons $C_P \in M_n(\mathbb{Z})$ la matrice compagnon associée à P . On sait que

$$\text{Spec}_{\mathbb{C}}(C_P) = [\lambda_1, \dots, \lambda_n] \text{ et donc } \text{Spec}_{\mathbb{C}}(C_P^k) = [\lambda_1^k, \dots, \lambda_n^k]$$

$\lambda_1^k, \dots, \lambda_n^k$ sont exactement les racines (avec multiplicité) de $\chi_{C_P^k}$. De plus $C_P \in \mathcal{M}_n(\mathbb{Z})$, donc $C_P^k \in \mathcal{M}_n(\mathbb{Z})$ et alors $\chi_{C_P^k} \in \mathbb{Z}[X]$ car $k \geq 1$. On a alors $\chi_{C_P^k} \in \mathbb{Z}_n[X]$ et est unitaire. Le polynôme $\chi_{C_P^k}$ convient donc.

2. Supposons que $|\lambda_1| = \dots = |\lambda_n| = 1$ et posons pour tout $k \geq 1$,

$$P_k = \prod_1^n (X - \lambda_i^k) = X^n + \sum_{i=0}^{n-1} a_{k,i} X^k \in \mathbb{Z}[X]$$

(existe d'après la question précédente). On veut montrer que les coefficients des polynômes P_k sont uniformément bornés. Deux méthodes sont possibles.

→ **Méthode 1 (Topologie)** : On pour tout $k \in \mathbb{N}^*$,

$$\forall x \in [0, 1], |P_k(x)| = \prod_{i=1}^n |x - \lambda_i^k| \leq \prod_{i=1}^n (|x| + |\lambda_i|^k) \leq \prod_{i=1}^n (1 + 1) = 2^n$$

Considérons les deux normes suivantes sur $\mathbb{R}_n[X]$

$$\|\cdot\|_{\infty} : \begin{cases} \mathbb{R}_n[X] & \longrightarrow \mathbb{R}^+ \\ P & \longmapsto \sup_{x \in [0,1]} |P(x)| \end{cases}$$

ainsi que

$$\|\cdot\|_{\infty, \text{coef}} : \begin{cases} \mathbb{R}_n[X] & \longrightarrow \mathbb{R}^+ \\ P & \longmapsto \sup_{k \in \llbracket 0; n \rrbracket} |a_k| \text{ lorsque } P(X) = \sum_{k=0}^n a_k X^k \end{cases}$$

$\mathbb{R}_n[X]$ est de dimension finie, donc toutes les normes y sont équivalentes (voir chapitre sur l'équivalence des normes). Il existe donc une constante $C > 0$ telle que

$$\forall P \in \mathbb{R}_n[X], \|P\|_{\infty, \text{coef}} \leq C \|P\|_{\infty}$$

On a donc pour tout $k \in \mathbb{N}^*$

$$\|P_k\|_{\infty, \text{coef}} \leq C 2^n$$

→ **Méthode 2 (Vieta)** : On souhaite borner les coefficients de P_k en utilisant une majoration des racines de ce dernier, il est donc naturel de chercher à utiliser des relations coefficients racines. Introduisons donc le lemme assez connu suivant

Lemme (Formules de Vieta) VIII.11.

Soit $n \in \mathbb{N}^*$, $P(X) = a_0 + a_1 X + \dots + a_n X^n$ et $\lambda_1, \dots, \lambda_n$ les racines (non nécessairement différentes) de P . Supposons que $a_n \neq 0$. On a pour tout $l \in \llbracket 0; n \rrbracket$

$$\sum_{1 \leq i_1 < i_2 < \dots < i_l \leq n} \left(\prod_{j=1}^l \lambda_{i_j} \right) = (-1)^l \frac{a_{n-l}}{a_n}$$

Nous ne démontrerons pas ce lemme, mais nous encourageons le lecteur à aller regarder la

preuve de ce lemme qui peut être quelques fois assez utile. Appliquons ce lemme, on a pour tout $k \in \mathbb{N}$ et $l \in [\![1; n]\!]$

$$\begin{aligned} |a_{k,n-l}| &= \left| \sum_{1 \leq i_1 < i_2 < \dots < i_l \leq n} \left(\prod_{j=1}^l \lambda_{i_j} \right) \right| \\ &\leq \sum_{1 \leq i_1 < i_2 < \dots < i_l \leq n} \left| \prod_{j=1}^l \lambda_{i_j} \right| \\ &= \sum_{1 \leq i_1 < i_2 < \dots < i_l \leq n} 1 = \binom{n}{l} \end{aligned}$$

Ceci nous permet donc d'affirmer que pour tout $i \in [\![0; n]\!]$ les coefficients $|a_{k,i}|$ sont bornés par une constante indépendante de k .

On a donc pour tout $i \in [\![0; n-1]\!]$, l'ensemble $\{a_{k,i}, k \in \mathbb{N}^*\}$ est une partie bornée de \mathbb{Z} , elle est donc finie. L'ensemble $\{P_k, k \in \mathbb{N}\}$ est alors fini, ce qui implique que pour tout $i \in [\![1; n]\!]$, l'ensemble $\{\lambda_i^k, k \in \mathbb{N}\}$ est fini. On en déduit que pour tout $i \in [\![1; n]\!]$, il existe $k, l \in \mathbb{N}$ différents (on suppose sans perte de généralité que $k < l$) tels que $\lambda_i^k = \lambda_i^l$, i.e. $\lambda_i^{k-l} = 1$ et enfin pour tout $i \in [\![1; n]\!]$, λ_i est une racine de l'unité.

Correction de l'exercice VII.9. :

1. On a

$$\begin{aligned} \mu_y \cdot y = 0 &\iff \mu_y \cdot (Q \cdot x) = 0 \iff (\mu_y Q) \cdot x = 0 \\ &\iff \mu_x | \mu_y Q \iff PQ | \mu_y Q \iff P | \mu_y \end{aligned}$$

Mais $P \cdot y = 0$, donc $\mu_y | P$ et ces deux polynômes sont unitaires, donc $\mu_y = P$.

2. Il est clair que $\mu_x \mu_y \cdot (x + y) = 0$ donc $\mu_{x+y} | \mu_x \mu_y$. De plus, on a

$$\mu_{x+y} \cdot (x + y) = 0 \implies \mu_{x+y} \mu_x \cdot y = 0 \implies \mu_y | \mu_{x+y} \mu_x$$

Mais $\mu_y \wedge \mu_x = 1$, donc d'après Gauß, $\mu_y | \mu_{x+y}$. Par le même raisonnement, on peut montrer également que $\mu_x | \mu_{x+y}$. Encore une fois, puisque $\mu_y \wedge \mu_x = 1$, on a $\mu_x \mu_y | \mu_{x+y}$. On en déduit donc que $\mu_x \mu_y = \mu_{x+y}$. $\mu_x \mu_y$ et μ_{x+y} sont unitaires ce qui nous permet d'affirmer que $\mu_x \mu_y = \mu_{x+y}$.

3. Posons $\mu_x = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ et $\mu_y = P_1^{\beta_1} \dots P_r^{\beta_r}$. Posons également

$$\alpha'_i = \begin{cases} \alpha_i & \text{si } \alpha_i \geq \beta_i \\ 0 & \text{sinon} \end{cases} \quad \text{et} \quad \beta'_i = \begin{cases} \beta_i & \text{si } \beta_i > \alpha_i \\ 0 & \text{sinon} \end{cases}$$

$$P_x = P_1^{\alpha'_1} \dots P_r^{\alpha'_r} \text{ et } Q_y = P_1^{\beta'_1} \dots P_r^{\beta'_r}$$

Posons également $x' = \frac{\mu_x}{P_x} x$ et $y' = \frac{\mu_y}{Q_y} y$. D'après la question 1, on sait que $\mu_{x'} = P_x$ et $\mu_{y'} = Q_y$. De plus, on a $P_x \wedge Q_y = 1$, donc d'après la question précédente,

$$\mu_{x'+y'} = P_x Q_y = \mu_x \vee \mu_y$$

On en déduit donc que $z = x' + y'$ convient.

4. Soit (e_1, \dots, e_n) une base de E . Par une récurrence rapide, on sait qu'il existe d'après la question précédente $a \in E \setminus \{0\}$ tel que $\mu_a = \mu_{e_1} \vee \dots \vee \mu_{e_n}$. On a donc pour tout $x = x_1 e_1 + \dots + x_n e_n \in E \setminus \{0\}$,

$$\mu_a \cdot x = x_1 \mu_a \cdot e_1 + \dots + x_n \mu_a \cdot e_n = 0$$

Donc $\mu_x|\mu_a$. On en déduit que $\mu_a(u) = 0$ i.e. $\mu_u|\mu_a$ et de plus $\mu_u \cdot a = 0$ donc $\mu_a|\mu_u$ et ces deux polynômes sont unitaires, donc $\mu_a = \mu_u$.

Correction de l'exercice VIII.3. :

Soit $(A_p) \in \tilde{F}^{\mathbb{N}}$ telle que $A_p \xrightarrow[p \rightarrow +\infty]{} A$ et $z \in \mathbb{C} \setminus F$. Posons pour tout $p \in \mathbb{N}$, $\text{Spec}_{\mathbb{C}}(A_p) = [\lambda_{1,p}, \dots, \lambda_{n,p}]$.

On a

$$|\chi_{A_p}(z)| = \prod_{i=1}^n |z - \lambda_{i,p}| \geq d(z, F)^n > 0$$

En passant donc à la limite, on a par continuité

$$|\chi_A(z)| \geq d(z, F)^n > 0$$

et donc $z \notin \text{Spec}_{\mathbb{C}}(A)$, i.e. $\text{Spec}_{\mathbb{C}}(A) \subset F$. On a donc bien que $A \in \tilde{F}$, i.e. \tilde{F} est fermé.

Correction de l'exercice VIII.5. :

Soit $\varepsilon > 0$. D'après la proposition VIII.4, Il existe $P \in GL_n(\mathbb{C})$ tel que

$$A = P \underbrace{\begin{pmatrix} \lambda_1 & & b_{ij} \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}}_B P^{-1}$$

et $\forall i, j \in \llbracket 1; n \rrbracket$ tels que $j > i$, $|b_{i,j}| < \varepsilon$. Munissons \mathbb{C}^n de la norme $\|\cdot\|_1$, dont on rappelle la définition

$$\begin{aligned} \|\cdot\|_1 : \left\{ \begin{array}{ccc} \mathbb{C}^n & \longrightarrow & \mathbb{R}^+ \\ (x_1, \dots, x_n)^T & \longmapsto & |x_1| + \dots + |x_n| \end{array} \right. \end{aligned}$$

En posant (e_1, \dots, e_n) la base canonique de \mathbb{C}^n , on a pour tout $X = x_1e_1 + \dots + x_ne_n \in \mathbb{C}^n$,

$$\|BX\|_1 = \left\| \sum_{i=1}^n x_i Be_i \right\|_1 \leq \sum_{i=1}^n |x_i| \|Be_i\|_1 \leq C \|X\|_1$$

Avec $C = \sup_{i \in \llbracket 1; n \rrbracket} \|Be_i\|$. On a donc, en considérant $\|\cdot\|$ la norme d'opérateur associée à $\|\cdot\|_1$ que

$$\|B\| \leq C = \sup_{i \in \llbracket 1; n \rrbracket} \|Be_i\|_1 = \sup_{i \in \llbracket 1; n \rrbracket} \left| \lambda_i + \sum_{j=i+1}^n b_{ij} \right| \leq \sup_{i \in \llbracket 1; n \rrbracket} |\lambda_i| + (n-1)\varepsilon$$

On choisit donc ε tel que $\sup_{i \in \llbracket 1; n \rrbracket} |\lambda_i| + (n-1)\varepsilon < 1$. Ceci nous permet d'avoir $\|B\| < 1$ et donc

$$\begin{aligned} \||A^p|\| &= \||P B^p P^{-1}|\| \leq \||P|\| \times \||B^p|\| \times \||P^{-1}|\| \\ &\leq \||P|\| \times \||P^{-1}|\| \times \||B|\|^p \xrightarrow[p \rightarrow +\infty]{} 0 \end{aligned}$$

et donc finalement $A^p \xrightarrow[p \rightarrow +\infty]{} 0$.

Correction de l'exercice VIII.6. :

Munissons $\mathcal{M}_n(\mathbb{C})$ de la norme $\|\cdot\|$ définie par

$$\|\cdot\| : \begin{cases} \mathcal{M}_n(\mathbb{C}) & \longrightarrow \mathbb{R}^+ \\ (a_{i,j})_{i,j \in \llbracket 1;n \rrbracket} & \longmapsto \sup_{i,j \in \llbracket 1;n \rrbracket} |a_{i,j}| \end{cases}$$

Pour tout $p \in \mathbb{N}$, $A^p \in \mathcal{M}_n(\mathbb{Z})$, donc $\|A^p\| \in \mathbb{Z}$. De plus, $\text{Spec}_{\mathbb{C}}(A) \subset B(0, 1)$, donc d'après l'exercice précédent et par équivalence des normes en dimension finie, $A^p \xrightarrow[p \rightarrow +\infty]{} 0$. $(\|A\|^p)_{p \in \mathbb{N}}$ est une suite à valeurs dans \mathbb{Z} qui converge vers 0, elle est donc stationnaire en 0. On en déduit donc que il existe $r \in \mathbb{N}$ tel que pour tout $p \geq r$, $\|A\|^p = 0$ i.e. $A^p = 0$. A est alors bien nilpotente.

Correction de l'exercice VIII.8. :

Posons $S = \{P^{-1}AP, P \in GL_n(\mathbb{C})\}$

→ (\Leftarrow) Supposons que S soit fermé et montrons qu'il existe une matrice diagonale D dans S . D'après la proposition VIII.4, il existe $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ et une suite de matrices $(P_k)_{k \in \mathbb{N}} \in GL_n(\mathbb{C})^{\mathbb{N}}$ telle que pour tout $k \in \mathbb{N}$

$$P_k^{-1}AP_k = \begin{pmatrix} \lambda_1 & & b_{k,i,j} \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

et pour tout $j > i$, $|b_{k,i,j}| \leq \frac{1}{k+1}$. Cet argument nous permet d'affirmer que

$$P_k^{-1}AP_k \xrightarrow[p \rightarrow +\infty]{} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

S est fermé, donc cette matrice appartient à S . On en déduit donc que A est semblable à une matrice diagonale, i.e. A est diagonalisable.

→ (\Rightarrow) Supposons que A soit diagonalisable. Montrons que $\bar{S} = S$. Soit $B \in \bar{S}$. On veut montrer que $B \in S$. L'application

$$\phi : \begin{cases} \mathcal{M}_n(\mathbb{C}) & \longrightarrow \mathbb{C}_n[X] \\ M & \longmapsto \chi_M \end{cases}$$

est continue, car pour tout $M \in \mathcal{M}_n(\mathbb{C})$, les coefficients de $\phi(M)$ dans $\mathbb{C}_n[X]$ sont polynomiaux en les coefficients de M dans $\mathcal{M}_n(\mathbb{C})$. De plus, ϕ est constante sur S égale à χ_A , elle est donc constante aussi sur \bar{S} égale à χ_A par continuité. Ceci nous permet de dire que $\chi_A = \chi_B$ et que A et B ont les mêmes valeurs propres et même multiplicité.

$$\psi : \begin{cases} \mathcal{M}_n(\mathbb{C}) & \longrightarrow \mathcal{M}_n(\mathbb{C}) \\ M & \longmapsto \mu_A(M) \end{cases}$$

est continue car polynômiale et constante sur S égale à 0, donc par continuité elle est aussi égale à 0 sur l'adhérence de S et alors $\mu_A(B) = 0$. A est diagonalisable, donc μ_A est scindé à racines simples et alors B est diagonalisable. D'après ce qui précéde, A et B ont même valeurs propres et même multiplicités, donc A et B sont semblables diagonalisables et finalement $B \in S$.

Correction de l'exercice VIII.10. :

Le cas $A = 0$ est trivial. Supposons que $A \neq 0$. Soit $\lambda \in \mathbb{C}$ une valeur propre de A . Supposons que $|\lambda| = |||A|||$. Quitte à diviser les deux côtés de l'égalité par $|\lambda|$, on suppose que $|||A||| = 1 = |\lambda|$. On

a alors

$$\forall p \in \mathbb{N}^*, \ |||A^p||| \leq |||A|||^p = 1$$

Soit $F = \text{Ker}(A - \lambda I)^{\alpha_A(\lambda)}$. En posant $u : X \mapsto AX$ et $v = u|_F^F$, on sait que il existe N nilpotente telle que $v = \lambda I + N$. On veut montrer donc que $N = 0$.

Idée : On sait que pour tout $p \in \mathbb{N}^*$, $|||v^p||| \leq |||A^p||| \leq 1$, donc v^p est borné. On va donc montrer que si $N \neq 0$, alors v^p est non bornée.

Supposons que $N \neq 0$. Soit $m > 1$ l'indice de nilpotence de N . Il existe donc $X \in \mathbb{C}^n$ tel que $N^{m-1}X \neq 0$. Posons $Y = N^{m-2}X$. On a alors $NY \neq 0$ et $N^2Y = 0$. On a alors pour tout $p \in \mathbb{N}^*$

$$v^p Y = (\lambda I + N)^p Y = \sum_{k=0}^p \binom{p}{k} \lambda^k N^{p-k} Y = \lambda^p Y + p\lambda^{p-1} NY$$

Or $\lambda^p Y$ est borné ca $|\lambda| \leq 1$ et

$$\|p\lambda^{p-1} NY\| = p \|NY\| \xrightarrow[p \rightarrow +\infty]{} +\infty$$

donc v^p est non bornée, ce qui est absurde. On en déduit donc que $N = 0$ et alors $\text{Ker}(A - \lambda I)^{\alpha_A(\lambda)} = \text{Ker}(A - \lambda I)$ i.e. λ est pure.



CHAPITRE 30.1

Probabilités

Dans tout ce chapitre, E désigne un ensemble.

Préliminaires

- Soient P et Q deux assertions. Si $A = \{P\}$, $B = \{Q\}$, alors $A^c = \{\neg P\}$, $A \cap B = \{P \wedge Q\}$, et $A \cup B = \{P \vee Q\}$.
- Soit Ω un ensemble. Soit $(A_n) \in \mathcal{P}(\Omega)^{\mathbb{N}}$. Alors,

$$\bigcap_{N=0}^{+\infty} \left(\bigcup_{n=N}^{+\infty} A_n \right) = \{\omega \in \Omega \mid \forall N \in \mathbb{N}, \exists n \in \llbracket N, +\infty \rrbracket, \omega \in A_n\}$$

Si $\omega \in \Omega$, alors ω appartient cet ensemble si, et seulement si, ω appartient à une infinité de termes de la suite $(A_n)_{n \in \mathbb{N}}$.

I Tribus

On appelle tribu sur E toute partie \mathcal{T} de $\mathcal{P}(E)$ qui vérifie les propriétés suivantes :

- \emptyset et $E \in \mathcal{T}$.
- Si $(A_n) \in \mathcal{T}^{\mathbb{N}}$, $\bigcup_{n=0}^{+\infty} A_n \in \mathcal{T}$.
- Si $A \in \mathcal{T}$, $A^c \in \mathcal{T}$.

i Exemples : $\{\emptyset, E\}$ est une tribu sur E , et si E est dénombrable, $\mathcal{P}(E)$ est une tribu sur E .

Proposition I.1.

Soit \mathcal{T} une tribu sur E . Soit $(A_n) \in \mathcal{T}^{\mathbb{N}}$.

→ Pour tout $N \in \mathbb{N}$, $\bigcup_{n=0}^N A_n = \left(\bigcup_{n=0}^N A_n \right) \cup \emptyset \cup \emptyset \cup \dots \in \mathcal{T}$.

→ Pour tout $N \in \mathbb{N}$, $\bigcap_{n=0}^N A_n = \left(\bigcup_{n=0}^N A_n^c \right)^c \in \mathcal{T}$.

→ Il existe une suite $(B_n) \in \mathcal{T}^{\mathbb{N}}$ d'ensembles deux à deux disjoints telle que $\bigcup_{n=0}^{+\infty} A_n = \bigcup_{n=0}^{+\infty} B_n$,

et, pour tout $N \in \mathbb{N}$, $\bigcup_{n=0}^N A_n = \bigcup_{n=0}^N B_n$.

→ Si Λ est un ensemble non vide, et $(\mathcal{T}_\lambda)_{\lambda \in \Lambda}$ une famille de tribus sur E , alors $\bigcap_{\lambda \in \Lambda} \mathcal{T}_\lambda$ est aussi une tribu sur E .



Preuve de la troisième propriété : En posant, pour tout $n \in \mathbb{N}$, $B_n = A_n \setminus \left(\bigcup_{k=0}^{n-1} A_k \right)$, on construit bien une suite d'ensembles deux à deux disjoints qui vérifie les deux propriétés.

Tribu engendrée

Définition I.2.

Soit X une partie de $\mathcal{P}(E)$, et notons \mathcal{T}_X l'ensemble des tribus sur E contenant X . On appelle *tribu engendrée par X* , la tribu

$$\mathcal{T}(X) = \bigcap_{\mathcal{T} \in \mathcal{T}_X} \mathcal{T}$$

C'est la plus petite tribu sur E contenant X .

i Exemples

- On appelle tribu borélienne sur \mathbb{R} , et on note $\mathcal{B}(\mathbb{R})$, la tribu engendrée par l'ensemble des ouverts de \mathbb{R} . Par complémentarité, cette tribu contient également tous les fermés de \mathbb{R} . Donc cette tribu contient tous les points de \mathbb{R} , et par union dénombrable, $\mathbb{Q} \subset \mathcal{B}(\mathbb{R})$ puis, par complémentarité, $\mathbb{R} \setminus \mathbb{Q} \subset \mathcal{B}(\mathbb{R})$.
- Soit $n \in \mathbb{N}^*$. Soient A_1, \dots, A_n des parties de E incluant \emptyset et E . Posons

$$\mathcal{T}_a = \left\{ \bigcap_{k=1}^n B_k \mid \forall k \in \llbracket 1; n \rrbracket, B_k \in \{A_k, A_k^c\} \right\}$$

Les éléments de \mathcal{T}_a sont deux à deux disjoints et la tribu engendrée par $\{A_1, \dots, A_n\}$ est l'ensemble de réunions d'ensembles appartenant à \mathcal{T}_a .

