

Physique

Produit vectoriel

Analyse Vectorielle

- Champ scalaire, champ vectoriel
- Champ à circulation conservative
- Champ à flux conservatif
- Circulation dans un champ de vecteur
- Divergence d'un champ vectoriel
- Flux au travers d'une surface
- Gradient d'un champ scalaire
- Laplacien
- Notation nabla
- Rotationnel d'un champ de vecteur
- Systèmes de coordonnées orthogonales
- Théorème de Green-Ostrogradski

Électricité

Amplificateurs Opérationels

Maths

Algèbre

Vocabulaire d'ensemble structuré

Algèbre Linéaire

- Algorithme du pivot de Gauss
- Base duale, antéduale
- Condition de liberté d'une forme linéaire à une famille
- Développement du déterminant par ligne ou par colonne
- Endomorphismes nilpotents
- Espaces supplémentaires
- Intersection d'hyperplans
- Lemme de factorisation
- Liberté d'une famille de l'espace dual
- Notations de matrices
- Somme directe de sous espaces vectoriels
- Théorème de la base télescopique
- Vandermonde, interpolation de Lagrange

Algèbres

- Algèbre engendrée
- Algèbres
- Algèbres commutatives intègres de dimension finie
- Algèbres et extensions de corps
- Clôture algébrique des rationnels
- Condition d'intégrité d'une sous-algèbre engendrée
- Morphisme d'algèbre
- Nombres algébriques
- Sous algèbres
- inversibilité des éléments d'une sous-algèbre engendrée

Anneaux et Corps

Irréductibles d'un anneau

Anneaux et corps

- Axiomes d'un anneau
- Axiomes d'un corps
- Axiomes d'un sous-corps
- Corps des fractions
- Corps gauche, anneau à division
- Diviseur de zéro
- Groupe des inversibles
- Idéal d'un anneau
- Idéaux maximaux, anneaux quotients
- Intégrité d'un anneau
- Primalité de la caractéristique d'un corps

Arithmétique

- Fonctions arithmétiques : Möbius et indicatrice d'Euler
- Formule du nombre de diviseurs
- Indicatrice d'Euler
- Lemme d'Euclide
- Nombres de Fermat
- Petit théorème de Fermat
- Propriétés diviseurs communs
- Théorème de Bézout
- Théorème de Gauss
- Théorème de Wilson
- Théorème des restes chinois
- Équations diophantiennes

Ensembles

Formule du crible

Espaces Vectoriels

- Axiomes d'un espace vectoriel
- Formes lineaires et hyperplans
- Théorème de caractérisation du rang

Groupes

- Actions de groupe
- Axiomes d'un groupe
- Axiomes d'un sous-groupe
- Démonstration du Théorème de Lagrange
- Développement de groupes
- Exercice : Les p-groupes
- Exercice : élément d'ordre p dans un groupe d'ordre divisé par p
- Formule des classes
- Groupe Diédral
- Groupes quotients
- Relation de cardinal pour un morphisme de groupe
- Signature d'une permutation
- Théorème de Burnside
- Théorème de Lagrange
- Existence et unicité des sous groupes de groupe cyclique

Matrices

- Matrices semblables
- Théorème de caractérisation des matrices inversibles

Polynômes

- Contenus d'un polynôme à coefficients entiers
- Critère d'Eisenstein
- Décomposition en éléments simples
- Entiers algébriques
- Fonctions symétriques des racines
- Formule de Taylor-Lagrange formelle
- Multiplicité d'une racine
- Polynômes associés
- Polynômes cyclotomiques
- Polynômes de Tchebycheff
- Polynômes en caractéristique strictement positive
- Polynômes irréductibles
- Polynômes scindés
- Propriétés des fractions rationnelles
- Propriétés des racines d'un polynôme

Relations

- Majorant, borne supérieure, élément maximale

Réduction

- Autre critère de diagonalisabilité
- Calcul de puissance de matrice : cas diagonalisable
- Calcul de puissance de matrice : polynôme annulateur
- Caractérisation des endomorphismes nilpotents
- Codagonalisabilité
- Commutant d'un endomorphisme diagonalisable
- Cotrigonalisation
- Critère de Diagonalisabilité
- Critère de trigonalisabilité sur le polynôme minimal
- Diagonalisabilité
- Diagonalisabilité d'un endomorphisme induit
- Décomposition de Dunford
- Décomposition en sous espaces caractéristiques
- Démonstration annexe du théorème des noyaux
- Endomorphisme commutateur de matrices
- Endomorphisme différence de produits de matrices
- Endomorphismes cycliques
- Endomorphismes de produit de matrices
- Endomorphismes nilpotents cycliques
- Endomorphismes semi-simples
- Endomorphismes simples
- Exercice : critère de nilpotence sur la trace des puissances
- Exercice : lien entre diagonalisabilité d'un endomorphisme et son carré
- Existence d'une droite ou d'un plan stable dans un espace vectoriel réel
- Matrice compagnon
- Multiplicités d'une valeur propre
- Polynôme caractéristique d'un endomorphisme
- Premier lien entre polynôme minimal et polynôme caractéristique
- Produit de Kronecker et diagonalisabilité
- Projecteurs spectraux d'un endomorphisme diagonalisable
- Propriétés diverses du polynôme caractéristique
- Pseudo-commutativité du polynôme caractéristique
- Racine k-ème de matrices
- Recherche d'hyperplans stables
- Réduction de matrice dans rang 1
- Somme directe des sous-espaces propres
- Sous-espaces caractéristiques et polynôme minimal
- Sous-espaces cycliques
- Sous-espaces stables d'un endomorphisme diagonalisable
- Suites récurrentes linéaires
- Théorème de Cayley-Hamilton
- Théorème des noyaux
- Trigonalisabilité
- Valeurs propres, espaces propres
- Vision matricielle de la cyclicité
- Équations matricielles