- Soit $(A_n) \in \mathcal{P}(E)^{\mathbb{N}}$ une suite de parties de E deux à deux disjointes telle que $\bigcup_{n=0}^{+\infty} A_n = E$. La tribu engendrée par l'ensemble des termes de $(A_n)_{n \in \mathbb{N}}$ est $\mathcal{T} = \left\{ \bigcup_{n \in I} A_n \mid I \subset \mathbb{N} \right\}$.

En effet, $E = \bigcup_{n=0}^{+\infty} A_n \in \mathcal{T}$, $\emptyset = \bigcup_{n \in \emptyset} A_n \in \mathcal{T}$, et \mathcal{T} est stable par union dénombrable.

Enfin, si $I \subset \mathbb{N}$, $\left(\bigcup_{n \in I} A_n \right)^c = \bigcup_{n \in \mathbb{N} \setminus I} A_n \in \mathcal{T}$.

Notation : Soient A et B deux parties de E . Si l'union $A \cup B$ est disjointe, on la note $A \sqcup B$.

Proposition I.3.

Soit F un ensemble, et f une application de E dans F . Si \mathcal{T}' est une tribu sur F , l'ensemble des images réciproques des éléments de \mathcal{T}' par f , noté $f^{-1}\langle \mathcal{T}' \rangle$, est une tribu sur E , appelée tribu image réciproque de \mathcal{T}' sous f .

Si, de plus, on munit E d'une tribu \mathcal{T} sur E , et F de la tribu \mathcal{T}' , alors (E, \mathcal{T}) et (F, \mathcal{T}') sont qualifiés d'espaces mesurables, et $f : (E, \mathcal{T}) \rightarrow (F, \mathcal{T}')$ est dite mesurable lorsque $f^{-1}\langle \mathcal{T}' \rangle \subset \mathcal{T}$

II Espaces probabilisés

Dans la suite du chapitre, on munit E d'une tribu \mathcal{T} sur E si bien que (E, \mathcal{T}) est un espace mesurable, ou encore un espace probabilisable. Les éléments de \mathcal{T} sont appelés *événements*.

Définition II.1.

On dit qu'une application $\mathbb{P} : \mathcal{T} \rightarrow [0, 1]$ est une probabilité sur l'espace probabilisable (E, \mathcal{T}) lorsqu'elle vérifie les propriétés suivantes :

- $\mathbb{P}(\emptyset) = 0$ et $\mathbb{P}(E) = 1$.
- Si $(A_n) \in \mathcal{T}^{\mathbb{N}}$ est une suite d'événements deux à deux incompatibles *i.e.* une suite d'éléments de \mathcal{T} deux à deux disjoints, alors $\mathbb{P}\left(\bigcup_{n=0}^{+\infty} A_n\right) = \sum_{n=0}^{+\infty} \mathbb{P}(A_n)$.

Proposition II.2.

Soit \mathbb{P} une probabilité sur (E, \mathcal{T}) . Alors \mathbb{P} vérifie les propriétés suivantes :

- Soit $n \in \mathbb{N}$. Si A_0, \dots, A_n sont des événements deux à deux incompatibles, alors

$$\mathbb{P}\left(\bigcup_{k=0}^n A_k\right) = \sum_{k=0}^n \mathbb{P}(A_k)$$

- *Croissance* : Soient A et B deux événements. Si $A \subset B$, alors $\mathbb{P}(A) \leq \mathbb{P}(B)$.

- Soit $n \in \mathbb{N}^*$. Soient $A_1, \dots, A_n \in \mathcal{T}$. Alors

$$\mathbb{P}\left(\bigcup_{k=1}^n A_k\right) \leq \sum_{k=1}^n \mathbb{P}(A_k) \quad \text{et} \quad \mathbb{P}\left(\bigcup_{k=1}^n A_k\right) = \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq j_1 < \dots < j_k \leq n} \mathbb{P}\left(\bigcap_{\ell=1}^k A_{j_\ell}\right)$$

L'égalité se nomme *la formule de Poincaré*.

- *Continuité croissante* : Soit $(A_n)_{n \in \mathbb{N}}$ une suite croissante d'événements *i.e.* pour tout $n \in \mathbb{N}$, $A_n \subset A_{n+1}$. Alors

$$\mathbb{P}(A_n) \xrightarrow{n \rightarrow +\infty} \mathbb{P}\left(\bigcup_{k=0}^{+\infty} A_k\right)$$

- *Continuité décroissante* : Soit $(A_n)_{n \in \mathbb{N}}$ une suite décroissante d'événements *i.e.* pour tout $n \in \mathbb{N}$, $A_{n+1} \subset A_n$. Alors

$$\mathbb{P}(A_n) \xrightarrow{n \rightarrow +\infty} \mathbb{P}\left(\bigcap_{k=0}^{+\infty} A_k\right)$$

 **Preuve de la continuité décroissante à partir de la continuité croissante**
 $\left(\bigcup_{k=0}^n A_k^c\right)_{n \in \mathbb{N}}$ est croissante donc $\underbrace{\mathbb{P}\left(\bigcup_{k=0}^n A_k^c\right)}_{=1-\mathbb{P}\left(\bigcap_{k=0}^n A_k\right)} \xrightarrow{n \rightarrow +\infty} \mathbb{P}\left(\bigcup_{k=0}^{+\infty} A_k^c\right) = 1 - \mathbb{P}\left(\bigcap_{k=0}^{+\infty} A_k\right)$



Conséquence : Si $(A_n)_{n \in \mathbb{N}}$ est une suite d'événements telle que $\sum_{n \geq 0} \mathbb{P}(A_n)$ converge, alors

$$\mathbb{P}\left(\bigcup_{n=0}^{+\infty} A_n\right) \leq \sum_{n=0}^{+\infty} \mathbb{P}(A_n)$$

Preuve : $\left(\bigcup_{k=0}^n A_k\right)_{n \in \mathbb{N}}$ est une suite croissante d'événements donc par continuité croissante

$$\mathbb{P}\left(\bigcup_{k=0}^{+\infty} A_k\right) = \lim_{n \rightarrow +\infty} \mathbb{P}\left(\bigcup_{k=0}^n A_k\right) \leq \lim_{n \rightarrow +\infty} \sum_{k=0}^n \mathbb{P}(A_k) = \sum_{n=0}^{+\infty} \mathbb{P}(A_n)$$

III Événement presque sûr, événement négligeable

Dans la suite du chapitre, on munit l'espace probabilisable (E, \mathcal{T}) d'une probabilité \mathbb{P} sur (E, \mathcal{T}) , si bien que $(E, \mathcal{T}, \mathbb{P})$ est un espace probabilisé.

Définition III.1.

On dit qu'un événement A est presque sûr lorsque $\mathbb{P}(A) = 1$. On dit qu'un événement A est négligeable lorsque $\mathbb{P}(A) = 0$.

Proposition III.2.

→ Soient A et B sont deux événements tels que $A \subset B$. Si A est presque sûr, alors B est presque sûr.

→ Si $(A_n)_{n \in \mathbb{N}}$ est une suite d'événements négligeables, alors $\bigcup_{n=0}^{+\infty} A_n$ est négligeable.

Preuve

→ $1 = \mathbb{P}(A) \leq \mathbb{P}(B) \leq 1$, donc B est presque sûr.

→ La série $\sum_{n \geq 0} \mathbb{P}(A_n)$ converge car elle est nulle donc $0 \leq \mathbb{P}\left(\bigcup_{n=0}^{+\infty} A_n\right) \leq \sum_{n \geq 0} \mathbb{P}(A_n) = 0$, donc $\bigcup_{n=0}^{+\infty} A_n$ est négligeable.

Exercice III.3.

Soit $(E, \mathcal{T}, \mathbb{P})$ un espace probabilisé. Soit $(A_n)_{n \in \mathbb{N}}$ une suite d'événements telle que $\sum_{n \geq 0} \mathbb{P}(A_n)$ converge.

Que dire que l'événement $\bigcap_{N=0}^{+\infty} \left(\bigcup_{n=N}^{+\infty} A_n\right)$?

IV Exemples d'espaces probabilisés

1. Ensembles finis

Espace avec équiprobabilité : Si E est non vide et fini, $\mathcal{T} = \mathcal{P}(E)$, et pour tout $A \in \mathcal{T}$, $\mathbb{P}(A) = \frac{|A|}{|X|}$ alors $(E, \mathcal{T}, \mathbb{P})$ est un espace probabilisé.

Espace image d'une loi binomiale : Soient $n \in \mathbb{N}^*$ et $p \in]0, 1[$. Si $E = \llbracket 0; n \rrbracket$, $\mathcal{T} = \mathcal{P}(E)$, et pour tout $k \in E$, $\mathbb{P}(\{k\}) = \binom{n}{k} p^k (1-p)^{n-k}$, alors $(E, \mathcal{T}, \mathbb{P})$ est un espace probabilisé.

2. Ensembles dénombrables

Supposons dans cette partie que E soit dénombrable. Soit $(x_n) \in E^{\mathbb{N}}$ une énumération bijective de E .

Soit $(a_n) \in \ell^1(\mathbb{N}, \mathbb{R}^+)$ telle que $\sum_{n=0}^{+\infty} a_n = 1$.

Posons $\mathcal{T} = \mathcal{P}(E)$. Pour tout $A \in \mathcal{T}$, posons $I_A = \{n \in \mathbb{N} \mid x_n \in A\}$, puis $\mathbb{P}(A) = \sum_{n \in I_A} a_n$.

On a bien $\mathbb{P}(\emptyset) = 0$, $\mathbb{P}(E) = 1$, et si (A_n) est une suite d'événements deux à deux incompatibles, alors

$$\mathbb{P}\left(\underbrace{\bigcup_{n=0}^{+\infty} A_n}_{\text{noté } A}\right) = \sum_{k \in I_A} a_k = \sum_{n=0}^{+\infty} \left(\sum_{k \in I_{A_n}} a_k \right) = \sum_{n=0}^{+\infty} \mathbb{P}(A_n)$$

Donc $(E, \mathcal{T}, \mathbb{P})$ est un espace probabilisé.

Exemples

- Soit $a > 1$. Si $E = \mathbb{N}^*$, $\mathcal{T} = \mathcal{P}(E)$ et, pour tout $n \in \mathbb{N}^*$, $\mathbb{P}(\{n\}) = \frac{1}{\zeta(a)n^a}$, alors $(E, \mathcal{T}, \mathbb{P})$ est un espace probabilisé. C'est l'univers image d'une loi ζ de paramètre a .
- Soit $p \in]0, 1[$. Si $E = \mathbb{N}^*$, $\mathcal{T} = \mathcal{P}(E)$ et, pour tout $n \in \mathbb{N}^*$, $\mathbb{P}(\{n\}) = (1-p)^{n-1}p$, alors $(E, \mathcal{T}, \mathbb{P})$ est un espace probabilisé. C'est l'univers image d'une loi géométrique de paramètre p .
- Soit $\lambda > 0$. Si $E = \mathbb{N}$, $\mathcal{T} = \mathcal{P}(E)$ et, pour tout $n \in \mathbb{N}$, $\mathbb{P}(\{n\}) = \frac{\lambda^n e^{-\lambda}}{n!}$, alors $(E, \mathcal{T}, \mathbb{P})$ est un espace probabilisé. C'est l'univers image d'une loi de Poisson de paramètre λ .
- Soit F un ensemble dénombrable et $(y_n)_{n \in \mathbb{N}}$ une énumération bijective de F . Soit $(b_n) \in \ell^1(\mathbb{N}, \mathbb{R}^+)$ tel que $\sum_{n=0}^{+\infty} b_n = 1$. Alors en posant, pour tout $n \in \mathbb{N}$, $\mathbb{P}(\{y_n\}) = b_n$, on définit bien une probabilité. On définit la probabilité produit \mathbb{P}_\times sur l'espace probabilisable $(E \times F, \mathcal{P}(E \times F))$ par

$$\forall (n, m) \in \mathbb{N}^2, \quad \mathbb{P}_\times(\{x_n, y_m\}) = a_n b_m$$

$$\text{On vérifie que } \mathbb{P}_\times(E \times F) = \sum_{(n,m) \in \mathbb{N}^2} a_n b_m = \left(\sum_{n=0}^{+\infty} a_n \right) \left(\sum_{m=0}^{+\infty} b_m \right) = 1.$$

Correction de l'exercice 8. :

Pour tout $M \in \mathbb{N}$,

$$\mathbb{P} \left(\bigcap_{N=0}^{+\infty} \left(\bigcup_{n \geq N} A_n \right) \right) \leq \mathbb{P} \left(\bigcup_{n \geq M} A_n \right) \leq \sum_{n=M}^{+\infty} \mathbb{P}(A_n) \xrightarrow[M \rightarrow +\infty]{} 0$$

↑
croissance de la probabilité

donc $\bigcap_{N=0}^{+\infty} \left(\bigcup_{n \geq N} A_n \right)$ est négligeable.



CHAPITRE 30.2

Indépendance, conditionnement

Dans tout ce chapitre, $(E, \mathcal{T}, \mathbb{P})$ désigne un espace probabilisé.

I Événements indépendants

Définition I.1.

Deux événements A et B sont indépendants lorsque $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$.

Si $A \cap B = \emptyset$, alors A et B sont indépendants si, et seulement si, A est négligeable ou B est négligeable.

Exemples

- Un événement négligeable est indépendant de tout autre.
- Un événement presque sûr est indépendant de tout autre. En effet, si A est presque sûr, et si B est un événement quelconque, alors $B = (A \cap B) \sqcup (\underbrace{A^c \cap B}_{\subset A^c \text{ qui est négligeable}})$, donc $\mathbb{P}(A)\mathbb{P}(B) = \mathbb{P}(B) = \mathbb{P}(A \cap B)$.

Proposition I.2.

Si A et B sont deux événements indépendants, alors A^c et B sont indépendants.

Preuve : $\mathbb{P}(B) = \mathbb{P}(A^c \cap B) + \mathbb{P}(A \cap B) = \mathbb{P}(A^c \cap B) + \mathbb{P}(A)\mathbb{P}(B)$. Donc $\mathbb{P}(A^c \cap B) = \mathbb{P}(B)(\underbrace{1 - \mathbb{P}(A)}_{=\mathbb{P}(A^c)})$.

Conséquence : Dans ce cas, B^c et A sont indépendants, ainsi que A^c et B^c .

Définition I.3.

Soit n un entier supérieur ou égal à 3. Des événements A_1, \dots, A_n sont dits mutuellement indépendants lorsque pour tout $I \subset \llbracket 1; n \rrbracket$, $\mathbb{P}\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} \mathbb{P}(A_i)$.

Proposition I.4.

Soit n un entier supérieur ou égal à 3. Soient A_1, \dots, A_n des événements mutuellement indépendants.

- Si I et $J \subset \llbracket 1; n \rrbracket$ et $I \cap J = \emptyset$, alors $\bigcap_{i \in I} A_i$ et $\bigcap_{j \in J} A_j$ sont indépendants.
- A_1^c, A_2, \dots, A_n sont mutuellement indépendants.

 **Conséquence :** Les événements de la tribu engendrée par $\{A_1, \dots, A_n\}$ sont mutuellement indépendants.

Exercice I.5.

Soit $(E, \mathcal{T}, \mathbb{P})$ un espace probabilisé. Soit n un entier supérieur ou égal à 3. Soient A_1, \dots, A_n des événements mutuellement indépendants. Montrer que la probabilité qu'aucun d'eux ne se réalise est majorée par $\exp\left(-\sum_{i=1}^n \mathbb{P}(A_i)\right)$.

II Conditionnement

Loi conditionnelle

Soit A un événement tel que $\mathbb{P}(A) \neq 0$.

Pour tout $B \in \mathcal{T}$, posons $\mathbb{P}(B | A) = \frac{\mathbb{P}(B \cap A)}{\mathbb{P}(A)}$. Alors $\mathbb{P}(\cdot | A)$ est une probabilité sur (E, \mathcal{T}) . Elle vérifie les propriétés suivantes :

- $\mathbb{P}(A \cap B) = \mathbb{P}(B | A)\mathbb{P}(A)$.
 - Si A et B sont deux événements indépendants (au sens de \mathbb{P}), alors $\mathbb{P}(B | A) = \mathbb{P}(B)$.
 - Si n est un entier supérieur ou égal à 3, et A_1, \dots, A_n sont des événements tels que, pour tout $i \in \llbracket 1; n-1 \rrbracket$, $\mathbb{P}\left(\bigcap_{k=1}^i A_k\right) > 0$, alors,
- $$\heartsuit \quad \mathbb{P}\left(\bigcap_{i=1}^n A_i\right) = \mathbb{P}(A_1)\mathbb{P}(A_2 | A_1)\mathbb{P}(A_3 | A_1 \cap A_2) \dots \mathbb{P}(A_n | A_1 \cap A_2 \cap \dots \cap A_{n-1})$$
- Si $(A_n)_{n \in \mathbb{N}}$ est une partition de E telle que pour tout $n \in \mathbb{N}$, $\mathbb{P}(A_n) > 0$, alors pour tout événement B non négligeable, on a

$$\mathbb{P}(B) = \sum_{n=0}^{+\infty} \mathbb{P}(B | A_n)\mathbb{P}(A_n) \quad \text{et} \quad \mathbb{P}(A_n | B) = \frac{\mathbb{P}(B | A_n)\mathbb{P}(A_n)}{\sum_{n=0}^{+\infty} \mathbb{P}(B | A_n)\mathbb{P}(A_n)}$$

III Tribus indépendantes

Définition III.1.

Soit I un ensemble contenant au moins deux éléments.

Une famille $(\mathcal{T}_i)_{i \in I}$ de tribus sur E est dite indépendante lorsque, pour tout ensemble fini $J \subset I$, toute famille $(A_j)_{j \in J} \in \prod_{j \in J} \mathcal{T}_j$ est une famille d'événements mutuellement indépendants.

Indépendance de tribus engendrées par des partitions indépendantes

Soient $(A_n)_{n \in \mathbb{N}}$ et $(B_n)_{n \in \mathbb{N}}$ deux partitions de E telles que, pour tout $(n, p) \in \mathbb{N}^2$, A_n et B_p soient indépendants. Les tribus engendrées par ces partitions, $\mathcal{T}_A = \left\{ \bigcup_{n \in I} A_n \mid I \in \mathcal{P}(\mathbb{N}) \right\}$ et $\mathcal{T}_B = \left\{ \bigcup_{n \in I} B_n \mid I \in \mathcal{P}(\mathbb{N}) \right\}$, sont indépendantes.

En effet, pour tous I et $J \in \mathcal{P}(\mathbb{N})$, en utilisant le théorème d'associativité pour les familles sommables,

$$\mathbb{P}\left(\left(\bigcup_{n \in I} A_n\right) \cap \left(\bigcup_{p \in J} B_p\right)\right) = \mathbb{P}\left(\bigsqcup_{(n,p) \in I \times J} (A_n \cap B_p)\right) = \sum_{(n,p) \in I \times J} \underbrace{\mathbb{P}(A_n \cap B_p)}_{\mathbb{P}(A_n)\mathbb{P}(B_p)} = \mathbb{P}\left(\bigcup_{n \in I} A_n\right) \mathbb{P}\left(\bigcup_{n \in J} B_p\right)$$

IV Borel-Cantelli

Théorème IV.1.

Soit $(A_n)_{n \in \mathbb{N}}$ une suite d'événements mutuellement indépendants telle que $\sum_{n \geq 0} \mathbb{P}(A_n)$ diverge.

Alors,

$$\mathbb{P}\left(\bigcap_{N=0}^{+\infty} \left(\bigcup_{n=N}^{+\infty} A_n\right)\right) = 1$$

 **Vocabulaire :** Si $\omega \in E$ réalise $\bigcap_{N=0}^{+\infty} \left(\bigcup_{n=N}^{+\infty} A_n\right)$ i.e. ω appartient à cet ensemble, alors ω réalise une infinité d'événements de la suite $(A_n)_{n \in \mathbb{N}}$. La conclusion de ce théorème assure alors que, presque sûrement, une infinité d'événements de $(A_n)_{n \in \mathbb{N}}$ sont réalisés, ou alors que A_n est réalisé infiniment souvent.

 **Preuve :** Posons, pour tout $N \in \mathbb{N}$, $B_N = \bigcup_{n=N}^{+\infty} A_n$. Alors pour tout $N \in \mathbb{N}$, $B_N^c = \bigcap_{n=N}^{+\infty} A_n^c$ et en introduisant la suite décroissante d'événements $(C_M^N)_{M \in \mathbb{N}} = \left(\bigcap_{n=N}^M A_n^c\right)_{M \in \mathbb{N}}$, on a, par continuité décroissante

$$\mathbb{P}(C_M^N) \xrightarrow[M \rightarrow +\infty]{} \mathbb{P}(B_N^c)$$

D'après l'exercice, par indépendance, pour tout $N \in \mathbb{N}$ et pour tout entier $M \geq N$,

$$\mathbb{P}(C_M^N) \leq \exp\left(-\sum_{n=N}^M \underbrace{\mathbb{P}(A_n)}_{=\mathbb{P}(A_n^c)^c}\right)$$

donc en passant à la limite $M \rightarrow +\infty$, il vient $\mathbb{P}(B_N^c) = 0$.

Donc $\mathbb{P}\left(\bigcup_{N=0}^{+\infty} B_N^c\right) = 0$ car $\mathbb{P}\left(\bigcup_{N=0}^{+\infty} B_N^c\right) \leq \underbrace{\sum_{N=0}^{+\infty} \mathbb{P}(B_N^c)}_{\text{somme d'une série convergente}}$. En passant au complémentaire, on obtient la

conclusion du théorème.

Théorème IV.2.

Soit $(A_n)_{n \in \mathbb{N}}$ une suite d'événements telle que $\sum_{n \geq 0} \mathbb{P}(A_n)$ converge. Alors,

$$\mathbb{P}\left(\bigcap_{N=0}^{+\infty} \left(\bigcup_{n=N}^{+\infty} A_n\right)\right) = 0$$

 **Preuve :** En reprenant les notations de la preuve précédente, $(B_N)_{N \in \mathbb{N}}$ est une suite décroissante

d'événements, donc par continuité décroissante

$$\mathbb{P}(B_N) \xrightarrow[N \rightarrow +\infty]{} \mathbb{P}\left(\bigcap_{N=0}^{+\infty} B_N\right)$$

Par ailleurs, pour tout $N \in \mathbb{N}$, $\mathbb{P}(B_N) \leq \sum_{n=N}^{+\infty} \mathbb{P}(A_n) \xrightarrow[N \rightarrow +\infty]{} 0$ donc par unicité de la limite, $\mathbb{P}\left(\bigcap_{N=0}^{+\infty} B_N\right) = 0$, ce qu'on voulait.

Correction de l'exercice 5. :

Par indépendance mutuelle,

$$\mathbb{P}\left(\bigcap_{i=1}^n A_i^c\right) = \prod_{i=1}^n (1 - \mathbb{P}(A_i)) \leq \prod_{i=1}^n e^{-\mathbb{P}(A_i)} = \exp\left(-\sum_{i=1}^n \mathbb{P}(A_i)\right)$$



Il est loisible de retenir que pour tout $x \in \mathbb{R}$, $e^x \geq 1 + x$.



CHAPITRE 30.3

Variables aléatoires

Dans tout ce chapitre, $(\Omega, \mathcal{T}, \mathbb{P})$ désigne un espace probabilisé, et (E, \mathcal{U}) un espace probabilisable.

I Généralités

Une variable aléatoire à valeurs dans E est une application $X : (\Omega, \mathcal{T}, \mathbb{P}) \rightarrow (E, \mathcal{U})$ telle que pour tout $U \in \mathcal{U}$, $X^{-1}(U) \in \mathcal{T}$. Autrement dit, $X : (\Omega, \mathcal{T}) \rightarrow (E, \mathcal{U})$ est une fonction mesurable.

Loi de probabilité : La loi de X , notée \mathcal{L}_X , est une application de \mathcal{U} dans $[0, 1]$ définie par

$$\forall U \in \mathcal{U}, \quad \mathcal{L}_X(U) = \mathbb{P}(X^{-1}(U))$$

Ainsi, $\mathcal{L}_X(E) = \mathbb{P}(\Omega) = 1$, $\mathcal{L}_X(\emptyset) = \mathbb{P}(\emptyset) = 0$ et, pour toute suite $(U_n) \in \mathcal{U}^{\mathbb{N}}$ d'événements deux à deux disjoints,

$$\mathcal{L}_X\left(\bigcup_{n=0}^{+\infty} U_n\right) = \mathbb{P}\left(\bigsqcup_{n=0}^{+\infty} X^{-1}(U_n)\right) = \sum_{n=0}^{+\infty} \mathbb{P}(X^{-1}(U_n)) = \sum_{n=0}^{+\infty} \mathcal{L}_X(U_n)$$

💡 Notons que sur tout espace probabilisable, on peut définir une loi de probabilité \mathcal{L} sans se donner de variable aléatoire.

II Variables discrètes

Définition II.1.

On dit qu'une variable aléatoire $X : (\Omega, \mathcal{T}, \mathbb{P}) \rightarrow (E, \mathcal{U})$ est discrète lorsque $X(\Omega)$ est dénombrable.

Notation II.2.

Soit $d \in \mathbb{N}^*$. Soit $X : (\Omega, \mathcal{T}, \mathbb{P}) \rightarrow (E, \mathcal{U})$ une variable aléatoire. Soient $x, y \in E$.

- L'événement $X^{-1}(\{x\})$ est noté $[X = x]$.
- Pour tout $A \in \mathcal{U}$, l'événement $X^{-1}(A)$ est noté $[X \in A]$.
- Si $(E, \mathcal{U}) = (\mathbb{R}, \mathcal{B}(\mathbb{R}))$, l'événement $X^{-1}(]-\infty, x])$ (respectivement $X^{-1}(]-\infty, x[)$) est noté $[X \leq x]$ (respectivement $[X < x]$).
- Si $(E, \mathcal{U}) = (\mathbb{R}, \mathcal{B}(\mathbb{R}))$, l'événement $X^{-1}([x, +\infty[)$ (respectivement $X^{-1}([x, +\infty[)$) est noté $[X \geq x]$ (respectivement $[X > x]$)).
- Si $(E, \mathcal{U}) = (\mathbb{R}, \mathcal{B}(\mathbb{R}))$, et $x \leq y$, l'événement $X^{-1}([x, y])$ est noté $[x \leq X \leq y]$, et on note de manière analogue les événements $X^{-1}(]x, y])$, $X^{-1}([x, y[)$, et $X^{-1}(]x, y[)$.

Proposition II.3.

Soit $d \in \mathbb{N}^*$. Soit $\lambda \in \mathbb{R}$. Si X et Y sont des variables aléatoires discrètes définies sur $(\Omega, \mathcal{T}, \mathbb{P})$ et à valeurs dans $(\mathbb{R}^d, \mathcal{B}(\mathbb{R}^d))$, alors $X + Y$ et λX sont des variables aléatoires discrètes.

🔍 Preuve : L'application

$$\begin{aligned} X(\Omega) \times Y(\Omega) &\longrightarrow \mathbb{R}^d \\ (x, y) &\longmapsto x + y \end{aligned}$$

a pour image une partie dénombrable de \mathbb{R}^d contenant $(X + Y)(\Omega)$.

De plus, pour tout $z \in \mathbb{R}^d$, $(X + Y)^{-1}(z) = \bigcup_{\substack{(x,y) \in X(\Omega) \times Y(\Omega) \\ x+y=z}} ([X = x] \cap [Y = y]) \in \mathcal{T}$ en tant qu'union dénombrable d'événements.

Remarque II.4.

L'union étant disjointe, la loi de $X + Y$ est donnée par

$$\forall z \in (X + Y)(\Omega), \quad \mathcal{L}_{X+Y}(z) = \sum_{\substack{(x,y) \in X(\Omega) \times Y(\Omega) \\ x+y=z}} \mathbb{P}([X = x] \cap [Y = y])$$

III Variables aléatoires discrètes indépendantes

Dans la suite, on considère que les variables aléatoires sont définies sur $(\Omega, \mathcal{T}, \mathbb{P})$ et à valeurs dans (E, \mathcal{U}) .

Définition III.1.

Soit $n \in \mathbb{N}^*$. Soient X_1, \dots, X_n des variables aléatoires.

On dit que X_1, \dots, X_n sont indépendantes lorsque, pour tous $A_1, \dots, A_n \in \mathcal{U}$, les événements $[X_1 \in A_1], \dots, [X_n \in A_n]$ sont mutuellement indépendants.

Suites : On dit que $(X_n)_{n \in \mathbb{N}}$ est une suite de variables aléatoires indépendantes lorsque pour toute partie finie I de \mathbb{N} , les variables aléatoires de $(X_i)_{i \in I}$ sont indépendantes.

Remarque III.2.

Soit $n \in \mathbb{N}^*$. Soient X_1, \dots, X_n des variables aléatoires. Alors X_1, \dots, X_n sont indépendantes si, et seulement si, les tribus images réciproques $X_1^{-1}\langle \mathcal{U} \rangle, \dots, X_n^{-1}\langle \mathcal{U} \rangle$ sont indépendantes.

Proposition III.3.

Soient $n, d \in \mathbb{N}^*$. On suppose que $(E, \mathcal{U}) = (\mathbb{R}^d, \mathcal{B}(\mathbb{R}^d))$. Soient X_1, \dots, X_n des variables aléatoires discrètes. Alors :

- X_1, \dots, X_n sont indépendantes si, et seulement si, pour tout $(x_1, \dots, x_n) \in E^n$, les événements $[X_1 = x_1], \dots, [X_n = x_n]$ sont mutuellement indépendants.
- *Lemme des coalitions* : Soient $p, q \in \mathbb{N}$ tels que $p + q = n$. Soient $f : (\mathbb{R}^d)^p \longrightarrow \mathbb{R}^d$ et $g : (\mathbb{R}^d)^q \longrightarrow \mathbb{R}^d$ deux fonctions.
Si X_1, \dots, X_n sont indépendantes alors, $f(X_1, \dots, X_p)$ est une variable aléatoire indépendante de $g(X_{p+1}, \dots, X_n)$.

Exemples : $X_1 + \dots + X_p$ et $X_{p+1} + \dots + X_n$ sont indépendantes.

Pour tout $i \in \mathbb{N}$ tel que $1 \leq i < i + 3 \leq n$, $X_i X_{i+1}$ et $X_{i+2} X_{i+3}$ sont indépendantes.

○ Preuve des propositions :

→ (\Leftarrow) Soient $A_1, \dots, A_n \subset E$. En utilisant le théorème d'associativité pour les familles sommables,

$$\begin{aligned}\mathbb{P}([X_1 \in A_1] \cap \dots \cap [X_n \in A_n]) &= \sum_{(x_1, \dots, x_n) \in A_1 \times \dots \times A_n} \mathbb{P}([X_1 = x_1] \cap \dots \cap [X_n = x_n]) \\ &= \sum_{(x_1, \dots, x_n) \in A_1 \times \dots \times A_n} \mathbb{P}(X_1 = x_1) \dots \mathbb{P}(X_n = x_n) \\ &= \mathbb{P}(X_1 \in A_1) \times \dots \times \mathbb{P}(X_n \in A_n)\end{aligned}$$

→ Soient $x, y \in \mathbb{R}^d$. Par indépendance des variables X_1, \dots, X_n ,

$$\begin{aligned}\mathbb{P}([f(X_1, \dots, X_p) = x] \cap g(X_{p+1}, \dots, X_n) = y) &= \sum_{\substack{(x_1, \dots, x_n) \in E^n \\ f(x_1, \dots, x_p) = x \\ g(x_{p+1}, \dots, x_n) = y}} \mathbb{P}([X_1 = x_1] \cap \dots \cap [X_n = x_n]) \\ &= \sum_{\substack{(x_1, \dots, x_n) \in E^n \\ f(x_1, \dots, x_p) = x \\ g(x_{p+1}, \dots, x_n) = y}} \mathbb{P}([X_1 = x_1]) \dots \mathbb{P}([X_n = x_n]) \\ &= \sum_{\substack{(x_1, \dots, x_p) \in E^p \\ f(x_1, \dots, x_p) = x}} \mathbb{P}([X_1 = x_1]) \dots \mathbb{P}([X_p = x_p]) \mathbb{P}(g(X_{p+1}, \dots, X_n) = y) \\ &= \mathbb{P}(f(X_1, \dots, X_p) = x) \mathbb{P}(g(X_{p+1}, \dots, X_n) = y)\end{aligned}$$

Exercice III.4.

Soit $(\Omega, \mathcal{T}, \mathbb{P})$ un espace probabilisé. Soit $X : (\Omega, \mathcal{T}, \mathbb{P}) \rightarrow (\mathbb{R}, \mathcal{B}(\mathbb{R}))$ une variable aléatoire discrète. Donner une condition nécessaire et suffisante pour que X soit indépendante d'elle-même.

Exercice III.5.

Soit $(\Omega, \mathcal{T}, \mathbb{P})$ un espace probabilisé. Soient X, Y deux variables aléatoires de $(\Omega, \mathcal{T}, \mathbb{P})$ à valeurs dans $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$, indépendantes, et telles que, pour tout $i \in \mathbb{N}^*$, $\mathbb{P}(X = i) = \mathbb{P}(Y = i) = \frac{1}{2^i}$.

1. Calculer $\mathbb{P}(X = Y)$.
2. Calculer $\mathbb{P}(X > Y)$.
3. Soit $N \in \mathbb{N}^*$. Calculer $\mathbb{P}(\min(X, Y) \leq N)$.

IV Lois usuelles

Dans cette partie, toutes les variables aléatoires sont discrètes.

Schéma de Bernoulli¹ : Soit $p \in]0, 1[$. Un schéma de Bernoulli est une suite finie d'expériences identiques, deux à deux indépendantes et ayant, chacune, exactement deux issues possibles : un succès ou un échec. La probabilité qu'une expérience soit un succès vaut p .

Cette suite d'expériences est modélisée par les termes d'une suite $(X_n)_{n \in \mathbb{N}}$ de variables aléatoires indépendantes, à valeurs dans $\{0, 1\}$, et suivant la même loi de Bernoulli $\mathcal{B}(p)$ i.e. pour tout $k \in \mathbb{N}$, $\mathbb{P}(X_k = 1) = p$.

Loi binomiale : Soient $n \in \mathbb{N}$, et $p \in]0, 1[$. Considérons un schéma de Bernoulli d'ordre n (i.e. où n expériences sont menées) où la probabilité de succès vaut p . Le nombre de succès est aléatoire et est compris entre 0 et n , et la probabilité que k succès aient lieu vaut la probabilité que l'une des situations où $k \in \llbracket 0; n \rrbracket$ succès sont disséminés parmi les n expériences ait lieu : l'une de ces situations a une probabilité $p^k(1-p)^{n-k}$ d'avoir lieu (par indépendance), et il y a $\binom{n}{k}$ combinaisons de k succès parmi n expériences à deux issues.

La variable aléatoire $S = \sum_{k=1}^n X_k$ qui compte le nombre de succès d'un schéma de Bernoulli d'ordre n et de probabilité de succès p est à valeurs dans $\llbracket 0; n \rrbracket$ et suit la loi binomiale $\mathcal{B}(n, p)$:

$$\forall k \in \llbracket 0; n \rrbracket, \quad \mathbb{P}(S = k) = \binom{n}{k} p^k (1-p)^{n-k}$$

Loi de Rademacher : Il est possible de modéliser un schéma de Bernoulli d'ordre $n \in \mathbb{N}$ et de probabilité de succès $p \in]0, 1[$ par les termes d'une suite $(Y_n)_{n \geq 0}$ de variables aléatoires à valeurs dans $\{-1, 1\}$ indépendantes et identiquement distribuées suivant la loi de Rademacher i.e. pour tout $k \in \mathbb{N}$, $\mathbb{P}(Y_k = 1) = p$.

Dans un tel contexte, il est loisible de se ramener à la suite $(X_n)_{n \in \mathbb{N}}$ de variables de Bernoulli correspondante en remarquant que, presque sûrement,

$$\forall k \in \mathbb{N}, \quad Y_k = 2X_k - 1$$

Loi géométrique : Considérons un schéma de Bernoulli infini i.e. où l'on réalise une infinité dénombrable d'expériences identiques et indépendantes, et où la probabilité de succès vaut $p \in]0, 1[$.

Le temps d'attente du premier succès est une variable aléatoire T à valeurs dans \mathbb{N}^* suivant une loi géométrique $\mathcal{G}(p)$.

Soit $n \in \mathbb{N}^*$. Pour que le premier succès ait lieu à la n -ième expérience, il faut et il suffit que les expériences antérieures se soldent toutes par des échecs et que la n -ième soit un succès, c'est-à-dire que

$$\mathbb{P}(T = n) = (1-p)^{n-1}p$$

Théorème IV.1.

Soit $p \in]0, 1[$. Soit $(X_n)_{n \in \mathbb{N}}$ une suite de variables aléatoires indépendantes et identiquement distribuées suivant la loi de Bernoulli $\mathcal{B}(p)$. Alors

- Presque sûrement, il existe $k \in \mathbb{N}^*$ tel que $X_k = 1$.
- $Y = \min\{k \in \mathbb{N}^* \mid X_k = 1\}$ est une variable aléatoire à valeurs dans \mathbb{N}^* suivant la loi géométrique $\mathcal{G}(p)$.

Preuve :

- La suite d'événements $\left(\bigcap_{k=1}^n [X_k = 0] \right)_{n \in \mathbb{N}^*}$ est décroissante, donc par continuité décroissante et uni-

1. Rappelons que Jacques Bernoulli n'est pas une nouille.

cité de la limite :

$$\underbrace{\mathbb{P}\left(\bigcap_{k=1}^n [X_k = 0]\right)}_{=(1-p)^n} \xrightarrow{n \rightarrow +\infty} \mathbb{P}(\neg[\exists k \in \mathbb{N}^*, X_k = 1]) = 0$$

→ Soit $n \in \mathbb{N}^*$. $[Y = n] = [X_0 = 0] \cap \dots \cap [X_{n-1} = 0] \cap [X_n = 1] \in \mathcal{T}$, donc Y est mesurable, c'est donc une variable aléatoire à valeurs dans $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$.

Par indépendance,

$$\mathbb{P}(Y = n) = (1 - p)^{n-1} p$$

Remarque IV.2.

Souvent, le premier succès arrive assez tôt. En effet, il existe $\mu > 0$ tel que $1 - p = e^{-\mu}$, donc $(1 - p)^{n-1} p = e^{-(n-1)\mu} (1 - e^{-\mu})$, ce qui exhibe une décroissance exponentielle de la probabilité du premier succès avec le rang de ce succès.

Proposition IV.3.

Soit $p \in]0, 1[$. Soit X une variable aléatoire suivant la loi géométrique $\mathcal{G}(p)$. Alors

$$\forall (n, k) \in \mathbb{N}^2, \quad \mathbb{P}(X > n + k \mid X > n) = \mathbb{P}(X > k)$$

 On dit qu'une loi géométrique est une loi sans mémoire.

 **Preuve :** Soit $(n, k) \in \mathbb{N}^2$.

$$\begin{aligned} \mathbb{P}(X > n + k \mid X > n) &= \frac{\mathbb{P}(X > n + k)}{\mathbb{P}(X > n)} \\ &= \frac{\sum_{m=n+k+1}^{+\infty} (1 - p)^{m-1} p}{\sum_{m=n+1}^{+\infty} (1 - p)^{m-1} p} \\ &= \frac{(1 - p)^{n+k} \times \frac{1}{1 - (1 - p)}}{(1 - p)^n \times \frac{1}{1 - (1 - p)}} \\ &= (1 - p)^k = \mathbb{P}(X > k) \quad \text{formule utile pour une loi géométrique} \end{aligned}$$

 **Loi de Poisson :** Soit $\lambda > 0$. On dit qu'une variable aléatoire X à valeurs dans \mathbb{N} suit une loi de Poisson $\mathcal{P}(\lambda)$ lorsque pour tout $n \in \mathbb{N}$, $\mathbb{P}(X = n) = e^{-\lambda} \frac{\lambda^n}{n!}$.

Théorème IV.4.

Soit $\lambda > 0$. Soit $(p_n) \in]0, 1[^{\mathbb{N}}$ telle que $np_n \xrightarrow[n \rightarrow +\infty]{} \lambda$. Soit $(X_n)_{n \in \mathbb{N}}$ une suite de variables aléatoires telle que pour tout $n \in \mathbb{N}$, X_n suit la loi $\mathcal{B}(n, p_n)$. Alors $(X_n)_{n \in \mathbb{N}}$ converge en loi vers une loi de Poisson $\mathcal{P}(\lambda)$ i.e.

$$\forall m \in \mathbb{N}, \quad \mathbb{P}(X_n = m) \xrightarrow[n \rightarrow +\infty]{} e^{-\lambda} \frac{\lambda^m}{m!}$$

 **Preuve :** Soit $m \in \mathbb{N}$. Pour tout entier $n > m$,

$$\begin{aligned} \mathbb{P}(X_n = m) &= \binom{n}{m} p_n^m (1 - p_n)^{n-m} \\ &= \frac{n \times \cdots \times (n - m + 1)}{m!} (1 - p_n)^{-m} p_n^m (1 - p_n)^n \end{aligned}$$

Or $(1 - p_n)^n \xrightarrow[n \rightarrow +\infty]{} e^{-\lambda}$ car $p_n \underset{n \rightarrow +\infty}{\sim} \frac{\lambda}{n}$. De plus,

$$n \times \cdots \times (n - m + 1)(1 - p_n)^{-m} p_n^m = \underbrace{(np_n)^m}_{\xrightarrow[n \rightarrow +\infty]{} \lambda^m} \underbrace{\left(1 - \frac{1}{n}\right) \times \cdots \times \left(1 - \frac{m-1}{n}\right)}_{\xrightarrow[n \rightarrow +\infty]{} 1} \underbrace{(1 - p_n)^{-m}}_{\xrightarrow[n \rightarrow +\infty]{} 1}$$

ce qu'il fallait démontrer.

Exercice IV.5.

Soient $\lambda > 0$ et $p \in]0, 1[$. On modélise le nombre d'œufs pondus par un poisson par une loi de Poisson $\mathcal{P}(\lambda)$. On modélise l'éclosion d'un œuf indépendamment des autres par une loi de Bernoulli $\mathcal{B}(p)$. Déterminer la loi du nombre d'œufs éclos.

Exercice IV.6.

Soit $(\Omega, \mathcal{T}, \mathbb{P})$ un espace probabilisé. Soit $p \in]0, 1[$. Soit $(X_i)_{i \in \mathbb{N}^*}$ une suite de variables aléatoires définies sur (Ω, \mathcal{T}) , indépendantes et identiquement distribuées suivant la loi de Rademacher de paramètre p .

On pose $S_0 = 0$ et, pour tout $n \in \mathbb{N}^*$, $S_n = X_1 + \cdots + X_n$. Pour tout $m \in \mathbb{N}^*$, on pose $A_m = \bigcap_{n=0}^{+\infty} [|S_n| \leq m]$.

1. On suppose que $p = \frac{1}{2}$. Montrer que pour tout $m \in \mathbb{N}^*$, $\mathbb{P}(A_m) = 0$.
2. On suppose que $p \neq \frac{1}{2}$. Montrer que $\mathbb{P}([S_n = 0] \text{ infiniment souvent}) = 0$.

V Compléments

Fonction de répartition : Soit X une variable aléatoire à valeurs dans $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$. On introduit la fonction de répartition de X , notée F_X , définie par

$$\begin{aligned} F_X : \mathbb{R} &\longrightarrow [0, 1] \\ x &\longmapsto \mathbb{P}(X \leq x) \end{aligned}$$

 Cette fonction ne caractérise que la loi de X .

Proposition V.1.

Soit X une variable aléatoire à valeurs dans $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$. Alors :

- F_X est croissante.
- $F_X(x) \xrightarrow{x \rightarrow -\infty} 0$ et $F_X(x) \xrightarrow{x \rightarrow +\infty} 1$.
- F_X est continue à droite en tout point de \mathbb{R} .
- Soit $a \in \mathbb{R}$. F_X n'est pas continue en a si, et seulement si, $\mathbb{P}(X = a) > 0$.