Analyse

Recherche d'équivalent d'une suite

Complexes

- Formule de Moivre
- Formules d'addition trigonometrique
- Formules de duplication trigonométrique
- Formules de factorisation trigonométrique
- Formules de linéarisation trigonométrique
- Formules de parité et périodicité trigonométriques
- Formules en tangente de theta sur deux
- Inégalité Triangulaire

Continuité

- Fonctions K-Lipschitziennes
- Théorème de Heine
- Théorème des bornes atteintes

Convexité

Propriétés de convexité

Dérivation

- Fonctions trigonometriques réciproques
- Inégalité des accroissements finis et de Taylor-Lagrange
- Propriété des extrémum locaux
- Taylor-Langrange
- Théorème de Rolle, théorème des accroissements finis

Développements Limités

- Développements limités
- Étude local et asymptotique de fonctions

EDL

- EDL d'ordre 1
- EDL d'ordre 2
- Méthode de séparation des variables
- Méthode de variation de la constante

Intégration

- Comparaison série intégrale
- Critère de convergence d'intégrales usuelles
- Fonction gamma
- Hölder
- Intégrales de Wallis
- Intégration de l'inverse d'un trinôme
- Lemme de Riemann-Lebesgue
- Taylor reste intégrale

Réels

- Adhérence
- Corps totalement ordonné
- Densité
- Inégalité Triangulaire
- Partie convexe de R
- Propriété de la borne supérieure
- Propriété fondamentale des réels
- Voisinage

Suites

Suites récurrentes linéaires

Suites Réelles

- Caractérisation séquentielle de l'adhérence
 - Comparaison asymptotiques usuelles
 - Manipulations asymptotiques
 - Moyennes de Cesàro
 - Suites adjacentes, emboîtées
 - Suites arithmético-géométriques
 - Suites récurrentes d'ordre 2
 - Suites récurrentes
 - Théorème de Bolzano-Weiestrass
- Séries
- Absolue convergence
 - Comparaison série intégrale
 - Exercice : Nature de la série terme général sur somme partielle
 - Familles sommables
 - Propriétés élémentaires sur les séries
 - Règle de Raabe-Duhamel
 - Séries de Bertrand
 - Théorème de comparaison des séries positives
 - Théorème de sommation des relations de comparaison pour les séries
 - Théorème de sommation par paquets
 - Théorème des séries alternées
 - Transformation d'Abel
 - Équivalents de référence : séries de Riemann

Taylor

- Taylor reste intégrale
- Taylor-Lagrange

Calculs

- Formule de newton
- Formules de somme d'entiers consécutifs
- Formules sur les coefficients binomiaux

Exercice

Algèbre Générale

- Développement de groupes
 - Exercice : Cyclicité des sous-groupes finis des inversibles d'un corps
 - Exercice : Dénombrement de morphismes
 - Exercice : Groupe d'éléments d'ordre inférieur à deux
 - Exercice : Les carrés de Fp
 - Exercice : Les p-groupes
 - Exercice : existence d'un élément d'ordre du ppcm de deux autres
 - Exercice : élément d'ordre p dans un groupe d'ordre divisé par p
- Algèbre Linéaire
- Exercice : Noyaux et images itérées
 - Exercice : Union de sous espaces vectoriels
 - Exercice : endomorphisme qui stabilise toutes les droites
 - Exercice : rang d'une comatrice
- Polynômes
- Exercice : Gauss-Lucas
 - Exercice : Irréductibilité dans les rationels
 - Exercice : Polynômes à coefficients entiers
 - Exercice : Produit de polynômes de rationels unitaire entier
 - Exercice : rationalité d'une racine de haute multiplicité
- Réduction
- Exercice : commutateur qui vaut l'un des opérande
 - Exercice : critère de diagonalisabilité sur l'existence de supplémentaires stables
 - Exercice : le bicommutant
 - Exercice : polynôme caractéristique d'une somme d'endomorphismes
 - Exercice : polynôme caractéristique divisant une puissance du polynôme minimal
 - Exercice : propriétés des endomorphismes cycliques
 - Exercice : valuation X-adique du polynôme minimal.
 - Exercice : vecteur dont le polynôme minimal ponctuel est le polynôme minimal