Preuves :

- La croissance de F_X découle de la croissance de \mathbb{P} .
- Soit $(x_n)_{n \in \mathbb{N}}$ une suite réelle décroissante divergeant vers $-\infty$. $([X \leq x_n])_{n \in \mathbb{N}^*}$ est une suite décroissante d'événements donc par continuité décroissante,

$$F_X(x_n) \xrightarrow{n \rightarrow +\infty} \mathbb{P}\left(\bigcap_{n=0}^{+\infty} [X \leq x_n]\right) = \mathbb{P}(\emptyset) = 0$$

Par un raisonnement analogue, on prouve de même que $F_X(x) \xrightarrow{n \rightarrow +\infty} 1$

- Soit $(x_n)_{n \in \mathbb{N}}$ une suite réelle décroissante convergeant vers $a \in \mathbb{R}$. $([X \leq x_n])_{n \in \mathbb{N}^*}$ est une suite décroissante d'événements donc par continuité décroissante, $F_X(x_n) \xrightarrow{n \rightarrow +\infty} F_X(a)$. Donc F_X est continue à droite en a .
- (\Rightarrow) Soit $(x_n)_{n \in \mathbb{N}}$ une suite réelle décroissante convergeant vers a et $(y_n)_{n \in \mathbb{N}}$ une suite réelle croissante convergeant vers a sans valoir a . Par continuité croissante et décroissante, on montre que $F_X(x_n) \xrightarrow{n \rightarrow +\infty} F_X(a)$ et $F_X(y_n) \xrightarrow{n \rightarrow +\infty} F_X(a^-)$.
Donc $\mathbb{P}(X = a) = F_X(a) - F_X(a^-) > 0$ car F_X est discontinue en a .
- (\Leftarrow) Si F_X est continue en a , alors $\mathbb{P}(X = a) = F_X(a) - F_X(a^-) = 0$.

Variables à densité : Soit X une variable aléatoire à valeurs dans $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$. On dit que X est une variable aléatoire à densité s'il existe une fonction $f : \mathbb{R} \longrightarrow \mathbb{R}^+$ intégrable et telle que

$$\forall a \in \mathbb{R}, \quad F_X(a) = \int_{-\infty}^a f(t) dt$$

Une telle fonction détermine entièrement la loi de X .

Exemples :

- Pour tout $t \in \mathbb{R}$, $f(t) = e^{-t} \mathbb{1}_{[0, +\infty[}(t)$. f est la densité d'une loi exponentielle $\mathcal{E}(1)$.
- Pour tout $t \in \mathbb{R}$, $f(t) = \frac{1}{\sqrt{2\pi}} e^{-t^2/2}$. f est la densité d'une loi normale centrée réduite $\mathcal{N}(0, 1)$.
- Pour tout $t \in \mathbb{R}$, $f(t) = \frac{1}{(1+t^2)\pi}$. f est la densité d'une loi de Cauchy.

Il est alors possible de définir, sous réserve d'existence, l'espérance et le moment d'ordre 2 de telles variables par $\mathbb{E}(X) = \int_{-\infty}^{+\infty} tf(t)dt$, et $\mathbb{E}(X^2) = \int_{-\infty}^{+\infty} t^2 f(t)dt$

Proposition V.2.

Si X est une variable aléatoire à densité, alors pour tout $a \in \mathbb{R}$, $\mathbb{P}(X = a) = 0$.

Preuve : Soit $a \in \mathbb{R}$. $\mathbb{P}(X = a) = F_X(a) - F_X(a^-) = 0$ car la fonction de répartition d'une variable aléatoire à densité est continue. En effet, soit $\varepsilon > 0$. Pour tout $x \in [a - \varepsilon, a]$,

$$|F_X(a) - F_X(x)| \leq \|f\|_{\infty, [a-\varepsilon, a]} |x - a|$$

ce qui démontre à la continuité à gauche, donc la continuité.

Correction de l'exercice 8. :

Supposons que X soit indépendante d'elle-même. Soit $x \in \mathbb{R}$ tel que $\mathbb{P}(X = x) > 0$. Alors par indépendance des événements $[X = x]$ et $[X = x]$, $\mathbb{P}(X = x) = \mathbb{P}([X = x] \cap [X = x]) = \mathbb{P}(X = x)^2$, donc $\mathbb{P}(X = x) = 1$. Donc X est presque sûrement constante.

Réciproquement, toute variable aléatoire constante est indépendante d'elle-même.

En conclusion, une variable aléatoire est indépendante d'elle-même si, et seulement si, elle est presque sûrement constante.

Correction de l'exercice 9. :

$$1. \mathbb{P}(X = Y) = \mathbb{P}\left(\bigcup_{i=1}^{+\infty} [X = i] \cap [Y = i]\right) = \sum_{i=1}^{+\infty} \frac{1}{4^i} = \frac{1}{3}.$$

↑
indépendance

$$2. \mathbb{P}(X > Y) = \mathbb{P}\left(\bigcup_{i=1}^{+\infty} [Y = i] \cap [X > i]\right) = \sum_{i=1}^{+\infty} \frac{1}{2^i} \sum_{j=1}^{+\infty} \frac{1}{2^{i+j}} = \sum_{i=1}^{+\infty} \frac{1}{4^i} = \frac{1}{3}.$$

↑
indépendance

$$3. \mathbb{P}(\min(X, Y) \leq N) = 1 - \mathbb{P}(\underbrace{\min(X, Y) > N}_{=[X>N] \cap [Y>N]} \uparrow \text{indépendance}) = 1 - \mathbb{P}(X > N)\mathbb{P}(Y > N) = 1 - \frac{1}{4^N}$$

↑
calcul aisément

Correction de l'exercice 14. :

Notons X la variable aléatoire désignant le nombre d'œufs pondus, et Y le nombre d'œufs ayant éclos.

Pour tout $n \in \mathbb{N}$, $\mathbb{P}(X = n) = e^{-\lambda} \frac{\lambda^n}{n!}$ et pour tout $k \in \llbracket 0; n \rrbracket$, $\mathbb{P}(Y = k \mid X = n) = \binom{n}{k} p^k (1-p)^{n-k}$ car

lorsque $[X = n]$ est réalisé, chaque éclosion est considérée, indépendamment des autres comme un succès dans un schéma de Bernoulli d'ordre n et de probabilité de succès p .

Soit $k \in \mathbb{N}$.

$$\begin{aligned} \mathbb{P}(Y = k) &= \sum_{n=k}^{+\infty} \mathbb{P}([Y = k] \cap [X = n]) = \sum_{n=k}^{+\infty} \mathbb{P}(Y = k \mid X = n) \mathbb{P}(X = n) \\ &= \sum_{n=k}^{+\infty} \binom{n}{k} p^k (1-p)^{n-k} \times e^{-\lambda} \frac{\lambda^n}{n!} \\ &\quad \uparrow \quad m = n - k \\ &= e^{-\lambda} \sum_{m=0}^{+\infty} \frac{(m+k)!}{k! m!} p^k (1-p)^m \frac{\lambda^{m+k}}{(m+k)!} \\ &= e^{-\lambda} \frac{(p\lambda)^k}{k!} \sum_{m=0}^{+\infty} \frac{(1-p)^m \lambda^m}{m!} = e^{-\lambda} \frac{(p\lambda)^k}{k!} e^{(1-p)\lambda} \\ &= e^{-p\lambda} \frac{(p\lambda)^k}{k!} \end{aligned}$$

Donc Y suit la loi de Poisson $\mathcal{P}(p\lambda)$.

Correction de l'exercice 15. :

1. Soit $m \in \mathbb{N}^*$. Soit $k \in \mathbb{N}^*$. Posons $B_k = \bigcap_{i=0}^{2m+1} [X_{km+i} = 1]$. Par indépendance, $\mathbb{P}(B_k) = \frac{1}{2^{2m+2}}$ et par construction, si B_k est réalisé, alors $|S_{mk+2m+1} - S_{mk-1}| \geq 2m + 2$ est réalisé, donc $[S_{mk+2m+1} \notin \llbracket -m; m \rrbracket] \cup [S_{mk-1} \notin \llbracket -m; m \rrbracket]$ est réalisé, et ceci est valable pour tout $k \in \mathbb{N}^*$. Pour tout $\ell \in \mathbb{N}^*$

posons $k_\ell = 4\ell m$. Par le lemme des coalitions, pour tous $\ell, \ell' \in \mathbb{N}^*$ tels que $\ell \neq \ell'$, les événements B_ℓ et $B_{\ell'}$ sont indépendants. De plus $\sum_{\ell \geq 1} \mathbb{P}(B_{k_\ell})$ est divergente (son terme général est non nul et indépendant de ℓ).

Le premier théorème de Borel-Cantelli assure alors que $\mathbb{P}\left(\bigcap_{\ell=1}^{+\infty} \left(\bigcup_{\ell'=l+1}^{+\infty} B_{k'_\ell}\right)\right) = 1$

Autrement dit, presque sûrement, B_{k_ℓ} est réalisé infiniment souvent, donc l'événement A_m est négligeable : il existe une partie infinie J de \mathbb{N} telle que pour tout $n \in J$, $S_n \notin \llbracket -m; m \rrbracket$.

2. Pour tout $m \in \mathbb{N}^*$, posons $u_m = \mathbb{P}(S_{2m} = 0)$.

Soit $m \in \mathbb{N}^*$. Remarquons que le retour à l'origine se fait si, et seulement si, autant de déplacements à gauche qu'à droite ont lieu et, sur $2m$ déplacements il y a $\binom{2m}{m}$ telles combinaisons et par indépendance des déplacements, $u_m = \binom{2m}{m} p^m (1-p)^m$. Alors

$$\frac{u_{m+1}}{u_m} = p(1-p) \frac{(2m+2)(2m+1)}{(m+1)^2} \xrightarrow[m \rightarrow +\infty]{} 4p(1-p) < 1$$

En effet, $y = x(1-x)$ est une parabole tournée vers le bas atteignant son maximum entre les deux racines de $X(X-1)$, donc en $x = \frac{1}{2}$, et celui-ci vaut $\frac{1}{4}$. $p \neq \frac{1}{2}$ donc l'inégalité est stricte. D'après la règle de d'Alembert, $\sum_{m \geq 1} u_m$ converge.

Le deuxième théorème de Borel-Cantelli assure alors que $\mathbb{P}([S_{2m} = 0] \text{ infiniment souvent}) = 0$.



CHAPITRE 30.4

Couples de variables aléatoires

Soit $d \in \mathbb{N}^*$. Dans tout ce chapitre, les variables aléatoires sont définies sur l'espace probabilisé $(\Omega, \mathcal{T}, \mathbb{P})$ et à valeurs dans l'espace mesurable $(\mathbb{R}^d, \mathcal{B}(\mathbb{R}^d))$.

I Loi conjointe, loi marginale

Définition I.1.

Soient X, Y deux variables aléatoires discrètes. La loi conjointe de (X, Y) est définie par

$$\forall (x, y) \in (\mathbb{R}^d)^2, \quad \mathcal{L}_{(X,Y)}(\{(x, y)\}) = \mathbb{P}([X = x] \cap [Y = y])$$

Les lois \mathcal{L}_X et \mathcal{L}_Y sont appelées lois marginales de $\mathcal{L}_{(X,Y)}$.

Remarque I.2.

Les lois marginales se calculent à partir de la loi conjointe :

$$\forall x \in \mathbb{R}^d, \quad \mathbb{P}(X = x) = \mathbb{P}\left(\bigsqcup_{y \in Y(\Omega)} [X = x] \cap [Y = y]\right) = \sum_{y \in Y(\Omega)} \mathcal{L}_{(X,Y)}(\{(x, y)\})$$

Exercice I.3.

Soit $(\Omega, \mathcal{T}, \mathbb{P})$ un espace probabilisé.

Soient X et Y deux variables aléatoires à valeurs dans $(\mathbb{N}, \mathcal{P}(\mathbb{N}))$ telles que pour tout $(i, j) \in \mathbb{N}^2$

$$\mathcal{L}_{(X,Y)}(\{(i, j)\}) = \frac{1}{2^{i+j+2}}$$

1. Vérifier que $\mathcal{L}_{(X,Y)}$ est bien une loi de probabilité.
2. Calculer les lois marginales \mathcal{L}_X et \mathcal{L}_Y .
3. X et Y sont-elles indépendantes ?

II Produit de convolution

Soient X et Y deux variables aléatoires à valeurs dans $(\mathbb{N}, \mathcal{P}(\mathbb{N}))$. On définit le produit de convolution de \mathcal{L}_X et \mathcal{L}_Y , et note $\mathcal{L}_X * \mathcal{L}_Y$, par :

$$\forall n \in \mathbb{N}, (\mathcal{L}_X * \mathcal{L}_Y)(\{n\}) = \sum_{\substack{(i,j) \in \mathbb{N}^2 \\ i+j=n}} \mathcal{L}_X(\{i\}) \mathcal{L}_Y(\{j\})$$

Si, de plus, X et Y sont indépendantes, alors $\mathcal{L}_{X+Y} = \mathcal{L}_X \star \mathcal{L}_Y$. En effet, pour tout $n \in \mathbb{N}$,

$$\mathbb{P}(X + Y = n) = \sum_{\substack{(i,j) \in \mathbb{N}^2 \\ i+j=n}} \mathbb{P}([X = i] \cap [Y = j]) = \sum_{\substack{(i,j) \in \mathbb{N}^2 \\ \text{indépendante} \\ i+j=n}} \mathbb{P}(X = i)\mathbb{P}(Y = j) = (\mathcal{L}_X \star \mathcal{L}_Y)(\{n\})$$

Exemples : On suppose que $d = 1$.

→ **Produit de convolution de lois binomiales :** Soient $n, m \in \mathbb{N}^*$ et $p \in]0, 1[$. Soient X_1, \dots, X_{n+m} des variables aléatoires indépendantes et identiquement distribuées suivant la loi $\mathcal{B}(p)$. Posons $X = X_1 + \dots + X_n$ et $Y = X_{n+1} + \dots + X_{n+m}$. Alors \mathcal{L}_{X+Y} est une loi binomiale $\mathcal{B}(n+m, p)$.

❖ **Produit de convolution de lois de Poisson :** Soient $\lambda, \mu > 0$. Posons $\mathcal{L}_1 = \mathcal{P}(\lambda)$ $\mathcal{L}_2 = \mathcal{P}(\mu)$. Alors, pour tout $n \in \mathbb{N}$,

$$\begin{aligned} (\mathcal{L}_1 \star \mathcal{L}_2)(\{n\}) &= \sum_{\substack{(i,j) \in \mathbb{N}^2 \\ i+j=n}} \frac{\lambda^i}{i!} e^{-\lambda} \cdot \frac{\mu^j}{j!} e^{-\mu} \\ &= e^{-(\lambda+\mu)} \sum_{\substack{(i,j) \in \mathbb{N}^2 \\ i+j=n}} \frac{1}{n!} \binom{n}{i} \lambda^i \mu^{n-i} \\ &= e^{-(\lambda+\mu)} \sum_{i=0}^n \frac{1}{n!} \binom{n}{i} \lambda^i \mu^{n-i} = \frac{(\lambda + \mu)^n}{n!} e^{-(\lambda+\mu)} \end{aligned}$$

On reconnaît une loi de Poisson $\mathcal{P}(\lambda + \mu)$.

Correction de l'exercice 3. :



1. Le nombre de manières d'écrire un entier naturel n non nul sous la forme d'une somme de deux entiers naturels vaut le nombre de manières de placer un baton parmi n objets alignés de sorte à les scinder en deux groupes d'objets en autorisant toutefois qu'au moins l'un des groupes n'en contienne aucun. De tels emplacements pour le baton, il y en a $n + 1$. Ainsi, dans la somme calculée ci-dessous, il y a $n + 1$ termes égaux à $\frac{1}{2^{i+j+2}}$ lorsque $i + j = n$.

Ce raisonnement est aisément généralisable si l'on veut écrire un entier naturel non nul sous la forme d'une somme à plus de deux termes d'entier naturel.

$$\sum_{(i,j) \in \mathbb{N}^2} \mathcal{L}_{(X,Y)}(\{(i,j)\}) = \sum_{n=0}^{+\infty} \frac{n+1}{2^{n+2}} = \frac{1}{4} \sum_{n=0}^{+\infty} \frac{n+1}{2^n} = \frac{1}{4} \cdot \frac{1}{\left(1 - \frac{1}{2}\right)^2} = 1$$

Donc $\mathcal{L}_{(X,Y)}$ est bien une loi de probabilité.



Il est loisible de retenir les sommes des séries dérivées d'une série géométrique convergente. Soit $q \in \mathbb{C}$ tel que $|q| < 1$. Alors

$$\sum_{n=1}^{+\infty} nq^{n-1} = \frac{1}{(1-q)^2} \quad \text{et} \quad \sum_{n=2}^{+\infty} n(n-1)q^{n-2} = \frac{2}{(1-q)^3}$$

2. Soit $i \in \mathbb{N}$.

$$\mathcal{L}_X(\{i\}) = \sum_{j=0}^{+\infty} \mathcal{L}_{(X,Y)}(\{(i,j)\}) = \frac{1}{2^{i+2}} \sum_{j=0}^{+\infty} \frac{1}{2^j} = \frac{1}{2^{i+1}} = \mathcal{L}_Y(\{i\})$$

3. Oui, car pour tout $(i,j) \in \mathbb{N}^2$, $\mathcal{L}_X(\{i\})\mathcal{L}_Y(\{j\}) = \frac{1}{2^{i+j+2}} = \mathcal{L}_{(X,Y)}(\{i,j\})$



Espaces préhilbertiens réels

Dans tout ce chapitre, E désigne un \mathbb{R} -espace vectoriel non réduit à $\{0\}$.

I Géométrie d'un espace préhilbertien

Définition I.1.

Un produit scalaire sur E est une application $\langle \cdot, \cdot \rangle : E^2 \rightarrow \mathbb{R}$ bilinéaire qui vérifie les propriétés suivantes :

- Elle est symétrique, *i.e.* pour tout $(x, y) \in E^2$, $\langle x, y \rangle = \langle y, x \rangle$.
- Elle est positive, *i.e.* pour tout $x \in E$, $\langle x, x \rangle \geq 0$.
- Elle est définie positive, *i.e.* pour tout $x \in E \setminus \{0\}$, $\langle x, x \rangle \neq 0$.

Exemples

- Pour tout $n \in \mathbb{N}^*$, le produit scalaire canonique sur \mathbb{R}^n est défini par :

$$\forall x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbb{R}^n, \quad \langle x, y \rangle = \sum_{i=1}^n x_i y_i$$

- Pour tout entier $n \geq 2$, le produit scalaire canonique sur $\mathcal{M}_n(\mathbb{R})$ est défini par :

$$\forall A, B \in \mathcal{M}_n(\mathbb{R}), \quad \langle A, B \rangle = \text{Tr}(A^\top B)$$

De plus, si $O \in \mathcal{O}_n(\mathbb{C})$, et A et $B \in \mathcal{M}_n(\mathbb{R})$, alors $\langle OA, OB \rangle = \text{Tr}(A^\top \underbrace{O^\top O}_{=I_n} B) = \langle A, B \rangle$

- Pour tout intervalle réel I , le produit scalaire canonique sur l'espace $L_c^2(I, \mathbb{R})$ des fonctions réelles continues sur I et de carré intégrable est défini par :

$$\forall f, g \in L_c^2(I), \quad \langle f, g \rangle = \int_I f(t)g(t)dt$$

- Le produit scalaire canonique sur l'espace $\ell^2(\mathbb{N}, \mathbb{R})$ des suites réelles de carré sommable est défini par :

$$\forall (u_n), (v_n) \in \ell^2(\mathbb{N}, \mathbb{R}), \quad \langle u, v \rangle = \sum_{n=0}^{+\infty} u_n v_n$$



L'existence des deux derniers produits scalaires est assurée par l'inégalité valable pour tous réels x et y : $|xy| \leq \frac{x^2 + y^2}{2}$.

Dans tout le reste du chapitre, on munit E d'un produit scalaire $\langle \cdot, \cdot \rangle$, si bien que $(E, \langle \cdot, \cdot \rangle)$ est un espace préhilbertien réel.

Théorème (Inégalité de Cauchy-Schwarz) I.2.

Pour tout $(x, y) \in E$,

$$|\langle x, y \rangle| \leq \sqrt{\langle x, x \rangle} \sqrt{\langle y, y \rangle}$$

et l'inégalité est une égalité si, et seulement si, x et y sont colinéaires.

Preuve : Supposons que $y \neq 0$. Introduisons la fonction réelle



$$\varphi : t \mapsto \langle x + ty, x + ty \rangle = \langle x, x \rangle + 2 \langle x, y \rangle t + \langle y, y \rangle t^2$$

Cette fonction polynomiale est positive, donc son discriminant, qui vaut $4 \langle x, y \rangle^2 - 4 \langle x, x \rangle \langle y, y \rangle$, est négatif ou nul, d'où l'inégalité.

Le cas d'égalité est réalisé si, et seulement si, il existe $t_0 \in \mathbb{R}$ tel que $\varphi(t_0) = 0$ donc si, et seulement si, $x + t_0 y = 0$.

Remarque I.3.

Supposons que $\langle \cdot, \cdot \rangle$ ne soit pas défini positif. Soit $y \in E \setminus \{0\}$ tel que $\langle y, y \rangle = 0$. Alors, pour tout $x \in E$, $\langle x, y \rangle = 0$.

En effet, φ serait affine et positive, donc constante.



Exemple : Si $(\Omega, \mathcal{A}, \mathbb{P})$ est un espace probabilisé dénombrable, l'application $f : (X, Y) \mapsto \mathbb{E}(XY)$ est une forme bilinéaire, symétrique, et positive sur l'espace $L_0^2(\Omega, \mathbb{R})$ des variables aléatoires réelles sur Ω d'espérances nulles et qui admettent un moment d'ordre 2, mais elle n'est pas définie positive car si $X \in L^2(\Omega, \mathbb{R})$, on a l'équivalence $\mathbb{E}(X^2) = 0 \iff \mathbb{P}(X = 0) = 1$ mais X n'est pas nécessairement nulle.



Analogie avec le théorème de Pythagore : La variance peut être interprétée comme le carré de la « norme » associée au « produit scalaire » f . En effet, pour tout entier $n \geq 2$, si $X_1, \dots, X_n \in L^2(\Omega, \mathbb{R})$ sont indépendantes, alors, pour tout $(i, j) \in \llbracket 1; n \rrbracket^2$ tel que $i \neq j$, $\text{Cov}(X_i, X_j) = \mathbb{E}(X_i X_j) = 0$, et on a bien

$$\mathbb{V}\left(\sum_{k=1}^n X_k\right) = \sum_{k=1}^n \mathbb{V}(X_k)$$

Théorème (Inégalité de Minkowski) I.4.