Séries

- Exercice : Nature de la série terme général sur somme partielle

Topologie

- Boules et sphères
- Comparaison de normes
- Distance
- Limites de suites
- Norme
- Norme euclidienne
- Norme produit
- Points extrémaux d'un convexe
- Topologie sur un espace métrique
- Topologie, espace topologique
- Valeurs d'adhérence d'une suite

Trigonométrie

Eulidienne

- Formules d'addition trigonometrique
- Formules de duplication trigonométrique
- Formules de factorisation trigonométrique
- Formules de linéarisation trigonométrique
- Formules de parité et périodicité trigonométriques
- Formules en tangente de theta sur deux

Physique ► Électricité

Amplificateurs Opérationnels

Systèmes de coordonnées orthogonales

Définitions élémentaires de système de coordonnées orthogonales en analyse vectorielle.

On peut décrire l'espace dans un système de coordonnées (q_1, q_2, q_3) associé au trièdre local $(\vec{e}_1, \vec{e}_2, \vec{e}_3)$.

Un déplacement élémentaire \overrightarrow{dM} s'exprime

$$\begin{aligned}\overrightarrow{dM} &= h_1(q_1, q_2, q_3) dq_1 \vec{e}_1 \\ &\quad + h_2(q_1, q_2, q_3) dq_2 \vec{e}_2 \\ &\quad + h_3(q_1, q_2, q_3) dq_3 \vec{e}_3\end{aligned}$$

- En cartésiennes (x, y, z) :

$$h_1 = h_2 = h_3 = 1$$

$$\overrightarrow{dM} = dx \vec{u}_x + dy \vec{u}_y + dz \vec{u}_z$$

- En cylindriques (r, θ, z) :

$$h_1 = h_3 = 1 \quad h_2 = r$$

$$\overrightarrow{dM} = dr \vec{u}_r + r d\theta \vec{u}_\theta + dz \vec{u}_z$$

- En sphériques (r, θ, φ) :

$$h_1 = 1 \quad h_2 = r \quad h_3 = r \sin \theta$$

$$\overrightarrow{dM} = dr \vec{u}_r + r d\theta \vec{u}_\theta + r \sin \theta d\varphi \vec{u}_\varphi$$

Champ scalaire, champ vectoriel

Définitions d'un champ scalaire,
champ vectoriel.

Un champ est une grandeur dans un domaine D de l'espace à un instant t , noté $\vec{G}(\vec{r}, t)$.

Un champ peut être vectoriel ou scalaire selon si la grandeur qu'il représente l'est.

Un champ est dit

Uniforme s'il est indépendant de \vec{r} .

Stationnaire ou permanent s'il est indépendant de t .

Constant S'il est les deux

- On appelle ligne de champ une courbe de l'espace qui est en tout points tangente au champ.
- Pour un champ $f(\vec{r}, t)$, on appelle surface équi- f une surface où f est uniforme.

Gradient d'un champ scalaire

Définition du gradient d'un champ scalaire.

Pour un champ scalaire $f(\vec{r}, t)$. On définit le gradient de f , noté $\overrightarrow{\text{grad}} f$ ou ∇f afin que

$$df = \nabla f \cdot d\vec{M}$$

En coordonnées cartésiennes

$$\overrightarrow{\text{grad}} f = \nabla f = \frac{\partial f}{\partial x} \vec{u}_x + \frac{\partial f}{\partial y} \vec{u}_y + \frac{\partial f}{\partial z} \vec{u}_z$$

Car

$$d\vec{M} = dx \vec{u}_x + dy \vec{u}_y + dz \vec{u}_z$$

$$\begin{aligned} df &= \frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy + \frac{\partial f}{\partial z} dz \\ &= \nabla f \cdot d\vec{M} \end{aligned}$$

En général

$$\nabla f = \frac{1}{h_1} \frac{\partial f}{\partial q_1} \vec{e}_1 + \frac{1}{h_2} \frac{\partial f}{\partial q_2} \vec{e}_2 + \frac{1}{h_3} \frac{\partial f}{\partial q_3} \vec{e}_3$$

Cas particulier

- En sphérique : $\nabla \frac{1}{r} = -\frac{1}{r^2} \vec{u}_r$
- En sphérique : $\nabla r^2 = 2r \vec{u}_r$

Flux au travers d'une surface

Définition du flux au travers d'une surface.

On considère une fonction vectorielle $\vec{F}(q_1, q_2, q_3)$

Pour une surface

- Fermée : on l'oriente de l'intérieur vers l'extérieur par convention.
- Ouverte : on oriente le contour sur lequel elle s'appuie et on applique la règle de la main droite.

Le flux Φ au travers de la surface S est

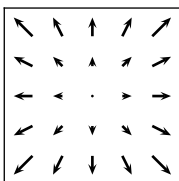
$$d\Phi = \vec{F} \cdot d\vec{S}$$
$$\Phi = \oiint_S \vec{F} \cdot d\vec{S}$$

Divergence d'un champ vectoriel

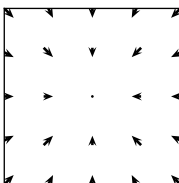
Définition de la divergence d'un champ vectoriel.