Pour tout $x \in E$, on note $\|x\|$ le réel $\sqrt{\langle x, x \rangle}$. Alors, pour tout $(x, y) \in E^2$,

$$\|x + y\| \leq \|x\| + \|y\|$$

et l'inégalité est une égalité si, et seulement si, il existe $\lambda \geq 0$ tel que $x = \lambda y$ ou $y = \lambda x$.

Preuve : $\|x + y\|^2 = \|x\|^2 + \|y\|^2 + 2 \langle x, y \rangle \leq \|x\|^2 + \|y\|^2 + 2 \|x\| \|y\| = (\|x\| + \|y\|)^2$ où l'on a utilisé l'inégalité de Cauchy-Schwarz.

$\|x + y\| = \|x\| + \|y\|$ si, et seulement si, $\langle x, y \rangle = \|x\| \|y\|$, donc, si et seulement si le cas d'égalité de l'inégalité de Cauchy-Schwarz est vérifié (car $\langle x, y \rangle \leq |\langle x, y \rangle| \leq \|x\| \|y\|$). Quitte à échanger x et y , supposons $x \neq 0$. Alors, l'inégalité de Minkowski est une égalité si, et seulement si, il existe $\lambda \in \mathbb{R}$ tel que $\lambda \langle x, x \rangle = |\lambda| \|x\|^2$, ce qu'il fallait démontrer.

Si n est un entier supérieur ou égal à 2, l'inégalité se généralise avec $x_1, \dots, x_n \in E$, et, s'il ne sont pas tous nuls, le cas d'égalité se traduit géométriquement par l'appartenance des x_i à une demi-droite d'origine O, dont le sens est déterminé par l'un des points non confondu avec l'origine (cf. chapitre 1).

Dans tout le reste du chapitre, E est également muni de la norme euclidienne $\|\cdot\|$ associée à $\langle \cdot, \cdot \rangle$.

Exercice I.5.

Soit $(E, \|\cdot\|)$ est un espace vectoriel normé non trivial. Soient C une partie convexe de E , et $x \in E$. x est un point extrémal de C s'il n'est contenu dans aucun segment de C non réduit à un point, donc si et seulement si, on a la propriété

$$\forall y, z \in C, (\exists t \in [0, 1], x = ty + (1 - t)z \implies x = y \text{ ou } x = z)$$

Déterminer les points extrémaux de $\overline{B}(0, 1)$.

Égalité de la médiane : Pour tout $(x, y) \in E^2$, $\|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2)$

Application

Soit $(a, b) \in E^2$ tel que $a \neq b$. Soit $r > 0$. Montrons que $\overbrace{\overline{B}(a, r)}^{\text{notée } \Gamma} \cap \overbrace{\overline{B}(b, r)}^{\text{notée } \Gamma} < 2r$.

Si, $\|a - b\| > 2r$, Γ est vide, et il n'y a rien à démontrer.

Si $\|a - b\| \leq 2r$, Γ n'est pas vide et $\frac{a+b}{2} \in \Gamma$. Soit $x \in \Gamma$.

$$\begin{aligned} \left\| x - \frac{a+b}{2} \right\|^2 &= \left\| \underbrace{\frac{1}{2}(x-a)}_{\text{noté } u} + \underbrace{\frac{1}{2}(x-b)}_{\text{noté } v} \right\|^2 \\ &= \frac{1}{4} \|u + v\|^2 \\ &= \frac{1}{2} \left(\underbrace{\|u\|^2}_{\substack{\leq r^2 \\ \uparrow \\ \text{égalité de la médiane}}} + \underbrace{\|v\|^2}_{\substack{\leq r^2 \\ < 2r^2}} \right) - \frac{1}{2} \|u - v\|^2 < r^2 \end{aligned}$$

Or, pour tout $(x, y) \in \Gamma^2$, $\|x - y\| \leq \left\| x - \frac{a+b}{2} \right\| + \left\| y - \frac{a+b}{2} \right\| < 2r$, ce qu'on voulait.

Exercice I.6.

Soit (E, \mathcal{N}) un \mathbb{R} -espace vectoriel normé. On suppose que pour tout $(x, y) \in E^2$,

$$\mathcal{N}(x+y)^2 + \mathcal{N}(x-y)^2 = 2(\mathcal{N}(x)^2 - \mathcal{N}(y)^2)$$

Montrer qu'il existe un produit scalaire sur E tel que \mathcal{N} soit la norme euclidienne qui lui est associée.

II Orthogonalité

1. Généralités

Définition II.1.

Soit I un ensemble non vide. Une famille $(x_i) \in E^I$ est dite orthogonale lorsque pour tout $(i, j) \in I^2$ tel que $i \neq j$, $\langle x_i, x_j \rangle = 0$.

Elle est dite orthonormée si, de plus, pour tout $i \in I$, $\|x_i\| = 1$.

Proposition II.2.

Soit I un ensemble non vide, et $(x_i)_{i \in I}$ une famille orthogonale de E .

- Pour tout partie finie J de I , et pour toute $(\lambda_i) \in \mathbb{R}^J$, $\left\| \sum_{i \in J} \lambda_i x_i \right\|^2 = \sum_{i \in J} |\lambda_i| \|x_i\|^2$
- Si, pour tout $i \in I$, $x_i \neq 0$, alors $(x_i)_{i \in I}$ est libre.

Exercice II.3.

On admet que $\ell^2(\mathbb{N}, \mathbb{R})$ est de dimension infinie non dénombrable. Montrer que $\ell^2(\mathbb{N}, \mathbb{R})$, muni de son produit scalaire canonique et de la norme associée notée $\|\cdot\|$, n'admet pas de base orthonormée.

2. Dimension finie

Dans cette partie, on suppose que E est de dimension finie n , i.e. $(E, \langle \cdot, \cdot \rangle)$ est un espace euclidien.

Théorème II.4.

L'application

$$\begin{aligned} j : E &\longrightarrow E^* \\ u &\longmapsto \langle u, \cdot \rangle \end{aligned}$$

est un isomorphisme.

Preuve : La bilinéarité du produit scalaire entraîne la linéarité de j .

Si $u \in \text{Ker}(j)$, alors, pour tout $v \in E$, $\langle u, v \rangle = 0$, donc $\langle u, u \rangle = 0$, donc $u = 0$ i.e. j est injective. L'égalité des dimensions de E et E^* permet de conclure.

Corollaire II.5.

Supposons que $n \geq 2$. Soit H un hyperplan de E . Alors, il existe $u \in E \setminus \{0\}$ tel que, pour tout $x \in E$, on ait l'équivalence

$$x \in H \iff \langle u, x \rangle = 0$$

L'ensemble de tels u est inclus dans une droite d'origine O, et $\mathbb{R}u$ est la normale à H .

Preuve : H est le noyau d'une forme linéaire sur E non nulle, donc d'après le théorème, il existe un unique $u \in E \setminus \{0\}$, dépendant du choix de cette forme linéaire, tel que $H = \text{Ker}(\langle u, \cdot \rangle)$, ce qui démontre

l'équivalence.

Soit φ une forme linéaire sur E non nulle de noyau H , et notons v_φ l'unique vecteur tel que $\langle v_\varphi, \cdot \rangle = \varphi$. Alors v_φ convient également, et $\text{Ker}(\langle v_\varphi, \cdot \rangle) = \text{Ker}(\langle u, \cdot \rangle) = H$ donc $\langle u, \cdot \rangle$ et $\langle v_\varphi, \cdot \rangle$ sont proportionnelles, i.e. il existe $\lambda \in \mathbb{R}^*$ tel que $\langle v_\varphi, \cdot \rangle = \lambda \langle u, \cdot \rangle = \langle \lambda u, \cdot \rangle$. j étant injective, $v_\varphi = \lambda u$.

Théorème II.6.

- E possède des bases orthonormées.
- Supposons que $n \geq 2$. Soit $p \in \mathbb{N}^*$ tel que $p < n$. Si (e_1, \dots, e_p) est une famille orthonormée de E , alors il existe une famille (e_{p+1}, \dots, e_n) telle que (e_1, \dots, e_n) soit une base de E .

Preuve :

- Si $n = 1$, un vecteur $x \in E$ de norme 1 forme à lui tout seul une base de E . Supposons que $n \geq 2$, et pour tout $k \in \llbracket 1; n-1 \rrbracket$ introduisons par récurrence descendante un hyperplan E_k de E_{k+1} . Pour tout $k \in \llbracket 1; n \rrbracket$ introduisons l'assertion

$$\mathcal{P}_k : \text{« } E_k \text{ possède une base orthonormée »}$$

\mathcal{P}_1 est vraie. Supposons qu'il existe $k \in \llbracket 1; n-1 \rrbracket$ tel que \mathcal{P}_k soit vraie. Alors, E_k , possède une base orthonormée (e_1, \dots, e_k) . Soit $u \in E_{k+1} \setminus \{0\}$ tel que $\mathbb{R}u$ soit la normale à E_k dans E_{k+1} , et posons $e_{k+1} = \frac{1}{\|u\|}u$ de sorte que $\|e_{k+1}\| = 1$. Alors la famille (e_1, \dots, e_{k+1}) est libre car e_{k+1} est orthogonal aux vecteurs de (e_1, \dots, e_k) . De plus, elle comporte $k+1$ vecteurs, et $\dim(E_{k+1}) = k+1$. Donc (e_1, \dots, e_{k+1}) est une base orthonormée de E_{k+1} . Donc \mathcal{P}_{k+1} est vraie. Par récurrence finie, E possède une base orthonormée. Chaque vecteur de la base construite peut être changé en son opposé, donc E admet des bases orthonormées.

- En complétant la famille libre (car orthonormée) (e_1, \dots, e_p) en une base $(e_1, \dots, e_p, u_{p+1}, \dots, u_p)$ de E , puis en posant $E_p = \text{Vect}(e_1, \dots, e_p)$, et, pour tout $k \in \llbracket p+1; n \rrbracket$, $E_k = \text{Vect}(e_1, \dots, e_p, u_{p+1}, \dots, u_k)$, la récurrence ci-dessus permet de compléter (e_1, \dots, e_p) en une base orthonormée de E .

Théorème (Procédé de Gram-Schmidt) II.7.

Soit (e_1, \dots, e_n) une base de E . Il existe une base orthonormée $(\varepsilon_1, \dots, \varepsilon_n)$ de E telle qu'on ait la propriété :

$$\forall k \in \llbracket 1; n \rrbracket, \quad \text{Vect}(\varepsilon_1, \dots, \varepsilon_k) = \text{Vect}(e_1, \dots, e_k)$$

De plus, si $(\varepsilon'_1, \dots, \varepsilon'_n)$ est une base orthonormée vérifiant la même propriété, alors, il existe $(\alpha_1, \dots, \alpha_n) \in \{-1, 1\}^n$ tel que pour tout $i \in \llbracket 1; n \rrbracket$, $\varepsilon'_i = \alpha_i \varepsilon_i$.

Preuve : Pour tout $k \in \llbracket 1; n \rrbracket$, introduisons l'assertion

$$\begin{aligned} \mathcal{A}_k : & \text{« Il existe une famille orthonormée } (\varepsilon_1, \dots, \varepsilon_k) \text{ de } E \text{ telle} \\ & \text{que pour tout } i \in \llbracket 1; k \rrbracket, \underbrace{\text{Vect}(e_1, \dots, e_i)}_{\text{noté } E_i} = \text{Vect}(\varepsilon_1, \dots, \varepsilon_i) \text{ »} \end{aligned}$$

- En posant $\varepsilon_1 = \pm \frac{1}{\|e_1\|}e_1$, on montre que \mathcal{A}_1 est vraie. Ces deux choix sont également les seuls possibles pour que \mathcal{A}_1 soit vraie.
- Soit $k \in \llbracket 1; n-1 \rrbracket$ tel que \mathcal{A}_k soit vraie. E_k est un hyperplan de E_{k+1} donc il existe $u \in E_{k+1} \setminus \{0\}$ tel que $\mathbb{R}u$ soit l'unique normale à E_k dans E_{k+1} passant par l'origine. Ainsi, pour que $(\varepsilon_1, \dots, \varepsilon_{k+1})$ soit une base orthonormée de E_{k+1} , il faut et il suffit que $\varepsilon_{k+1} = \pm \frac{1}{\|u\|}u$.



Le caractère suffisant de cette condition suffit pour mener à terme cette récurrence.

Alors, $\text{Vect}(\varepsilon_1, \dots, \varepsilon_{k+1}) = E_{k+1} = \text{Vect}(e_1, \dots, e_{k+1})$. L'hypothèse de récurrence assure par ailleurs que pour tout $i \in \llbracket 1; k \rrbracket$, $\text{Vect}(e_1, \dots, e_i) = \text{Vect}(\varepsilon_1, \dots, \varepsilon_i)$. Donc \mathcal{A}_{k+1} est vraie.

→ Finalement, le principe de récurrence assure que \mathcal{A}_n est vraie.

Nous avons exhibé, lors de la construction de $(\varepsilon_1, \dots, \varepsilon_n)$, que chaque ε_i peut être échangé avec son opposé, et seulement son opposé, si bien que l'ensemble des bases orthonormées vérifiant la propriété démontrée par récurrence est $\{(\alpha_1 \varepsilon_1, \dots, \alpha_n \varepsilon_n) \mid (\alpha_1, \dots, \alpha_n) \in \{-1, 1\}^n\}$

Expression matricielle : La matrice de (e_1, \dots, e_n) relativement la base $(\varepsilon_1, \dots, \varepsilon_n)$ est triangulaire supérieure. En effet, pour tout $i \in \llbracket 1; n \rrbracket$, e_i est une combinaison linéaire des vecteurs de la famille $(\varepsilon_1, \dots, \varepsilon_i)$ en vertu de l'égalité $\text{Vect}(e_1, \dots, e_i) = \text{Vect}(\varepsilon_1, \dots, \varepsilon_i)$.

Proposition II.8.

Soient x et $y \in E$, et introduisons leurs décompositions dans une base orthonormée (e_1, \dots, e_n) de E :

$$x = \sum_{i=1}^n x_i e_i \quad y = \sum_{i=1}^n y_i e_i$$

Alors,

$$\langle x, y \rangle = \sum_{i=1}^n x_i y_i \quad \|x\|^2 = \sum_{i=1}^n \langle x, e_i \rangle^2 = \sum_{i=1}^n x_i^2$$

Remarque II.9.

La décomposition de x étant unique dans la base (e_1, \dots, e_n) , l'application

$$\begin{aligned} E &\longrightarrow \mathbb{R}^n \\ x &\longmapsto (\langle x, e_i \rangle)_{1 \leq i \leq n} \end{aligned}$$

est un isomorphisme.

Exercice II.10.

Soit $(E, \langle \cdot, \cdot \rangle)$ un espace euclidien de dimension $n \geq 1$, et notons $\|\cdot\|$ la norme euclidienne associée à $\langle \cdot, \cdot \rangle$. Soit m un entier supérieur ou égal à n . Soit $(e_1, \dots, e_m) \in E^m$ tel que pour tout $x \in E$,

$$\|x\|^2 = \sum_{i=1}^n \langle x, e_i \rangle^2$$

1. Montrer que $\text{Vect}(e_1, \dots, e_m) = E$.
2. Donner un exemple d'espace euclidien et des exemples de vecteurs vérifiant les hypothèses de l'exercice lorsque $m = 3$, $n = 2$, et $\|e_1\| = \|e_2\| = \|e_3\|$.
3. Supposons que $n = m$. Montrer que (e_1, \dots, e_n) est une base orthonormée de E .

3. Orthogonal d'une partie

On rappelle que $(E, \langle \cdot, \cdot \rangle)$ est un espace préhilbertien réel, et que $\|\cdot\|$ est la norme associée à $\langle \cdot, \cdot \rangle$.

Définition II.11.

Soit A une partie de E . On appelle *orthogonal de A* l'ensemble

$$A^\perp = \{x \in E \mid \forall y \in A, \langle x, y \rangle = 0\}$$

Proposition II.12.

Soient A et B des parties de E .

$$\rightarrow \{0\}^\perp = E \text{ et } E^\perp = \{0\}.$$

$\rightarrow A^\perp = \bigcap_{x \in A} \text{Ker}(\langle x, \cdot \rangle)$ est un sous-espace vectoriel de E .

\rightarrow Si $A \subset B$, alors $B^\perp \subset A^\perp$.

Conséquence : Pour toute partie A de E , on a $A \subset (A^\perp)^\perp$, donc $A^\perp = ((A^\perp)^\perp)^\perp$.

Définition II.13.

Soit F un sous-espace vectoriel de E . On dit que F admet un supplémentaire orthogonal dans E s'il existe un sous espace vectoriel G de F^\perp tel que $E = F \oplus G$.

Conséquence : Dans ce cas, $G = F^\perp$.

Preuve de l'unicité sous réserve d'existence : Si, $x \in F^\perp$, il existe $y \in F$, et $z \in G$ tels que $x = y + z$, donc $y = x - z \in F^\perp$ donc $y = 0$, donc $x = z \in G$. Ainsi, $F^\perp \subset G$.

Observation : Soit F une partie de E . Alors F^\perp est fermé dans E .

Preuve : Pour tout $y \in F$, l'application linéaire $x \mapsto \langle x, y \rangle$ est continue en vertu de l'inégalité de Cauchy-Schwarz, son noyau est donc fermé en tant qu'image réciproque de $\{0\}$, fermé dans \mathbb{R} . Or F^\perp est l'intersection de tels fermés, d'où l'observation.

4. Orthogonal d'un sous-espace vectoriel de dimension finie

Dans cette partie, on suppose que $(E, \langle \cdot, \cdot \rangle)$ est un espace euclidien de dimension n .

Théorème II.14.

Soit F un sous-espace vectoriel de E . Alors $F \oplus F^\perp = E$.

Preuve : Notons p la dimension de F . Soit (e_1, \dots, e_p) une base orthonormée de F que l'on complète en une base orthonormée (e_1, \dots, e_n) de E . Alors, pour tout $x \in E$, il existe $(x_1, \dots, x_n) \in \mathbb{R}^n$ tel que

$$x = \underbrace{\sum_{i=1}^p x_i e_i}_{\in F} + \underbrace{\sum_{i=p+1}^n x_i e_i}_{\in F^\perp}$$

Donc $F + F^\perp = E$. De plus, $F \cap F^\perp = \{0\}$, donc $E = F \oplus F^\perp$.

Proposition II.15.

Soient F et G des sous-espaces vectoriels de E .

$$\rightarrow \dim(F^\perp) = n - \dim(F).$$

$$\rightarrow (F^\perp)^\perp = F. \text{ En effet, } F \subset (F^\perp)^\perp \text{, et } \dim((F^\perp)^\perp) = \dim(F).$$

$\rightarrow (F + G)^\perp = F^\perp \cap G^\perp$. En effet, par bilinéarité du produit scalaire, $F^\perp \cap G^\perp \subset (F + G)^\perp$, et l'inclusion réciproque est vraie car $F \subset F + G$ et $G \subset F + G$.

$$\rightarrow (F \cap G)^\perp = ((F^\perp)^\perp \cap (G^\perp)^\perp)^\perp = ((F^\perp + G^\perp)^\perp)^\perp = F^\perp + G^\perp.$$



L'orthogonal d'une somme est l'intersection des orthogonaux, et l'orthogonal d'une intersection est la somme des orthogonaux.

5. Projecteurs orthogonaux

On rappelle que $(E, \langle \cdot, \cdot \rangle)$ est un espace préhilbertien réel, et que $\|\cdot\|$ est la norme euclidienne associée à $\langle \cdot, \cdot \rangle$.

Définition II.16.

Soit $p \in \mathcal{L}(E)$. On dit que p est un projecteur orthogonal lorsque $p = p \circ p$ et $\text{Ker}(p) \perp \text{Im}(p)$.

Proposition II.17.

Soit $p \in \mathcal{L}(E)$ tel que p soit un projecteur orthogonal.

$$\rightarrow \text{Ker}(p) = \text{Im}(p)^\perp \text{ et } \text{Im}(p) = \text{Ker}(p)^\perp.$$

$\rightarrow \text{Ker}(p)$ et $\text{Im}(p)$ sont fermés.

$$\rightarrow \text{Si } p \neq 0, \|p\| = 1.$$

Preuve

$$\rightarrow \text{Ker}(p) \oplus \text{Im}(p) = E \text{ et } \text{Im}(p) \subset \text{Ker}(p)^\perp \text{ donc } \text{Im}(p) = \text{Ker}(p)^\perp.$$

\rightarrow La première propriété entraîne immédiatement la deuxième.

$$\rightarrow \text{Soit } x = \underbrace{y}_{\in \text{Ker}(p)} + \underbrace{z}_{\in \text{Im}(p)} \in E. \text{ Alors } \|x\|^2 = \|y\|^2 + \|z\|^2 \geq \|z\|^2 = \|p(x)\|^2.$$

Donc, pour tout $x \in E \setminus \{0\}$, $\frac{\|p(x)\|^2}{\|x\|^2} \leq 1$, ce qui assure que $\|p\| \leq 1$. De plus, ce majorant est atteint pour tout $x \in \text{Im}(p) \setminus \{0\}$, ce qui assure que $\|p\| = 1$.

Théorème II.18.

Soit F un sous-espace vectoriel de E . Alors F possède un supplémentaire orthogonal si, et seulement si, il existe un projecteur orthogonal d'image F .

Preuve : (\Leftarrow) S'il existe un projecteur orthogonal p de E tel que $F = \text{Im}(p)$, alors un supplémentaire orthogonal de F est $\text{Ker}(p)$.

(\Rightarrow) Le projecteur sur F parallèlement à F^\perp est bien un projecteur orthogonal d'image F .

Proposition II.19.

Soit F un sous-espace vectoriel de E tel qu'il soit image d'un projecteur orthogonal p . Alors, pour tout $x \in E$,

$$d(x, F) = \|x - p(x)\|$$

et $p(x)$ est l'unique vecteur de F tel que cette égalité est vérifiée.

Preuve : Soit $y \in F = \text{Im}(p)$. $x - y = \underbrace{x - p(x)}_{\in F^\perp} + \underbrace{p(x) - y}_{\in F}$, donc

$$\|x - y\|^2 = \|x - p(x)\|^2 + \|p(x) - y\|^2 \geq \|x - p(x)\|^2$$

et ce minorant est réalisé si, et seulement si, $y = p(x)$ (car sinon, la norme ne serait pas séparante).

Théorème II.20.

Soit F un sous-espace vectoriel de E de dimension finie $d \geq 1$. Soit (e_1, \dots, e_d) une base orthonormée de F . Alors l'application

$$\begin{aligned} \pi : E &\longrightarrow F \\ x &\longmapsto \sum_{i=1}^d \langle e_i, x \rangle e_i \end{aligned}$$

est un projecteur orthogonal de E sur F et $E = F \oplus F^\perp$.

De plus, pour tout $x \in E$, $d(x, F)^2 = \|x\|^2 - \sum_{i=1}^d \langle e_i, x \rangle^2$.

Preuve : π est linéaire et $\text{Im}(\pi) = F$. En effet, pour tout $x \in F$, $x = \sum_{i=1}^d \langle x, e_i \rangle e_i = \pi(x)$.

Montrons que $\text{Ker}(\pi) \perp F$. Soit $x \in \text{Ker}(\pi)$. Alors, $0 = \pi(x) = \sum_{i=1}^d \langle x, e_i \rangle e_i$. Or (e_1, \dots, e_d) est libre, donc pour tout $i \in \llbracket 1; d \rrbracket$, $\langle e_i, x \rangle = 0$. Donc $\text{Ker}(\pi) \subset F^\perp$. Donc $\text{Ker}(\pi) = F^\perp$, et $E = F \oplus F^\perp$.

De plus, pour tout $x \in E$, $\|x\|^2 = \|x - \pi(x)\|^2 + \|\pi(x)\|^2 = d(x, F)^2 + \sum_{i=1}^d \langle x, e_i \rangle^2$.

 On prouve au passage l'inégalité de Bessel : pour toute famille orthonormée (e_1, \dots, e_d) de E , et pour tout $x \in E$,

$$\sum_{i=1}^d \langle x, e_i \rangle^2 \leq \|x\|^2$$

Caractérisation des projecteurs orthogonaux parmi les projecteurs

Soit $p \in \mathcal{L}(E)$ tel que $p^2 = p$. Montrons que p est orthogonal si, et seulement si, p est continu et $\|p\| \leq 1$.

Nous avons déjà démontré que si p est un projecteur orthogonal de E , alors $\|p\| = 1 \leq 1$, ce qui entraîne sa continuité.

Supposons que p soit continu et que $\|p\| \leq 1$.

Soit $(x, y) \in \text{Ker}(p) \times \text{Im}(p)$. Alors, pour tout $t \in \mathbb{R}$,

$$\|p(x + ty)\|^2 \leq \|x + ty\|^2 \quad \text{donc} \quad \|x\|^2 \leq \|x\|^2 + 2t \langle x, y \rangle + \|y\|^2 t^2$$

Donc pour tout $t > 0$, $2 \langle x, y \rangle + t \|y\|^2 \geq 0$, puis par passage à la limite, $t \rightarrow 0^+$, $\langle x, y \rangle \geq 0$.

De même, pour tout $t < 0$, $2 \langle x, y \rangle + t \|y\|^2 \leq 0$, puis par passage à la limite, $t \rightarrow 0^-$, $\langle x, y \rangle \leq 0$.

Donc $\langle x, y \rangle = 0$, donc $\text{Im}(p) \subset \text{Ker}(p)^\perp$. Ainsi, p admet un supplémentaire orthogonal dans E , ce qui assure que $\text{Im}(p) = \text{Ker}(p)^\perp$. Donc p est orthogonal.

Exercice II.21.

Soit $(E, \langle \cdot, \cdot \rangle)$ un espace préhilbertien réel, et notons $\|\cdot\|$ la norme euclidienne associée à $\langle \cdot, \cdot \rangle$.

Soient p et q deux projecteurs orthogonaux de E . Montrer que $p \circ q$ est un projecteur orthogonal de E si $p \circ q = q \circ p$.

Correction de l'exercice I.5. :

 On conjecture aisément que les points extrémaux sont ceux de la sphère unité.

→ Soit $x \in B(0, 1)$. Si $x = 0$ alors en fixant $a \in \overline{B}(0, 1) \setminus \{0\}$, $x = \frac{1}{2}(a - a)$ et pourtant $x \neq a$ et $x \neq -a$.

Si $x \neq 0$, alors $x = (1 - \|x\|) \cdot 0 + \|x\| \frac{x}{\|x\|}$ et pourtant $x \neq 0$ et $x \neq \frac{x}{\|x\|}$.

Donc les points de $B(0, 1)$ ne sont pas des points extrémaux de $\overline{B}(0, 1)$.

→ Soit $x \in S(0, 1)$. Soient $y, z \in C$. Supposons qu'il existe $t \in [0, 1]$ tel que $x = ty + (1 - t)z$. Si $t = 0$ ou $t = 1$, il n'y a rien à démontrer. Sinon, d'après l'inégalité triangulaire,

$$1 \leq t \|y\| + (1 - t) \|z\| \leq t + (1 - t) = 1$$

donc $t \|y\| + (1 - t) \|z\| = \|ty + (1 - t)z\|$. D'après le cas d'égalité de l'inégalité de Minkowski, il existe $\lambda \geq 0$ tel que $y = \lambda z$ ou $\lambda y = z$. Par ailleurs,

$$\underbrace{t(1 - \|y\|)}_{\geq 0} + \underbrace{(1 - t)(1 - \|z\|)}_{\geq 0} = 0$$

Donc $\|y\| = \|z\| = 1$, donc $\lambda = 1$. Donc $x = y$ ou $x = z$.

Donc $S(0, 1)$ est l'ensemble des points extrémaux de $B(0, 1)$.

Correction de l'exercice I.6. :

Introduisons l'application

 $\varphi : (x, y) \longmapsto \mathcal{N}(x + y)^2 - \mathcal{N}(x - y)^2$

définie sur $E \times E$. φ est clairement symétrique et définie positive. Il reste à montrer qu'elle est bilinéaire. Soient x, y et $z \in E$. D'après l'égalité de la médiane,

$$\begin{aligned} \varphi(x, y + z) &= 2(\mathcal{N}(x + y)^2 + \mathcal{N}(z)^2) - \mathcal{N}(x + y - z)^2 - \mathcal{N}(x - y - z)^2 \\ &= 2(\mathcal{N}(x + y)^2 + \mathcal{N}(z)^2) - 2(\mathcal{N}(x - z)^2 + \mathcal{N}(y)^2) \\ \varphi(-x, y + z) &= 2(\mathcal{N}(x - y)^2 + \mathcal{N}(z)^2) - \mathcal{N}(x - y + z)^2 - \mathcal{N}(x + y + z)^2 \\ &= 2(\mathcal{N}(x - y)^2 + \mathcal{N}(z)^2) - 2(\mathcal{N}(x + z)^2 + \mathcal{N}(y)^2) \end{aligned}$$

Or, $\varphi(-x, y + z) = -\varphi(x, y + z)$, donc en soustrayant membre à membre,

$$\varphi(x, y + z) = (\mathcal{N}(x + y)^2 - \mathcal{N}(x - y)^2) + (\mathcal{N}(x + z)^2 - \mathcal{N}(x - z)^2) = \varphi(x, y) + \varphi(x, z)$$

En remarquant que $\varphi(x, 0) = 0$, une récurrence immédiate permet de montrer que pour tout $n \in \mathbb{N}$,

$$\varphi(x, ny) = n\varphi(x, y)$$

Or, $\varphi(x, -y) = -\varphi(x, y)$, donc pour tout $m \in \mathbb{Z}$, $\varphi(x, my) = m\varphi(x, y)$.

Soit $r = \frac{p}{q} \in \mathbb{Q}$ tel que $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$. Alors

 $p\varphi(x, y) = \varphi(x, py) = \varphi(x, qry) = q\varphi(x, ry)$

donc $\varphi(x, ry) = \frac{p}{q}\varphi(x, y) = r\varphi(x, y)$ et ceci est valable pour tout rationnel r .

Enfin, soit $\lambda \in \mathbb{R}$. Par densité de \mathbb{Q} dans \mathbb{R} , il existe $(\lambda_n) \in \mathbb{Q}^{\mathbb{N}}$ tel que $\lambda_n \xrightarrow{n \rightarrow +\infty} \lambda$.

Or $u \mapsto \varphi(x, u)$ est continue, donc $\underbrace{\lambda_n \varphi(x, y)}_{n \rightarrow +\infty} = \varphi(x, \lambda_n y) \xrightarrow{n \rightarrow +\infty} \varphi(x, \lambda y)$, donc par unicité de la limite

$$\varphi(x, \lambda y) = \lambda \varphi(x, y)$$

et ceci est valable pour tout $\lambda \in \mathbb{R}$. Donc φ est linéaire selon la deuxième variable. Étant de plus symétrique, elle est bilinéaire. Donc φ est un produit scalaire sur E .

Correction de l'exercice II.3. :

Soit I un ensemble infini non dénombrable.

Raisonnons par l'absurde en supposant que $\ell^2(\mathbb{N}, \mathbb{R})$ admet une base orthonormée $(e^i) \in \ell^2(\mathbb{N}, \mathbb{R})^I$.

→ Montrons que $\ell^2(\mathbb{N}, \mathbb{R})$ est séparable, i.e. $\ell^2(\mathbb{N}, \mathbb{R})$ contient une partie dénombrable dense.

Soit $(x_n) \in \ell^2(\mathbb{N}, \mathbb{R})$. Soit $\varepsilon > 0$. Il existe $n_\varepsilon \in \mathbb{N}$ tel que $\sum_{n=n_\varepsilon+1}^{+\infty} x_n^2 \leq \frac{\varepsilon^2}{2}$.

Par ailleurs, pour tout $n \in \llbracket 0; n_\varepsilon \rrbracket$, il existe $a_n \in \mathbb{Q}$ tel que $|a_n - x_n| \leq \frac{\varepsilon}{\sqrt{2(n_\varepsilon + 1)}}$.

Prolongeons $(a_0, \dots, a_{n_\varepsilon})$ en une suite presque nulle $(a_n) \in \mathbb{Q}[X]$ en posant, pour tout entier $n > n_\varepsilon$, $a_n = 0$.

 Rappelons qu'on se donne une telle suite si, et seulement si, on se donne un polynôme à coefficients rationnels, d'où la notation commune des deux ensembles.

Ainsi,

$$\|(x_n)_{n \in \mathbb{N}} - (a_n)_{n \in \mathbb{N}}\|^2 = \sum_{n=1}^{n_\varepsilon} (x_n - a_n)^2 + \sum_{n=n_\varepsilon+1}^{+\infty} x_n^2 \leq \frac{\varepsilon^2}{2} + \frac{\varepsilon^2}{2} = \varepsilon^2$$

ce qui prouve que $\mathbb{Q}[X]$ est dense dans $\ell^2(\mathbb{N}, \mathbb{R})$.

→ $\mathbb{Q}[X]$ est dénombrable. En effet, $\mathbb{Q}[X] = \bigcup_{n=0}^{+\infty} \mathbb{Q}_n[X]$, et il est clair que pour tout $n \in \mathbb{N}$, $\mathbb{Q}_n[X]$ est en bijection avec \mathbb{Q}^{n+1} qui est dénombrable en tant que produit cartésien d'ensembles dénombrables.

→ Ainsi, pour tout $i \in I$, il existe $(a_n^i)_{n \in \mathbb{N}} \in \mathbb{Q}[X]$ telle que $\|(e_n^i)_{n \in \mathbb{N}} - (a_n^i)_{n \in \mathbb{N}}\| < \frac{1}{2}$. Soit $(i, j) \in \mathbb{N}^2$ tel que $a^i = a^j$. Alors,

$$\underbrace{\|(e_n^i)_{n \in \mathbb{N}} - (e_n^j)_{n \in \mathbb{N}}\|}_{=2\delta_{i,j}} \leq \|(e_n^i)_{n \in \mathbb{N}} - (a_n^i)_{n \in \mathbb{N}}\| + \|(e_n^j)_{n \in \mathbb{N}} - (a_n^j)_{n \in \mathbb{N}}\| < 1$$

donc $i = j$. Donc $i \mapsto (a_n^i)$ est une injection de I dans $\mathbb{Q}[X]$, donc I est dénombrable, ce qui est faux.

En conclusion, $\ell^2(\mathbb{N}, \mathbb{R})$ n'admet pas de base orthonormée.

Correction de l'exercice II.10. :

1. Supposons qu'il existe un hyperplan H de E tel que $\text{Vect}(e_1, \dots, e_m) \subset H$. Soit $u \in E \setminus \{0\}$ tel que $H^\perp = \mathbb{R}u$. Alors

$$\|u\|^2 = \sum_{i=1}^n \langle u, e_i \rangle = 0$$

ce qui est faux. Donc $E = \text{Vect}(e_1, \dots, e_m)$.

2. Considérons \mathbb{R}^2 muni de produit scalaire canonique, et posons $u_1 = (1, 0)$, $u_2 = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ et

$u_3 = \left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$. Alors, $\|u_1\| = \|u_2\| = \|u_3\|$. De plus, pour tout $x = (x_1, x_2) \in \mathbb{R}^2$,

$$\sum_{i=1}^3 \langle x, u_i \rangle^2 = x_1^2 + \left(-\frac{1}{2}x_1 + \frac{\sqrt{3}}{2}x_2\right)^2 + \left(-\frac{1}{2}x_1 - \frac{\sqrt{3}}{2}x_2\right)^2 = \frac{3}{2} \|x\|^2$$

donc en posant $(e_1, e_2, e_3) = \sqrt{\frac{2}{3}}(u_1, u_2, u_3)$, on a bien $\|e_1\| = \|e_2\| = \|e_3\|$, et

$$\sum_{i=1}^3 \langle x, e_i \rangle^2 = \|x\|^2$$

3. Soit $i \in \llbracket 1; n \rrbracket$. $\|e_i\|^2 = \sum_{j=1}^n \langle e_i, e_j \rangle^2 = \|e_i\|^4 + \underbrace{\sum_{\substack{j=1 \\ j \neq i}}^n \langle e_i, e_j \rangle^2}_{\geq 0}$, donc $\|e_i\|^2 \geq \|e_i\|^4$ donc $\|e_i\| \leq 1$.

Soit $u \in \text{Vect}((e_j)_{1 \leq j \neq i \leq n})^\perp$ tel que $\|u\| = 1$. Alors,

$$1 = \|u\|^2 = \langle e_i, u \rangle^2 \leq \|u\|^2 \|e_i\|^2 \leq \|e_i\|^2$$

\uparrow
Cauchy-Schwarz

Donc $\|e_i\| = 1$. Ainsi, $\chi = \|e_i\|^2 = \underbrace{\|e_i\|^4}_{=1} + \underbrace{\sum_{\substack{j=1 \\ j \neq i}}^n \langle e_i, e_j \rangle^2}_{\geq 0}$, donc $\sum_{\substack{j=1 \\ j \neq i}}^n \langle e_i, e_j \rangle^2 = 0$, donc pour tout $j \in \llbracket 1; n \rrbracket$ tel que $j \neq i$, $\langle e_i, e_j \rangle = 0$. Donc (e_1, \dots, e_n) est une base orthonormée de E .

Correction de l'exercice II.21. :

Si $p \circ q = q \circ p$, alors $(p \circ q)^2 = p \circ q \circ p \circ q = p \circ q \circ q \circ p = p \circ q \circ p = p \circ p \circ q = p \circ q$, donc $p \circ q$ est un projecteur. Or, $\|p \circ q\| \leq \|p\| \|q\| \leq 1$ donc $p \circ q$ est orthogonal.



COMPLÉMENTS

Espaces préhilbertiens réels, compléments

Dans tout le document, $(E, \langle \cdot, \cdot \rangle)$ désigne espace préhilbertien réel et on note $\|\cdot\|$ la norme associée au produit scalaire $\langle \cdot, \cdot \rangle$. De plus, n désigne un entier supérieur ou égal à 1.

I Décomposition de Cartan (Iwasawa)

Dans cette partie on suppose que E est de dimension finie n .

1. Changements de base, orientation

Rappel I.1.

Soient \mathcal{E} , \mathcal{F} , et \mathcal{G} des bases de E .

- La matrice de passage de \mathcal{E} à \mathcal{F} est la matrice $[\mathcal{F}]_{\mathcal{E}}$ de $\mathcal{M}_n(\mathbb{R})$ telle que, pour tout $k \in \llbracket 1; n \rrbracket$, la k -ième colonne de $[\mathcal{F}]_{\mathcal{E}}$ est la représentation du k -ième vecteur de \mathcal{F} dans la base \mathcal{E} .
- $[\mathcal{F}]_{\mathcal{E}}[\mathcal{G}]_{\mathcal{F}}$ est la matrice de passage de \mathcal{E} à \mathcal{G} : elle vaut $[\mathcal{G}]_{\mathcal{E}}$.

Définition I.2.

Soient \mathcal{E} et \mathcal{F} deux bases de E . On dit que \mathcal{E} et \mathcal{F} ont la même orientation, et on note $\mathcal{E} \sim \mathcal{F}$, lorsque

$$\det_{\mathcal{E}}(\mathcal{F}) := \det([\mathcal{F}]_{\mathcal{E}}) > 0$$

Proposition I.3.

\sim est une relation d'équivalence possédant exactement deux classes.

Preuve : Soit $\mathcal{E} = (e_1, \dots, e_n)$ une base de E . On a

$$\det_{\mathcal{E}}(-e_1, e_2, \dots, e_n) = \begin{vmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{vmatrix} = -1 < 0$$

Donc $\mathcal{E} \not\sim \underbrace{(-e_1, e_2, \dots, e_n)}_{\text{notée } \tilde{\mathcal{E}}}.$ Donc \sim admet au moins deux classes d'équivalence.

Soit \mathcal{F} une base de E .

- Si $\det_{\mathcal{E}}(\mathcal{F}) > 0$, alors on a $\mathcal{F} \in \overline{\mathcal{E}}$.

- Sinon, $\det_{\mathcal{E}}(\mathcal{F}) < 0$. Or $[\mathcal{F}]_{\tilde{\mathcal{E}}} = [\mathcal{E}]_{\tilde{\mathcal{E}}}[\mathcal{F}]_{\mathcal{E}} = \begin{pmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} [\mathcal{F}]_{\mathcal{E}}$ donc $\det_{\tilde{\mathcal{E}}}(\mathcal{F}) = -\det_{\mathcal{E}}(\mathcal{F}) > 0$,

i.e. $\mathcal{F} \in \overline{\mathcal{E}}$.

On en déduit que les deux seules classes d'équivalences sont celles de \mathcal{E} et $\tilde{\mathcal{E}}$.

Dans la suite de cette partie, E est associé à l'une de ses bases orthonormées \mathcal{E} . On dit alors que E est orienté.

Définition I.4.

Soit \mathcal{F} une base de E . On dit que \mathcal{F} est positive ou directe dans E lorsque $\mathcal{F} \in \overline{\mathcal{E}}$.

Dans le cas contraire, \mathcal{F} est négative ou indirecte.

Proposition I.5.

Soient \mathcal{F} une base orthonormée de E et $(x_1, \dots, x_n) \in E^n$

→ Si \mathcal{F} est directe, alors $\det_{\mathcal{F}}(x_1, \dots, x_n) = \det_{\mathcal{E}}(x_1, \dots, x_n)$.

→ Si \mathcal{F} est indirecte, alors $\det_{\mathcal{F}}(x_1, \dots, x_n) = -\det_{\mathcal{E}}(x_1, \dots, x_n)$

Preuves :

→ On pose $P = [\mathcal{F}]_{\mathcal{E}}$ et, pour tout $i \in \llbracket 1; n \rrbracket$, $X_i = [x_i]_{\mathcal{E}}$ et $X'_i = [x_i]_{\mathcal{F}}$. Ainsi, pour tout $i \in \llbracket 1; n \rrbracket$, $X_i = PX'_i$. Donc

$$\det_{\mathcal{E}}(x_1, \dots, x_n) = \det(X_1, \dots, X_n) = \det(PX'_1, \dots, PX'_n) = \underbrace{\det(P)}_{=1} \det(X'_1, \dots, X'_n) = \det_{\mathcal{F}}(x_1, \dots, x_n)$$

car P est une matrice orthogonale et \mathcal{F} est orientée positivement (relativement à \mathcal{E}).

→ Le calcul est identique, seulement $\det(P) = -1$ car P est orthogonale et orientée négativement (relativement à \mathcal{E}).

Proposition I.6.

On suppose que $n = 3$. Soit $(x, y) \in E^2$. Il existe un unique $w \in E$ vérifiant la propriété

$$\forall z \in E, \det_{\mathcal{E}}(x, y, z) = \langle w, z \rangle$$

w est le produit vectoriel de x et y et est noté $x \wedge y$.

Preuve : On considère la forme linéaire $\varphi : z \mapsto \det_{\mathcal{E}}(x, y, z)$. D'après le théorème à la page 4 du chapitre sur les espaces préhilbertien réels, il existe un unique vecteur w tel que $\varphi = \langle w, \cdot \rangle$, ce qu'on voulait.

Remarque : Comme en physique, les coordonnées de w s'obtiennent à partir des coordonnées de x et y :

$$w_1 = \begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix} \quad w_2 = \begin{vmatrix} x_3 & y_3 \\ x_1 & y_1 \end{vmatrix} \quad w_3 = \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}$$

Exercice I.7.

Soit $(E, \langle \cdot, \cdot \rangle)$ un espace euclidien de dimension 3.

Montrer que pour tous $a, b, c \in E$

$$a \wedge (b \wedge c) = \langle a, c \rangle b - \langle a, b \rangle c$$

2. Décomposition de Cartan

On note $\mathcal{T}_n^+(\mathbb{R})$ l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$ qui sont triangulaires supérieures et dont les coefficients diagonaux sont strictement positifs.

Proposition I.8.

Soit $A \in \mathrm{GL}_n(\mathbb{R})$. Il existe un unique couple $(O, T) \in \mathcal{O}_n(\mathbb{R}) \times \mathcal{T}_n^+(\mathbb{R})$ tel que $A = OT$.