La divergence d'un champ de vecteur représente à quelle point le champ diverge ou converge en ce points. On écrit $\text{div } \vec{F}$ ou $\nabla \cdot \vec{F}$.

$$\nabla \cdot \vec{F} > 0$$



$$\nabla \cdot \vec{F} < 0$$



Son expression est

$$\nabla \cdot \vec{F} = \frac{1}{h_1 h_2 h_3} \left[\frac{\partial}{\partial q_1} (h_2 h_3 F_{q_1}) + \frac{\partial}{\partial q_2} (h_1 h_3 F_{q_2}) + \frac{\partial}{\partial q_3} (h_1 h_2 F_{q_3}) \right]$$

En cartésiennes

$$\nabla \cdot \vec{F} = \frac{\partial F_x}{\partial x} + \frac{\partial F_y}{\partial y} + \frac{\partial F_z}{\partial z}$$

Cas particuliers

- En cylindrique : $\nabla \cdot \frac{\vec{u}_r}{r} = 0$ (sauf en 0)
- En sphérique : $\nabla \cdot \frac{\vec{u}_r}{r^2} = 0$ (sauf en 0)
- $\nabla \cdot \vec{r} = \dim E$

Théorème de Green-Ostrogradski

Énoncé du théorème de Green-Ostrogradski.

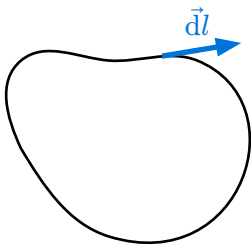
Pour un champ vectoriel \vec{F} et une surface fermée S qui délimite un volume V , on a

$$\Phi = \oiint_S \vec{F} \cdot \overrightarrow{dS} = \iiint_V \nabla \cdot \vec{F} \, d\tau$$

Circulation dans un champ de vecteur

Définition de la circulation dans un champ de vecteurs.

Pour C un contour orienté



On définit la circulation du champ \vec{F} sur C comme

$$d\mathcal{C} = \vec{F} \cdot d\vec{l}$$
$$\mathcal{C} = \int_C \vec{F} \cdot d\vec{l}$$

Rotationnel d'un champ de vecteur

Définition du rotationnel d'un champ de vecteur.

$$\overrightarrow{rot} \vec{F} = \nabla \wedge \vec{F}$$

$$= \begin{pmatrix} \frac{1}{h_2 h_3} \left[\frac{\partial (h_3 F_{q_3})}{\partial q_2} - \frac{\partial (h_2 F_{q_2})}{\partial q_3} \right] \\ \frac{1}{h_3 h_1} \left[\frac{\partial (h_1 F_{q_1})}{\partial q_3} - \frac{\partial (h_3 F_{q_3})}{\partial q_1} \right] \\ \frac{1}{h_1 h_2} \left[\frac{\partial (h_2 F_{q_2})}{\partial q_1} - \frac{\partial (h_1 F_{q_1})}{\partial q_2} \right] \end{pmatrix}$$

En cartésienne

$$\nabla \wedge \vec{F} = \begin{pmatrix} \frac{\partial F_z}{\partial y} - \frac{\partial F_y}{\partial z} \\ \frac{\partial F_x}{\partial z} - \frac{\partial F_z}{\partial x} \\ \frac{\partial F_y}{\partial x} - \frac{\partial F_x}{\partial y} \end{pmatrix}$$

Produit vectoriel

Expression du produit vectoriel.

$$\begin{aligned} \begin{pmatrix} a_x \\ a_y \\ a_z \end{pmatrix} \wedge \begin{pmatrix} b_x \\ b_y \\ b_z \end{pmatrix} &= \begin{pmatrix} \begin{vmatrix} a_y & b_y \\ a_z & b_z \end{vmatrix} \\ - \begin{vmatrix} a_x & b_y \\ a_z & b_z \end{vmatrix} \\ \begin{vmatrix} a_x & b_y \\ a_z & b_z \end{vmatrix} \end{pmatrix} \\ &= \begin{pmatrix} a_y b_z - b_y a_z \\ a_z b_y - b_z a_y \\ a_x b_z - b_y a_z \end{pmatrix} \end{aligned}$$

Propriétés

$$\begin{aligned} \vec{u} \wedge \vec{v} &= -(\vec{v} \wedge \vec{u}) \\ (\vec{u} \wedge \vec{v}) \cdot \vec{w} &= [\vec{u}, \vec{v}, \vec{w}] \\ &= [\vec{w}, \vec{u}, \vec{v}] \\ &= [\vec{v}, \vec{w}, \vec{u}] \\ \vec{u} \wedge \vec{u} &= 0 \end{aligned}$$

Notation nabla

Notation nabla.

En coordonnées cartésiennes, on “définit”

$$\nabla = \begin{pmatrix} \frac{\partial}{\partial x} \\ \frac{\partial}{\partial y} \\ \frac{\partial}{\partial z} \end{pmatrix}$$

Ainsi on retrouve les formules des opérateurs (toujours en cartésiennes)

$$\overrightarrow{grad} f = \nabla f$$

$$\text{div } \vec{F} = \nabla \cdot \vec{F}$$

$$\overrightarrow{rot} \vec{F} = \nabla \wedge \vec{F}$$

En général

$$\nabla = \begin{pmatrix} \frac{1}{h_1} \frac{\partial}{\partial q_1} \\ \frac{1}{h_2} \frac{\partial}{\partial q_2} \\ \frac{1}{h_3} \frac{\partial}{\partial q_3} \end{pmatrix}$$

Champ à circulation conservative

Définition de champ à circulation conservative.

Un champ \vec{F} est dit à circulation conservative ssi pour toute courbe fermée \mathcal{C} on a

$$\oint_{\mathcal{C}} \vec{F} \cdot d\vec{l} = 0$$

Ainsi la circulation de toute courbe passant par A et B deux points est la même, elle ne dépend pas du chemin choisis.

On peut alors définir le potentiel V , un champ scalaire tel que

$$V(A) = V_A$$

$$V(B) = V_A + \int_A^B \vec{F} \cdot d\vec{l}$$

Entre \vec{M} et $\vec{M} + d\vec{M}$

$$V(M) - V(M + dM) = dV(M) = \vec{F} \cdot d\vec{M}$$

Ainsi

$$\vec{F} = \nabla V$$

De plus

$$\oint_{\mathcal{C}} \vec{F} \cdot d\vec{l} = \iint_S (\nabla \wedge \vec{F}) \cdot d\vec{S} = 0$$

$$\Rightarrow \nabla \wedge \vec{F} = 0 \quad (\nabla \wedge (\nabla V) = 0)$$

Champ à flux conservatif

Définition d'un champ à flux conservatif.

Un champ \vec{F} est dit à flux conservatif si pour toute surface S fermée qui délimite un volume V .

$$\oiint_S \vec{F} \cdot \overrightarrow{dS} = 0$$

Ainsi

$$\begin{aligned} \oiint_S \vec{F} \cdot \overrightarrow{dS} &= \iiint_V \nabla \cdot \vec{F} \, d\tau = 0 \\ \Rightarrow \nabla \cdot \vec{F} &= 0 \quad \left(\nabla \cdot (\nabla \wedge \vec{F}) = 0 \right) \end{aligned}$$

De plus on dispose de \vec{A} (champ potentiel vecteur, H.P.) tel que

$$\vec{F} = \nabla \wedge \vec{A}$$

Laplacien

Définition du laplacien d'un champ.

Scalaire

On appelle laplacien scalaire d'un champ scalaire V le champ scalaire

$$\Delta V = \nabla \cdot (\nabla V)$$

En cartésiennes :

$$\Delta V = \frac{\partial^2 V}{\partial x^2} + \frac{\partial^2 V}{\partial y^2} + \frac{\partial^2 V}{\partial z^2}$$

En général :

$$\Delta V = \frac{1}{h_1 h_2 h_3} \left[\frac{\partial}{\partial q_1} \left(\frac{h_2 h_3}{h_1} \frac{\partial V}{\partial q_1} \right) + \frac{\partial}{\partial q_2} \left(\frac{h_1 h_3}{h_2} \frac{\partial V}{\partial q_2} \right) + \frac{\partial}{\partial q_3} \left(\frac{h_1 h_2}{h_3} \frac{\partial V}{\partial q_3} \right) \right]$$

Vectoriel

On appelle laplacien vectoriel d'un champ vectoriel \vec{F} le champ vectoriel

$$\Delta \vec{F} = \nabla (\nabla \cdot \vec{F}) - \nabla \wedge (\nabla \wedge \vec{F})$$

En cartésiennes :

$$\begin{aligned} \Delta \vec{F} &= \begin{pmatrix} \frac{\partial^2 F_x}{\partial x^2} + \frac{\partial^2 F_x}{\partial y^2} + \frac{\partial^2 F_x}{\partial z^2} \\ \frac{\partial^2 F_y}{\partial x^2} + \frac{\partial^2 F_y}{\partial y^2} + \frac{\partial^2 F_y}{\partial z^2} \\ \frac{\partial^2 F_z}{\partial x^2} + \frac{\partial^2 F_z}{\partial y^2} + \frac{\partial^2 F_z}{\partial z^2} \end{pmatrix} \\ &= \begin{pmatrix} \Delta F_x \\ \Delta F_y \\ \Delta F_z \end{pmatrix} \end{aligned}$$

Taylor-Lagrange

Théorème de Taylor-Lagrange, et conditions d'application.

Soit $f : [a, b] \rightarrow \mathbb{R}$, C^n sur $[a, b]$ et D^{n+1} sur $]a, b[$

Il existe $c \in]a, b[$ tel que

$$f(b) = \sum_{k=0}^n f^{(k)}(a) \frac{(b-a)^k}{k!} + f^{(n+1)}(c) \frac{(b-a)^{n+1}}{(n+1)!}$$

Taylor reste intégrale

Théorème de Taylor reste
intégrale, et conditions
d'application.