Preuves

→ Unicité

S'il existe deux tels couples (O_1, T_1) et (O_2, T_2) alors $O_1 T_1 = O_2 T_2$, donc $O_1^{-1} O_2 = T_1 T_2^{-1}$.

$U := O_1^{-1} O_2$ est orthogonale, triangulaire supérieure à coefficients diagonaux strictement positifs, car l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$ inversibles et triangulaires supérieures est un sous-groupe de $(\mathrm{GL}_n(\mathbb{R}), \times)$.

Or, $U^\top = U^{-1} = (T_1 T_2^{-1})^{-1} = T_2 T_1^{-1} \in \mathcal{T}_n^+(\mathbb{R})$. Donc U^\top est aussi triangulaire supérieure à coefficients diagonaux strictement positifs.

Donc U est diagonale et à coefficients strictement positifs. On en déduit que $U = I_n$, donc $O_1 = O_2$ et $T_1 = T_2$.

→ Existence

Notons $\mathcal{A} = (A_1, \dots, A_n)$ la base de $\mathcal{M}_{n,1}(\mathbb{R})$ donnée par les colonnes de A , et \mathcal{F} une base de $\mathcal{M}_{n,1}(\mathbb{R})$ obtenue à l'aide du procédé de Gram-Schmidt appliqué à \mathcal{A} .

Quitte à échanger certains vecteurs de \mathcal{F} par leurs opposés, le théorème de Gram-Schmidt assure que $T := [\mathcal{F}]_{\mathcal{A}}$ est triangulaire supérieure et ses coefficients diagonaux sont strictement positifs.

Posons $O = [\mathcal{F}]_{\mathrm{Can}(\mathcal{M}_{n,1}(\mathbb{R}))}$. Alors, $AT = O$ car $A = [\mathcal{A}]_{\mathrm{Can}(\mathcal{M}_{n,1}(\mathbb{R}))}$. Ainsi $A = OT^{-1}$.

Exercice I.9.

Soit $n \in \mathbb{N}^*$. Montrer que

$$\begin{aligned} f : \mathcal{O}_n(\mathbb{R}) \times \mathcal{T}_n^+(\mathbb{R}) &\longrightarrow \mathrm{GL}_n(\mathbb{R}) \\ (O, T) &\longmapsto OT \end{aligned}$$

est un homéomorphisme.

Exercice I.10.

Soit $n \in \mathbb{N}^*$. On note $\mathrm{GL}_n^+(\mathbb{R})$ l'ensemble des matrices inversibles de déterminant strictement positif.

Montrer que $\mathrm{GL}_n^+(\mathbb{R})$ est connexe.

3. Inégalité de Hadamard

Exercice I.11.

Soit $(E, \langle \cdot, \cdot \rangle)$ un espace euclidien de dimension n orienté par l'une de ses bases orthonormées \mathcal{E} . Soit $(x_1, \dots, x_n) \in E^n$. Montrer que

$$\left| \det_{\mathcal{E}}(x_1, \dots, x_n) \right| \leq \prod_{k=1}^n \|x_k\|$$

Montrer de plus qu'il y a égalité si, et seulement si, (x_1, \dots, x_n) est orthogonale.

II Matrices de Gram

On rappelle que $(E, \langle \cdot, \cdot \rangle)$ un espace préhilbertien réel.

Définition II.1.

Soit $(x_1, \dots, x_n) \in E^n$. On appelle matrice de Gram associée à (x_1, \dots, x_n) la matrice

$$G(x_1, \dots, x_n) = (\langle x_i, x_j \rangle)_{1 \leq i, j \leq n}$$

On note aussi $|G|(x_1, \dots, x_n)$ le déterminant de cette matrice de Gram.

Proposition II.2.

Soit $(x_1, \dots, x_n) \in E^n$.

→ Soit $(\varepsilon_1, \dots, \varepsilon_n)$ un système orthonormé tel que $x_1, \dots, x_p \in \text{Vect}(\varepsilon_1, \dots, \varepsilon_n)$. Notons $A = [(x_1, \dots, x_n)]_{(\varepsilon_1, \dots, \varepsilon_n)}$. Alors,

$$G(x_1, \dots, x_n) = A^\top A$$

→ $|G|(x_1, \dots, x_n) > 0$ si, et seulement si, (x_1, \dots, x_n) est libre.

→ Notons M la matrice $G(x_1, \dots, x_n)$. Pour tout $\Lambda = (\lambda_k)_{1 \leq k \leq n} \in \mathcal{M}_{n,1}(\mathbb{R})$,

$$\|\lambda_1 x_1 + \dots + \lambda_n x_n\|^2 = \Lambda^\top M \Lambda$$

→ Pour tout $\lambda \in \text{Sp}(M)$, $\lambda \geq 0$.

→ On suppose E de dimension finie. Soient $(x_1, \dots, x_n) \in E^n$ et $(y_1, \dots, y_n) \in E^n$. On a l'équivalence

$$G(x_1, \dots, x_n) = G(y_1, \dots, y_n) \iff \exists u \in \mathcal{O}(E), \quad \forall i \in \llbracket 1; n \rrbracket, \quad u(x_i) = y_i$$

Preuves

→ On note A_1, \dots, A_n les colonnes de A . Alors

$$A^\top A = [A_i^\top A_j]_{1 \leq i, j \leq n} = (\langle x_i, x_j \rangle)_{1 \leq i, j \leq n} = G(x_1, \dots, x_n)$$

→ D'après la proposition précédente, $|G|(x_1, \dots, x_p) = \det(A^\top A) = (\det(A))^2 > 0$ donc $\det(A) = 0$, d'où l'équivalence.

→ On rappelle une identité classique :

$$\forall M = (m_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{C}), \forall x = (x_k)_{1 \leq k \leq n} \in \mathcal{M}_{n,1}(\mathbb{C}), \quad X^\top MX = \sum_{1 \leq i,j \leq n} x_i x_j m_{i,j}$$

$$\text{Ainsi } \|\lambda_1 x_1 + \cdots + \lambda_n x_n\|^2 = \sum_{1 \leq i,j \leq n} \lambda_i \lambda_j \langle x_i, x_j \rangle = {}^t \Lambda M \Lambda.$$

→ Il existe $\Lambda \in \mathcal{M}_{n,1}(\mathbb{R})$ tel que $M\Lambda = \lambda\Lambda$, donc $\Lambda^\top M\Lambda = \lambda\Lambda^\top\Lambda$ et d'après la proposition précédente

$$\|\lambda_1 x_1 + \cdots + \lambda_n x_n\|^2 = \Lambda^\top M\Lambda = \mu(\lambda_1^2 + \cdots + \lambda_p^2)$$

Donc $\lambda \geq 0$.

→ (\Leftarrow) Supposons qu'un tel u existe. Alors on a pour tout $i, j \in \llbracket 1; n \rrbracket$,

$$\begin{aligned} \langle y_i, y_j \rangle &= \langle u(x_i), u(x_j) \rangle = \langle x_i, x_j \rangle \\ &\quad \uparrow \\ &\quad u \text{ conserve le produit scalaire} \end{aligned}$$

donc les deux matrices de Gram sont égales.

(\Rightarrow) Remarquons que l'implication est vraie si tous les x_i (et donc tous les y_i) sont nuls. Supposons que les x_i ne sont pas tous nuls.

À l'aide d'une permutation σ de $\llbracket 1; n \rrbracket$, permutons les x_i de sorte à considérer l'entier naturel non nul $r \leq n$ tel que $(x_{\sigma(1)}, \dots, x_{\sigma(r)})$ soit libre et $x_{\sigma(r+1)}, \dots, x_{\sigma(n)} \in \underbrace{\text{Vect}(x_{\sigma(1)}, \dots, x_{\sigma(r)})}_{\text{noté } A}$.

Posons, pour tout $i \in \llbracket 1; r \rrbracket$, $a_i = x_{\sigma(i)}$ et $b_i = y_{\sigma(i)}$. Alors

(i) D'après la deuxième proposition, (b_1, \dots, b_r) est libre car $|G|(b_1, \dots, b_r) = |G|(a_1, \dots, a_r) > 0$.

(ii) Pour tout entier $k \geq r+1$,

$$\begin{aligned} |G|(b_1, \dots, b_r, y_{\sigma(k)}) &= |G|(a_1, \dots, a_r, x_{\sigma(k)}) = 0 \\ &\quad \uparrow \quad \uparrow \\ &\quad \text{égalité des matrices de Gram} \quad \text{deuxième proposition} \end{aligned}$$

$$\text{donc } y_{\sigma(k)} \in \underbrace{\text{Vect}(b_1, \dots, b_r)}_{\text{noté } B}.$$

Notons p la dimension de E . Si $r < p$, introduisons les systèmes orthonormés (a_{r+1}, \dots, a_p) et (b_{r+1}, \dots, b_p) de sorte que les familles (a_1, \dots, a_p) et (b_1, \dots, b_p) soient des bases adaptées aux décompositions $E = A \oplus A^\perp$ et $E = B \oplus B^\perp$.

On considère $u \in \mathcal{L}(E)$ tel que pour tout $i \in \llbracket 1; n \rrbracket$, $u(a_i) = b_i$.

u est une isométrie sur E . En effet, pour tout $x \in E$, il existe $\Lambda = (\lambda_k)_{1 \leq k \leq n} \in \mathcal{M}_{r,1}(\mathbb{R})$ et $(\lambda_{r+1}, \dots, \lambda_p) \in \mathbb{R}^{p-r}$ tel que $x = \lambda_1 a_1 + \cdots + \lambda_p a_p$, et

$$\|x\|^2 = \|\lambda_1 a_1 + \cdots + \lambda_r a_r\|^2 + \sum_{i=r+1}^n \lambda_i^2 \|a_i\|^2 \quad (\text{Pythagore})$$

$$= \Lambda^\top G(a_1, \dots, a_r) \Lambda + \sum_{i=r+1}^n \lambda_i^2 \|b_i\|^2 \quad (\text{troisième proposition})$$

$$= \Lambda^\top G(b_1, \dots, b_r) \Lambda + \|\lambda_{r+1} u(a_{r+1}) + \cdots + \lambda_p u(a_p)\|^2$$

$$= \|\lambda_1 b_1 + \cdots + \lambda_r b_r\|^2 + \|\lambda_{r+1} u(a_{r+1}) + \cdots + \lambda_p u(a_p)\|^2 \quad (\text{troisième proposition})$$

$$= \|u(x)\|^2 \quad (\text{Pythagore})$$

Par ailleurs, pour tout $k \in \llbracket r+1; n \rrbracket$, et pour tout $i \in \llbracket 1; r \rrbracket$

$$\begin{aligned} \langle u(x_{\sigma(k)}) - y_{\sigma(k)}, b_i \rangle &= \langle u(x_{\sigma(k)}), b_i \rangle - \langle y_{\sigma(k)}, b_i \rangle = \underbrace{\langle x_{\sigma(k)}, a_i \rangle}_{u \text{ conserve le produit scalaire}} - \underbrace{\langle y_{\sigma(k)}, b_i \rangle}_{\text{égalité des matrices de Gram}} = 0 \end{aligned}$$

Ainsi, pour tout $k \in \llbracket r+1; n \rrbracket$, $u(x_{\sigma(k)}) - y_{\sigma(k)} \perp B$ et $u(x_{\sigma(k)}) - y_{\sigma(k)} \in B$, donc $u(x_{\sigma(k)}) - y_{\sigma(k)} = 0$.
Donc, pour tout $i \in \llbracket 1; n \rrbracket$ $u(x_i) = y_i$.

Exercice II.3.

Soit $(E, \langle \cdot, \cdot \rangle)$ un espace préhilbertien réel. On suppose que (x_1, \dots, x_n) est libre dans E et on pose $F = \text{Vect}(x_1, \dots, x_n)$. Soit $a \in E$.

Montrer que

$$d(a, F)^2 = \frac{|G|(a, x_1, \dots, x_p)}{|G|(x_1, \dots, x_p)}$$

Correction de l'exercice I.7. :

Soit \mathcal{E} une base orthonormée de E qui détermine le sens direct. On note (a_1, a_2, a_3) , (b_1, b_2, b_3) , et (c_1, c_2, c_3) les coordonnées respectives de a , b et c dans cette base.

$$\text{Calculons : } [b \wedge c]_{\mathcal{E}} = \begin{pmatrix} b_2 c_3 - b_3 c_2 \\ b_3 c_1 - b_1 c_3 \\ b_1 c_2 - b_2 c_1 \end{pmatrix}, \text{ puis } [a \wedge (b \wedge c)]_{\mathcal{E}} = \begin{pmatrix} a_2(b_1 c_2 - b_2 c_1) - a_3(b_3 c_1 - b_1 c_3) \\ a_3(b_2 c_3 - b_3 c_2) - a_1(b_1 c_2 - b_2 c_1) \\ a_1(b_3 c_1 - b_1 c_3) - a_2(b_2 c_3 - b_3 c_2) \end{pmatrix}.$$

$$\text{Par ailleurs : } [\langle a, c \rangle b - \langle a, b \rangle c]_{\mathcal{E}} = \begin{pmatrix} (a_1 e_1 + a_2 c_2 + a_3 c_3)b_1 - (a_1 b_1 + a_2 b_2 + a_3 b_3)c_1 \\ (a_1 c_1 + a_2 e_2 + a_3 c_3)b_2 - (a_1 b_1 + a_2 b_2 + a_3 b_3)c_2 \\ (a_1 c_1 + a_2 c_2 + a_3 e_3)b_3 - (a_1 b_1 + a_2 b_2 + a_3 b_3)c_3 \end{pmatrix}.$$

En factorisant par le couple de coordonnées de a qui apparaît dans chaque ligne, ou en développant chaque ligne des deux résultats, on obtient que les deux colonnes sont égales.

Correction de l'exercice I.9. :

Il s'agit de montrer que :

- f est continue : c'est vrai par continuité du produit matriciel.
- f est bijective : c'est vrai d'après la décomposition de Cartan.
- f^{-1} est continue : c'est le plat de résistance de l'exercice.

Soit $M \in \text{GL}_n(\mathbb{R})$.

Considérons une suite $(M_m)_{m \in \mathbb{N}}$ à valeurs dans $\text{GL}_n(\mathbb{R})$ convergeant vers $M \in \text{GL}_n(\mathbb{R})$, et montrons que $f^{-1}(M_m) \xrightarrow[m \rightarrow +\infty]{} f^{-1}(M)$.

Introduisons la décomposition de Cartan $(O, T) \in \mathcal{O}_n(\mathbb{R}) \times \mathcal{T}_n^+(\mathbb{R})$ de M , et pour tout $m \in \mathbb{N}$, la décomposition de Cartan $(O_m, T_m) \in \mathcal{O}_n(\mathbb{R}) \times \mathcal{T}_n^+(\mathbb{R})$ de M_m .

Rappelons que $\mathcal{O}_n(\mathbb{R})$ est compact : il est fermé (c'est l'image réciproque du fermé $\{I_n\}$ par l'application continue $X \mapsto X^\top X$) et borné car tous les coefficients d'une matrice orthogonale sont majorés par 1 en valeur absolue.

Ainsi, de $(O_m)_{m \in \mathbb{N}}$ on peut extraire une sous-suite $(O_{\varphi(m)})_{m \in \mathbb{N}}$ convergeant vers $\tilde{O} \in \mathcal{O}_n(\mathbb{R})$.

Pour tout $m \in \mathbb{N}$, $T_{\varphi(m)} = (O_{\varphi(m)})^{-1} M_{\varphi(m)} \xrightarrow[m \rightarrow +\infty]{} \tilde{O}^{-1} M$.

Or $\tilde{T} := \tilde{O}^{-1} M$ est aussi triangulaire supérieure à coefficients diagonaux positifs, car l'ensemble des matrices triangulaires supérieures à coefficients diagonaux positifs est fermé.

Ainsi, $M = \tilde{O}\tilde{T}$ et $(\tilde{O}, \tilde{T}) \in \mathcal{O}_n(\mathbb{R}) \times \mathcal{T}_n^+(\mathbb{R})$. Par unicité de la décomposition de Cartan de M , $O = \tilde{O}$ et $T = \tilde{T}$.

Remarquons alors que toute extraction convergente de la suite $(O_m)_{m \in \mathbb{N}}$ exhibe une unique valeur d'adhérence pour cette suite, et cette valeur est O .

Cette suite est à valeurs dans un compact et admet une unique valeur d'adhérence, c'est donc une suite convergente de limite O .

Ainsi, $T_m = O_m^{-1} M_m \xrightarrow[m \rightarrow +\infty]{} O^{-1} M = T$. Donc,

$$f^{-1}(M_m) = (O_m, T_m) \xrightarrow[m \rightarrow +\infty]{} (O, T) = f^{-1}(M)$$

ce qui prouve la continuité de f^{-1} .

Correction de l'exercice I.10. :

L'application

$$\begin{aligned} f : \mathcal{SO}_n(\mathbb{R}) \times \mathcal{T}_n^+(\mathbb{R}) &\longrightarrow \text{GL}_n^+(\mathbb{R}) \\ (O, T) &\longmapsto OT \end{aligned}$$

est continue (car le produit matriciel l'est) et surjective : pour toute $M \in \text{GL}_n^+(\mathbb{R})$, la décomposition de Cartan donne un couple $(O, T) \in \mathcal{O}_n(\mathbb{R}) \times \mathcal{T}_n^+(\mathbb{R})$ tel que $OT = M$, mais en fait, $O \in \mathcal{SO}_n(\mathbb{R})$ car sinon,

le déterminant de M serait négatif, celui de T étant positif.

Par ailleurs, $\mathcal{SO}_n(\mathbb{R})$ est connexe (*cf. chapitre 35*) et $\mathcal{T}_n^+(\mathbb{R})$ est connexe car convexe, donc leur produit cartésien est connexe.

$\mathrm{GL}_n^+(\mathbb{R})$ est donc connexe en tant qu'image d'un connexe par une fonction continue.

Correction de l'exercice I.11. :

On pose $M = [x_1, \dots, x_n]_{\mathcal{E}}$. Remarquons que les colonnes de M sont les colonnes X_i représentatives des vecteurs x_i .

→ Si (X_1, \dots, X_n) est liée, $\det M = 0$ donc l'inégalité est vraie.

→ Sinon, remarquons que M est la matrice de passage de la base canonique de $\mathcal{M}_{n,1}(\mathbb{R})$ à $\mathcal{X} := (X_1, \dots, X_n)$.

Notons $\mathcal{U} = (U_1, \dots, U_n)$ une base orthonormée de $\mathcal{M}_{n,1}(\mathbb{R})$ donnée par le procédé de Gram-Schmidt, puis T la matrice de passage de \mathcal{U} à \mathcal{X} . D'après le théorème de Gram-Schmidt, T est triangulaire supérieure. Ses colonnes étant les représentations des vecteurs de \mathcal{X} dans \mathcal{U} qui est orthonormée, pour tout $i \in \llbracket 1; n \rrbracket$, le i -ème coefficient diagonal de T est $U_i^\top X_i$.

Ainsi, en notant U la matrice de passage de la base canonique de $\mathcal{M}_{n,1}(\mathbb{R})$ à \mathcal{U} ,

$$|\det(M)| = |\det(UT)| = |\det(T)| = \prod_{k=1}^n \left| U_k^\top X_k \right| \stackrel{\text{Cauchy-Schwarz}}{\leq} \prod_{k=1}^n \sqrt{X_k^\top X_k} \underbrace{\sqrt{U_k^\top U_k}}_{=1} = \prod_{k=1}^n \sqrt{X_k^\top X_k}$$

Correction de l'exercice II.3. :

Introduisons la décomposition $a = u + v$ adaptée à $E = F \oplus F^\perp$.

$$\begin{aligned} |G|(a, x_1, \dots, x_p) &= \left| \begin{array}{cccc} \langle a, a \rangle & \overbrace{\langle a, x_1 \rangle \dots \langle a, x_p \rangle}^{\text{ligne notée } L} \\ \langle x_1, a \rangle & \langle x_1, x_1 \rangle \dots \langle x_1, x_p \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle x_p, a \rangle & \langle x_p, x_1 \rangle \dots \langle x_p, x_p \rangle \end{array} \right| \\ &= \left| \begin{array}{cc} \|u\|^2 + \|v\|^2 & L \\ L^\top & G(x_1, \dots, x_n) \end{array} \right| \\ &= \left| \begin{array}{cc} \|v\|^2 & L \\ 0 & G(x_1, \dots, x_n) \end{array} \right| + \left| \begin{array}{cc} \|u\|^2 & L \\ L^\top & G(x_1, \dots, x_n) \end{array} \right| \\ &= \|v\|^2 |G|(x_1, \dots, x_p) + \underbrace{|G|(u, x_1, \dots, x_p)}_{=0 \text{ car } (u, x_1, \dots, x_p) \text{ est liée}} \\ &= d(a, F)^2 |G|(x_1, \dots, x_p) \end{aligned}$$



CHAPITRE 36

Espaces préhilbertiens complexes

Dans tout ce chapitre, E désigne un \mathbb{C} -espace vectoriel non trivial et n désigne un entier supérieur ou égal à 1.

I Espaces hermitiens

Définition I.1.

Une application $\langle \cdot, \cdot \rangle : E^2 \rightarrow \mathbb{C}$ est un produit scalaire hermitien si

- Pour tout $x \in E$, $y \mapsto \langle x, y \rangle$ est \mathbb{C} -linéaire.
- Pour tout $y \in E$, $x \mapsto \langle x, y \rangle$ est semi-linéaire, i.e. pour tout $\lambda \in \mathbb{C}$ et pour tout $x \in E$,

$$\langle \lambda x, y \rangle = \bar{\lambda} \langle x, y \rangle$$

- Pour tout $(x, y) \in E^2$, $\langle x, y \rangle = \overline{\langle y, x \rangle}$
- Pour tout $x \in E \setminus \{0\}$, $\langle x, x \rangle \in \mathbb{R}^{+*}$

Dorénavant, E est muni d'un produit scalaire hermitien $\langle \cdot, \cdot \rangle$. On dit que $(E, \langle \cdot, \cdot \rangle)$ est un espace préhilbertien complexe ou encore un espace hermitien. On notera également $\|\cdot\|$ la norme associée à ce produit scalaire : pour tout $x \in E$, $\|x\| = \sqrt{\langle x, x \rangle}$.

Identités remarquables I.2.