Soit $f : [a, b] \rightarrow \mathbb{R}$, C^{n+1}

$$f(b) = \sum_{k=0}^n f^{(k)}(a) \frac{(b-a)^k}{k!} + \int_a^b f^{(n+1)}(t) \frac{(b-t)^n}{n!} dt$$

Inégalité Triangulaire

Inégalité triangulaire première
et deuxième forme.

Soit $a, b \in \mathbb{C}$

$$|a + b| \leq |a| + |b|$$

$$||a| - |b|| \leq |a - b| \leq |a| + |b|$$

Formule de Moivre

Formule de Moivre.

Soit $\theta \in \mathbb{R}$

$$(\cos \theta + i \sin \theta)^n = \cos(n\theta) + i \sin(n\theta)$$

Formules d'addition trigonometrique

Formules d'additions
trigonométriques.

Soient $\theta, \varphi \in \mathbb{R}$

$$\cos(\theta + \varphi) = \cos \theta \cos \varphi - \sin \theta \sin \varphi$$

$$\sin(\theta + \varphi) = \cos \theta \sin \varphi + \sin \theta \cos \varphi$$

$$\tan(\theta + \varphi) = \frac{\tan \theta + \tan \varphi}{1 - \tan \theta \tan \varphi}$$

Formules de duplication trigonométrique

Formules de duplication
trigonométriques.

Soit $\theta \in \mathbb{R}$

$$\cos(2\theta) = \cos^2 \theta - \sin^2 \theta$$

$$\sin(2\theta) = 2 \cos \theta \sin \theta$$

$$\tan(2\theta) = \frac{2 \tan \theta}{1 - \tan^2 \theta}$$

Formules de linéarisation trigonométrique

Formules de linéarisation
trigonométriques.

Soient $a, b \in \mathbb{R}$

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

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

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

Formules de factorisation trigonométrique

Formules de factorisation
trigonométriques.

Soient $p, q \in \mathbb{R}$

$$\cos p + \cos q = 2 \cos\left(\frac{p+q}{2}\right) \cos\left(\frac{p-q}{2}\right)$$

$$\cos p - \cos q = -2 \sin\left(\frac{p+q}{2}\right) \sin\left(\frac{p-q}{2}\right)$$

$$\sin p + \sin q = 2 \sin\left(\frac{p+q}{2}\right) \cos\left(\frac{p-q}{2}\right)$$

Formules en tangente de theta sur deux

Formules en $\tan \frac{\theta}{2}$.

Soit $\theta \in \mathbb{R}$

$$\cos \theta = \frac{1 - \tan^2 \frac{\theta}{2}}{1 + \tan^2 \frac{\theta}{2}}$$

$$\sin \theta = \frac{2 \tan \frac{\theta}{2}}{1 + \tan^2 \frac{\theta}{2}}$$

$$\tan \theta = \frac{2 \tan \frac{\theta}{2}}{1 - \tan^2 \frac{\theta}{2}}$$

Formules de parité et périodicité trigonométriques

Formules de parité et périodicité
trigonométriques.

Soit $\theta \in \mathbb{R}$

$$\sin\left(\frac{\pi}{2} - \theta\right) = \cos \theta$$

$$\cos\left(\frac{\pi}{2} - \theta\right) = \sin \theta$$

$$\cos(\pi + \theta) = -\cos \theta$$

$$\sin(\pi + \theta) = -\sin \theta$$

Formules de somme d'entiers consécutifs

Forme explicites des sommes suivantes :

$$\sum_{k=1}^n k = ?$$

$$\sum_{k=1}^n k^2 = ?$$

$$\sum_{k=1}^n k^3 = ?$$

$$\sum_{k=1}^n k = \frac{n(n+1)}{2}$$

$$\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{k=1}^n k^3 = \left(\frac{n(n+1)}{2} \right)^2 = \frac{n^2(n+1)^2}{4}$$

EDL d'ordre 1

Soit $a, b \in \mathbb{C}$, $c(x)$ et $C(x)$ tel que $C'(x) = c(x)$.

$$(E_1) : y' = ay + b$$

$$(E_2) : y' = a(x)y$$

Les solutions S_1 et S_2 de (E_1) et (E_2) sont

$$S_1 = \left\{ x \mapsto \lambda e^{ax} - \frac{b}{a}, \lambda \in \mathbb{R} \right\}$$

$$S_2 = \{ x \mapsto \lambda e^{A(x)}, \lambda \in \mathbb{R} \}$$

Méthode de séparation des variables

Soit $a(x) \in D^1$

$$\frac{dy}{dx} = a(x)y$$

$$y(x) = ?$$

Soient $a(x) \in D^1$ et $A(x)$ une primitive de $a(x)$.

$$\frac{dy}{dx} = a(x)y$$

$$\frac{dy}{y} = a(x) dx$$

$$\int_{y_0}^y \frac{dy}{y} = \int_{x_0}^x a(x) dx$$

$$\ln y - \ln y_0 = A(x) - A(x_0)$$

$$y = \underbrace{y_0 e^{-A(x_0)}}_{\lambda} e^{A(x)}$$

Méthode de variation de la constante

Soient $a(x), b(x) : \mathbb{R} \rightarrow \mathbb{R}$ et $A(x)$ une primitive de $a(x)$.

$$y' = a(x)y + b(x)$$

$$f_h : y(x) = \lambda e^{A(x)}$$

Trouver f_p solution particulière par la variation de la constante.

Soient $a(x), b(x) : \mathbb{R} \rightarrow \mathbb{R}$ et $A(x)$ une primitive de $a(x)$.

$$y' = a(x)y + b(x)$$

$$f_h : y(x) = \lambda e^{A(x)}$$

On fait varier la constante : $\lambda \rightarrow \lambda(x)$:

$$f_p(x) = \lambda(x)e^{A(x)}$$

$$\begin{aligned} f_{p'}(x) &= a(x)f_p(x) + b(x) \\ &= \lambda'(x)e^{A(x)} + \lambda(x)a(x)e^{A(x)} \\ &= \lambda(x)a(x)e^{A(x)} + b(x) \end{aligned}$$

$$\lambda'(x) = b(x)e^{-A(x)}$$

$$\lambda(x) = \int b(x)e^{-A(x)} dx$$

EDL d'ordre 2

Soient $a, b, c \in \mathbb{C}$, résolution de l'équation homogène :

$$ay'' + by' + cy = 0$$

Soient $a, b, c \in \mathbb{C}$

$$ay'' + by' + cy = 0$$

On appelle équation caractéristique

$$(EC) : az^2 + bz + c = 0$$

- Si $\Delta > 0$, soit r_1, r_2 les racines (réelles) de (EC)

$$f_{h(x)} = \lambda e^{r_1 x} + \mu e^{r_2 x}, \quad \lambda, \mu \in \mathbb{R}$$

- Si $\Delta = 0$, soit r la racine double de (EC)

$$f_{h(x)} = (\lambda + \mu x)e^{rx}, \quad \lambda, \mu \in \mathbb{R}$$

- Si $\Delta < 0$, soit $\alpha + i\beta$ et $\alpha - i\beta$ les racines complexes de (EC)

$$f_{h(x)} = e^{\alpha x} (\lambda \cos(\beta x) + \mu \sin(\beta x))$$

Corps totalement ordonné

Définition d'un corps totalement ordonné.

Soit $(K, +, \cdot)$ un corps et un ordre \leq .

1. $\forall x, y, z \in K, x \leq y \Rightarrow x + z \leq y + z$
2. $\forall x, y \in K, x \geq 0 \text{ et } y \geq 0 \Rightarrow xy \geq 0$

\mathbb{R} et \mathbb{Q} sont ordonnés, \mathbb{C} ne l'est pas. Mais il existe un seul corps totalement ordonné (à isomorphisme près) : \mathbb{R} .

Propriété fondamentale des réels

Propriété fondamentale des réels.

Toute partie non vide majoré de \mathbb{R} admet une borne sup. De même pour minoré.

On en déduit (car \mathbb{R} est totalement ordonné) que

- $x \geq 0 \Rightarrow -x \leq 0$
- Loi du signe de produit
- $x^2 \geq 0$
- $1 > 0$
- $x > 0 \Rightarrow \frac{1}{x} > 0$
- $0 < x \leq y \Rightarrow \frac{1}{x} \geq \frac{1}{y}$

Propriété de la borne supérieure

Propriété de la borne supérieure.

Soit $A \subseteq \mathbb{R}$ non vide majoré, $S = \sup A$ ssi

1. $\forall x \in A, x \leq S$
2. $\forall \varepsilon > 0, \exists y \in A, s - \varepsilon < y$

Partie convexe de \mathbb{R}

Définition de partie convexe.

Une partie convexe de \mathbb{R} est un ensemble $C \subseteq \mathbb{R}$ tel que

$$\forall x \leq y \in C, [x, y] \subseteq C$$

Les parties convexes de \mathbb{R} sont des intervalles.

Densité

Définition de densité.

Soit $D \subseteq \mathbb{R}$, D est dense dans \mathbb{R} si

$$\forall a < b \in \mathbb{R},]a, b[\cap D \neq \emptyset$$

\mathbb{Q} est dense dans \mathbb{R} , preuve : saut de grenouille.

Voisinage

Définition de voisinage.

Soit $x \in \overline{\mathbb{R}}$, $V \subseteq \mathbb{R}$ est un voisinage de x si

$$\exists \varepsilon > 0,]x - \varepsilon, x + \varepsilon[\subseteq V$$

On note $\mathcal{V}(x)$ l'ensemble des voisinages de x .

Adhérence

Définition et propriétés de l'adhérence d'un ensemble.