Les identités remarquables sur un espace préhilbertien complexe sont différentes de celles sur un espace préhilbertien réel. Si la norme est toujours réelle, le produit scalaire peut ne pas l'être. Ainsi, pour tous $x, y \in E$,

$$\begin{aligned} \|x + y\|^2 &= \|x\|^2 + 2 \operatorname{Re}(\langle x, y \rangle) + \|y\|^2 & \|x - iy\|^2 &= \|x\|^2 + 2 \operatorname{Im}(\langle x, y \rangle) + \|y\|^2 \\ \|x - y\|^2 &= \|x\|^2 - 2 \operatorname{Re}(\langle x, y \rangle) + \|y\|^2 & \|x + iy\|^2 &= \|x\|^2 - 2 \operatorname{Im}(\langle x, y \rangle) + \|y\|^2 \\ \langle x, y \rangle &= \frac{1}{4} \left(\|x + y\|^2 - \|x - y\|^2 + i (\|x - iy\|^2 - \|x + iy\|^2) \right) \end{aligned}$$

↑
identité de polarisation

Quelques produits scalaires usuels

- $E = \mathbb{C}$, et $\langle \cdot, \cdot \rangle : (z, w) \mapsto \bar{z}w$
- $E = \mathbb{C}^n$, $\langle \cdot, \cdot \rangle : (z, w) \mapsto \sum_{k=0}^n \bar{z}_k w_k$
- $E = \mathcal{M}_n(\mathbb{C})$, $\langle \cdot, \cdot \rangle : (A, B) \mapsto \operatorname{Tr}({}^t \bar{A} B)$
- $E = \mathcal{C}_{2\pi}(\mathbb{R}, \mathbb{C})$, $\langle \cdot, \cdot \rangle : (f, g) \mapsto \int_0^{2\pi} \bar{f}g$ où $\mathcal{C}_{2\pi}(\mathbb{R}, \mathbb{C})$ est le sous-espace de $\mathcal{C}^0(\mathbb{R}, \mathbb{C})$ ne contenant que des fonctions 2π -périodiques.

Proposition I.3.

L'inégalité de Cauchy-Schwarz est valide sur l'espace préhilbertien complexe E :

$$\forall (x, y) \in E, |\langle x, y \rangle| \leq \|x\|^2 \|y\|^2$$

 **Preuve :** On suppose que $y \neq 0$. Soit $\theta \in \mathbb{R}$ vérifiant $e^{i\theta} \langle x, y \rangle = |\langle x, y \rangle|$. Pour tout $t \in \mathbb{R}$, posons

$$\varphi(t) = \|x + te^{i\theta}y\|^2$$

Alors, pour tout $t \in \mathbb{R}$,

$$\varphi(t) = \|x\|^2 + 2 \operatorname{Re} \langle x, te^{i\theta}y \rangle + t^2 \|y\|^2 = \|x\|^2 + 2t |\langle x, y \rangle| + t^2 \|y\|^2$$

Ainsi, φ est une fonction polynomiale de degré 2 et positive, donc son discriminant est négatif ou nul. Or, celui-ci vaut $4|\langle x, y \rangle|^2 - 4\|x\|^2\|y\|^2$, ce qu'on voulait.

 Nombre de notions relatives aux espaces préhilbertiens réels définies en première année et au chapitre 34 sont toujours valables sur un espace préhilbertien complexe. Plus précisément :

- La notion d'orthogonalité se définit de la même manière sur E que sur un espace préhilbertien réel : produit scalaire nul. On peut donc considérer des familles orthogonales ou orthonormées de E , ainsi que l'orthogonal d'une partie de E ou deux parties orthogonales de E , de même qu'un vecteur normal à un hyperplan de E .
- L'inégalité de Minkowski, le théorème de Pythagore et l'égalité de la médiane sont toujours valides sur E .
- Si F est un sous-espace vectoriel de dimension finie de E , on a toujours $E = F \oplus F^\perp$.
- E possède des bases orthonormées.
- Les formules de projections orthogonales sont toujours valables.
- L'inégalité de Bessel est toujours valable.
- Le procédé de Gram-Schmidt appliqué à une base de E donne une base orthonormée de E .

Avertissement I.4.

Soit F un sous-espace vectoriel de E de dimension finie n et (e_1, \dots, e_n) une base orthonormée de F . Soit $x \in E$. Le projeté de x sur F s'écrit toujours

$$\sum_{k=1}^n \langle e_k, x \rangle e_k$$

Le **vecteur à projeter** est dans la **case de droite** du produit scalaire hermitien. Tout fonctionne identiquement au cas réel pour les projections, le procédé de Gram-Schmidt et l'inégalité de Bessel à condition de ne pas négliger ce petit détail.

Remarque I.5.

On suppose que E est de dimension finie n .

Soit (e_1, \dots, e_n) une base orthonormée de E . Soient $\lambda_1, \dots, \lambda_n \in \mathbb{C}$. Considérons l'hyperplan de E défini par $H = \left\{ x := \sum_{k=1}^n x_k e_k \mid \lambda_1 x_1 + \dots + \lambda_n x_n = 0 \right\}$. Alors $y := \sum_{k=1}^n \overline{\lambda_k} e_k$ est un vecteur normal à H .

Exercice I.6.

Soit G un groupe fini d'ordre n . On pose $E = \mathcal{F}(G, \mathbb{C})$.

On considère le produit scalaire hermitien sur E vérifiant, pour tous x et y dans E ,

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{a \in G} \overline{f(a)} g(a)$$

On dit que χ est un caractère de G si $\chi \in \text{Hom}(G, \mathbb{C}^*)$.

1. Montrer que tout caractère de G est à valeurs dans \mathbb{U}_n .
2. Montrer que si Φ est un caractère non constant, alors $\sum_{a \in G} \Phi(a) = 0$.
3. Montrer que si χ et ψ sont deux caractères distincts, alors ils sont orthogonaux et que $\|\chi\|^2 = 1$.

II Opérations unitaires

Définition II.1.

Soit $u \in \mathcal{L}(E)$. On dit que u est unitaire lorsque pour tout $x \in E$,

$$\|u(x)\| = \|x\|$$

On note $\mathcal{U}(E)$ l'ensemble de tels endomorphismes.



On dit qu'un endomorphisme unitaire u de E préserve la norme. De plus, en vertu de l'identité de polarisation, il préserve aussi le produit scalaire *i.e.* pour tous $x, y \in E$,

$$\langle u(x), u(y) \rangle = \langle x, y \rangle$$

Proposition II.2.

Soit $u \in \mathcal{U}(E)$ et $v \in \mathcal{L}(E)$.

- $(\mathcal{U}(E), \circ)$ est un sous-groupe de $\text{GL}(E)$.
- Si E est de dimension finie n et (e_1, \dots, e_n) est une base orthonormée de E , alors v est unitaire si, et seulement si, $(v(e_1), \dots, v(e_n))$ est une base orthonormée de E .
- F est stable par u si, et seulement si, F^\perp est stable par u
- v est unitaire si, et seulement si, v est diagonalisable en base orthonormée et $\text{Sp}(u) \subset \mathbb{U}$.

Notation : Soit $U \in \mathcal{M}_n(\mathbb{C})$. On note U^* , et on appelle matrice adjointe, la matrice \bar{U}^\top .

Définition II.3.

Soit $U \in \mathcal{M}_n(\mathbb{C})$. On dit que U est unitaire si $UU^* = I_n$.



Remarquons alors que U est inversible et que l'on a aussi $U^*U = I_n$. Ces deux égalités sont en fait équivalentes.

Proposition II.4.

On suppose que E est de dimension finie n . Soit $U \in \mathcal{M}_n(\mathbb{C})$. Les propositions suivantes sont équivalentes.

- (1) U est unitaire.
- (2) Les colonnes de U forment une base orthonormée de $\mathcal{M}_{n,1}(\mathbb{R})$.
- (3) U est la matrice d'un endomorphisme $u \in \mathcal{U}(E)$ dans une base orthonormée.

 **Preuve**

$\rightarrow (1) \Rightarrow (2)$

Pour tout $k \in \llbracket 1; n \rrbracket$, on note C_k la k -ième colonne de U .

Pour tous $k, j \in \llbracket 1; n \rrbracket$, le coefficient à la ligne i et à la colonne j dans U^*U est égal à $C_k^*C_j$.

Or, $C_k^*C_j = \delta_{k,j}$, donc les colonnes de U forment bien une base orthonormée de $\mathcal{M}_{n,1}(\mathbb{R})$.

$\rightarrow (2) \Rightarrow (3)$

Considérons une base orthonormée (e_1, \dots, e_n) de E et définissons $u \in \mathcal{L}(E)$ tel que sa matrice relativement à cette base vale U .

Soit $x \in E$ et X sa colonne représentative relativement à cette même base. Alors

$$\|u(x)\|^2 = X^* \underbrace{U^*U}_{=I_n} X = X^*X = \|x\|^2$$

Donc $u \in \mathcal{U}(E)$.

$\rightarrow (3) \Rightarrow (1)$

Rappelons que u préserve aussi le produit scalaire. Ainsi, pour tous $X, Y \in \mathcal{M}_{n,1}(\mathbb{C})$,

$$X^*U^*UY = X^*Y \quad (\star)$$

Rappelons que pour tous $k, j \in \llbracket 1; n \rrbracket$ et pour toute $M \in \mathcal{M}_n(\mathbb{C})$,


$$E_k^\top M E_j = M[k, j] \quad \text{et} \quad E_k^\top E_j = \delta_{k,j}$$

Ainsi, en évaluant l'identité (\star) en chaque E_k , il vient que $U^*U = I_n$. Donc U est unitaire.

Correction de l'exercice I.6. :

1. Soit χ un caractère de G . Soit $a \in G$. Le théorème de Lagrange assure que l'ordre de a divise n , donc $a^n = e$, donc $\chi(a)^n = \chi(a^n) = 1$. Donc χ est à valeurs dans \mathbb{U}_n .
2. Soit Φ un caractère non constant. Il existe $b \in G$ tel que $\Phi(b) \neq 1$. L'application $a \mapsto ab$ est une bijection de G dans G , donc

$$\sum_{a \in G} \Phi(a) = \sum_{a \in G} \Phi(ab) = \Phi(b) \sum_{a \in G} \Phi(a)$$

Donc $\sum_{a \in G} \Phi(a) = 0$.

3. Soient χ et ψ deux caractères distincts. Calculons leur produit scalaire :

$$\langle \psi, \chi \rangle = \frac{1}{|G|} \sum_{a \in G} \overline{\psi(a)} \chi(a) = \frac{1}{|G|} \sum_{a \in G} \frac{\chi}{\psi}(a) \uparrow$$

$\psi(a) \in \mathbb{U}_n \quad \frac{\chi}{\psi}$ est un caractère

De plus,

$$\langle \chi, \chi \rangle = \frac{1}{|G|} \sum_{a \in G} |\chi(a)|^2 = \frac{1}{|G|} \sum_{a \in G} 1 = 1$$

$\chi(a) \in \mathbb{U}_n$



CHAPITRE 42

Endomorphismes d'un espace hermitien

Dans tout ce chapitre, $(E, \langle \cdot, \cdot \rangle)$ désigne un espace hermitien de dimension $n \geq 1$.

Exemples

→ Sur \mathbb{C}^n : pour tous $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbb{C}^n$, $\langle x, y \rangle = \sum_{k=1}^n \overline{x_k} y_k$.

→ Sur \mathcal{T}_n : pour tous $P, Q \in \mathcal{T}_n$, $\langle P, Q \rangle = \frac{1}{2\pi} \int_0^{2\pi} \overline{P(t)} Q(t) dt$.

i Si, pour tout $k \in \llbracket -n; n \rrbracket$, l'application $x \mapsto e^{ikx}$ est notée e_k , rappelons que $\mathcal{T}_n = \text{Vect}(e_{-n}, \dots, e_n)$.

I Adjonction matricielle

Définition I.1.

Soit $A \in \mathcal{M}_n(\mathbb{C})$. On appelle *matrice adjointe de A*, et on note A^* , la matrice \overline{A}^\top .

Proposition I.2.

Pour toutes $A, B \in \mathcal{M}_n(\mathbb{C})$, et pour tout $\lambda \in \mathbb{C}$,

→ $(A + B)^* = A^* + B^*$, $(\lambda A)^* = \overline{\lambda} A^*$, et $(AB)^* = B^* A^*$.

→ $\det(A^*) = \overline{\det(A)}$, et $\chi_{A^*} = \overline{\chi_A}$

→ $\text{rg}(A^*) = \text{rg}(A)$. En effet $\text{rg}(A^*) = \text{rg}(\overline{A}) = \text{rg}(A)$

i Si un polynôme P s'écrit $\sum_{k=0}^n a_k X^k$, alors $\overline{P} = \sum_{k=0}^n \overline{a_k} X^k$

Matrices hermitiennes : Une matrice carrée est hermitienne si elle est égale à sa matrice adjointe.

Proposition I.3.

→ L'ensemble des matrices hermitiennes d'ordre n

$$\mathcal{H}_n(\mathbb{C}) = \{A \in \mathcal{M}_n(\mathbb{C}) \mid A^* = A\}$$

est un \mathbb{R} -espace vectoriel de dimension n^2 .

→ Si $A \in \mathcal{H}_n(\mathbb{C})$, alors $\chi_A \in \mathbb{R}[X]$.

Preuves

→ Soit $A = B + iC \in \mathcal{M}_n(\mathbb{C})$ telle que B et $C \in \mathcal{M}_n(\mathbb{R})$. On a les équivalences suivantes :

$$A \in \mathcal{H}_n(\mathbb{C}) \iff A^* = A \iff B^\top = B \quad \text{et} \quad C^\top = -C$$

Donc $\mathcal{H}_n(\mathbb{C})$ est isomorphe $\mathcal{S}_n(\mathbb{R}) \times \mathcal{A}_n(\mathbb{R})$. Donc $\dim(\mathcal{H}_n(\mathbb{C})) = \frac{n(n+1)}{2} + \frac{n(n-1)}{2} = n^2$.

→ Si $A \in \mathcal{H}_n(\mathbb{C})$, alors $\chi_A = \chi_{A^*} = \overline{\chi_A}$.

Matrices unitaires : Les matrices unitaires sont les matrices de l'ensemble

$$\mathcal{U}_n(\mathbb{C}) = \{U \in \mathcal{M}_n(\mathbb{C}) \mid U^*U = I_n\}$$

Proposition I.4.

- $\mathcal{U}_n(\mathbb{C})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$.
- $U \in \mathcal{U}_n(\mathbb{C}) \iff$ les colonnes de U forment une base orthonormée de $\mathcal{M}_{n,1}(\mathbb{C})$
 \iff les lignes de U forment une base orthonormée de $\mathcal{M}_{1,n}(\mathbb{C})$.
- $U \in \mathcal{U}_n(\mathbb{C})$ si, et seulement si, il existe deux bases orthonormées \mathcal{B} et \mathcal{B}' de E telles que U soit la matrice de la famille \mathcal{B}' relativement à la base \mathcal{B} .

Preuve de la deuxième proposition : Soit $U = (u_{k,l})_{1 \leq k, l \leq n} \in \mathcal{U}_n(\mathbb{C})$. Alors pour tous $p, q \in \llbracket 1; n \rrbracket$, $(U^*U)(p, q) = \sum_{k=1}^n \overline{u_{k,p}} u_{k,q}$, donc pour $p \neq q$, $\sum_{k=1}^n \overline{u_{k,p}} u_{k,q} = 0$ et pour $p = q$, $\sum_{k=1}^n |u_{k,p}|^2 = 1$. Donc, les colonnes de U forment une base orthonormée de $\mathcal{M}_{n,1}(\mathbb{C})$.

De même, en examinant les coefficients de UU^* , il vient que les lignes de U forment une base orthonormée de $\mathcal{M}_{1,n}(\mathbb{C})$. Les réciproques sont immédiates.

Matrices normales Une matrice M de $\mathcal{M}_n(\mathbb{C})$ est dite normale si $AA^* = A^*A$.

II Adjonction dans $\mathcal{L}(E)$

Théorème - définition II.1.

Soit $u \in \mathcal{L}(E)$. Alors, il existe un unique endomorphisme v de E tel que :

$$\forall (x, y) \in E^2, \quad \langle u(x), y \rangle = \langle x, v(y) \rangle$$

De plus, la matrice de v relativement à toute base orthonormée \mathcal{B} de E est la matrice adjointe de la matrice de u relativement à la même base \mathcal{B} , et v est appelé *endomorphisme adjoint* de u et est noté u^* .

Preuve : Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base orthonormée de E , et $A = (a_{k,\ell})_{1 \leq k, \ell \leq n}$ la matrice de u relativement à \mathcal{B} . Posons v tel que sa matrice relativement à \mathcal{B} vaille A^* .

Alors, pour tous $x = x_1e_1 + \dots + x_ne_n$, $y = y_1e_1 + \dots + y_ne_n \in E$,

$$\langle u(x), y \rangle = \left\langle \sum_{\ell=1}^n x_\ell u(e_\ell), \sum_{\ell=1}^n y_\ell e_\ell \right\rangle = \left\langle \sum_{\ell=1}^n x_\ell \left(\sum_{k=1}^n a_{k,\ell} e_k \right), \sum_{j=1}^n y_j e_j \right\rangle = \sum_{\substack{1 \leq \ell, k \leq n \\ \text{on conserve les termes où } k=j}} \overline{x_\ell} a_{k,\ell} y_k$$

et

$$\langle x, v(y) \rangle = \left\langle \sum_{j=1}^n x_j e_j, \sum_{\ell=1}^n y_\ell \left(\sum_{k=1}^n \overline{a_{\ell,k}} e_k \right) \right\rangle = \sum_{1 \leq \ell, k \leq n} \overline{x_k} y_\ell \overline{a_{\ell,k}} = \langle u(x), y \rangle$$

De plus, si un endomorphisme w , de matrice notée $(w_{j,k})_{1 \leq j, k \leq n}$ relativement à la base \mathcal{B} , vérifie la même identité, alors pour tous $j, k \in \llbracket 1; n \rrbracket$, $w_{j,k} = \langle e_j, w(e_k) \rangle = \langle u(e_j), e_k \rangle = \overline{a_{k,j}}$, donc $w = v$.

Proposition II.2.

Soit F un sous-espace vectoriel de E , et u un endomorphisme de E .

Si F est stable par u , alors F^\perp est stable par u^* .

Preuve : Si $y \in F^\perp$, alors, pour tout $x \in F$, alors $0 = \langle u(x), y \rangle = \langle x, u^*(y) \rangle$, donc $u^*(y) \in F^\perp$.

Proposition II.3.

Soit u un endomorphisme de E .

1. Les trois assertions suivantes sont équivalentes :

- u est hermitien *i.e.* $u = u^*$.
- Il existe une base orthonormée de E telle que la matrice de u relativement à cette base soit hermitienne.
- Pour toute base orthonormée \mathcal{B} de E , la matrice de u relativement à \mathcal{B} est hermitienne.

2. Les trois assertions suivantes sont également équivalentes :

- u est unitaire *i.e.* pour tous $x, y \in E$, $\langle u(x), u(y) \rangle = \langle x, y \rangle$.
- Il existe une base orthonormée de E telle que la matrice de u relativement à cette base soit unitaire.
- Pour toute base orthonormée \mathcal{B} de E , la matrice de u relativement à \mathcal{B} est unitaire.

Preuves : La première chaîne d'équivalences est immédiate car la matrice de u relativement à une base orthonormée \mathcal{B} de E (et il en existe) est la matrice adjointe de la matrice de u^* relativement à \mathcal{B} . Pour la deuxième chaîne d'équivalences, il convient de remarquer que u est unitaire si, et seulement si, pour tout $(x, y) \in E^2$, $\langle x, (u^* \circ u)(y) \rangle = \langle x, y \rangle$, donc si, et seulement si, $u^* \circ u = \text{Id}_E$ (car pour tout $x \in E$, $\langle x, (u^* \circ u)(x) \rangle = \langle x, x \rangle$).

 On note $\mathcal{U}(E)$ les endomorphismes unitaires de E .

Exercice II.4.

Soit $(E, \langle \cdot, \cdot \rangle)$ un espace hermitien de dimension $n \geq 1$ et on note $\|\cdot\|$ la norme associée au produit scalaire $\langle \cdot, \cdot \rangle$. Montrer que $\mathcal{U}(E)$ est compact.

Théorème II.5.

Soit $u \in \mathcal{L}(E)$.

- u est normal si, et seulement si, u est diagonalisable dans une base orthonormée de E .
- u est hermitien si, et seulement si, u est diagonalisable dans une base orthonormée de E et $\text{Sp}(u) \subset \mathbb{R}$.
- u est unitaire si, et seulement si, u est diagonalisable dans une base orthonormée de E et $\text{Sp}(u) \subset \mathbb{U}$.

Correction de l'exercice II.4. :

Montrons que $\mathcal{U}_n(\mathbb{C})$ est un compact de $\mathcal{M}_n(\mathbb{C})$. Notons $\|\cdot\|$ la norme associée au produit scalaire canonique sur $\mathcal{M}_n(\mathbb{C})$. Pour toute $U \in \mathcal{U}_n(\mathbb{C})$, $\|U\| = 1$, donc $\mathcal{U}_n(\mathbb{C})$ est borné.

De plus, $\mathcal{U}_n(\mathbb{C})$ est fermé dans $\mathcal{M}_n(\mathbb{C})$ en tant qu'image réciproque de $\{0\}$, fermé dans \mathbb{R} , par l'application continue $U \mapsto U^*U - I_n$. Donc $\mathcal{U}_n(\mathbb{C})$ est compact.

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base orthonormée de E . Introduisons l'application de $\mathcal{M}_n(\mathbb{C})$ à valeurs dans $\mathcal{L}(E)$

$$\varphi : M = (m_{j,k})_{1 \leq j, k \leq n} \longmapsto \left(x = \sum_{j=1}^n x_j e_j \longmapsto \sum_{j=1}^n x_i \left(\sum_{k=1}^n m_{k,j} e_j \right) \right)$$

Cette application est linéaire donc continue car $\mathcal{M}_n(\mathbb{C})$ est de dimension finie. Il est clair que $\mathcal{U}(E)$ est l'image par φ de $\mathcal{U}_n(\mathbb{C})$, qui est compact, donc $\mathcal{U}(E)$ est compact.