Soit $A \subseteq \mathbb{R}$, $x \in \overline{\mathbb{R}}$, $x \in \mathbb{R}$ est adhérent à A si

$$\forall V \in \mathcal{V}(x), V \cap A \neq \emptyset$$

L'adhérence de A est alors

$$\begin{aligned}\text{adh}(A) &= \{x \in \mathbb{R} \mid x \text{ adhérent à } A\} \\ &= \{x \in \mathbb{R} \mid \forall \varepsilon > 0,]x - \varepsilon, x + \varepsilon[\cap A \neq \emptyset\}\end{aligned}$$

Propriétés :

- $A \subseteq \text{adh}(A)$
- Si A non vide borné :
 $\{\inf A, \sup A\} \subseteq A$
- $\text{adh}(]a, b[) = [a, b]$
- D est dense dans \mathbb{R} ssi
 $\text{adh}(D) = \mathbb{R}$
- $\text{adh}(\text{adh}(A)) = \text{adh}(A)$

Suites arithmético-géométriques

Formule explicite d'une suite arithmético-géométrique.

Soit $a, b \in \mathbb{R}$ et (u_n) une suite tel que

$$\forall n \in \mathbb{N}, u_{n+1} = au_n + b$$

On note $f(x) = ax + b$, on trouve le point fixe $w = \frac{b}{1-a}$. Soit $v_n = u_n - w$.

$$v_{n+1} = au_n + b - \underbrace{(aw + b)}_{-w}$$

$$= a(u_n - w) = av_n$$

$$v_n = a^n v_0$$

$$u_n = a^n(v_0 - w) + w$$

Suites récurrentes d'ordre 2

Formule explicite d'une suite récurrente d'ordre 2.

Soit $a, b \in \mathbb{R}$, (u_n) une suite tel que

$$u_{n+2} = au_{n+1} + bu_n$$

On résout l'équation caractéristique

$$x^2 = ax + b$$

- Deux racines r_1, r_2

$$u_n = \lambda r_1^n + \mu r_2^n$$

- Racine double r

$$u_n = (\lambda + \mu n)r^n$$

Avec $\lambda, \mu \in \mathbb{R}$ déterminés par u_0 et u_1 .

Caractérisation séquentielle de l'adhérence

Caractérisation séquentielle de l'adhérence et la borne supérieure.

Soit $A \subseteq \mathbb{R}$.

- Si (u_n) une suite à valeur dans A et $u_n \rightarrow l$, alors $l \in \text{adh}_{\mathbb{R}}(A)$.
- Si $x \in \text{adh}_{\mathbb{R}}$, alors il existe $(u_n) \in A^{\mathbb{N}}$ tel que $u_n \rightarrow x$.

Ainsi

$$\begin{aligned} & \text{adh}(A) \\ &= \{x \in \mathbb{R} \mid \exists (u_n) \in A^{\mathbb{N}}, u_n \rightarrow x\} \end{aligned}$$

Et $S = \sup A$ existe si A non vide majoré par S et il existe $(u_n) \in A^{\mathbb{N}}$ tel que $u_n \rightarrow S$.

Suites adjacentes, emboîtées

Définition et théorème des suites adjacentes et emboîtées.

- Adjacentes :

Deux suites (a_n) et (b_n) sont adjacentes si

$$(a_n) \nearrow, \quad (b_n) \searrow$$

$$\text{et } \lim_{n \rightarrow \infty} (b_n - a_n) = 0$$

Théorème : (a_n) et (b_n) et $\lim a_n = \lim b_n$.

Preuve : Théorème de la limite croissante pour la convergence.

- Emboîtées :

La même chose avec des segments.

Théorème :

$$\bigcap_{n=0}^{\infty} [a_n, b_n] = \{x\}$$

$$\text{avec } x = \lim a_n = \lim b_n$$

Théorème de Bolzano-Weiestrass

Théorème de Bolzano-Weiestrass et démonstration.

Toute suite réelle bornée admet une sous-suite convergente.

Dans \mathbb{R}^n (et \mathbb{C}), il suffit d'être borné en norme ou module.

Preuve :

Soit (u_n) une suite bornée par a_0 et b_0 , notons $A = \{u_n, n \in \mathbb{N}\}$. Par récurrence :

- **Ini :** $|[a_0, b_0] \cap A| = \infty$
- **Héré :** On suppose $|[a_n, b_n] \cap A| = \infty$, et on coupe en $m = \frac{a_n + b_n}{2}$:
 - Si $|[a_n, m] \cap A| = \infty$, $\begin{cases} a_{n+1} = a_n \\ b_{n+1} = m \end{cases}$
 - Si $|[m, b_n] \cap A| = \infty$, $\begin{cases} a_{n+1} = m \\ b_{n+1} = b_n \end{cases}$

Par le théorème des suites emboîtées :

$$\exists l \in [a_0, b_0], \bigcap_{n=0}^{\infty} [a_n, b_n] = \{l\}$$

Soit φ une extractrice, par récurrence :

- **Ini :** $\varphi(0) = 0$
- **Héré :** $[a_{n+1}, b_{n+1}]$ est infini, donc il existe $m > \varphi(n)$ tel que $u_m \in [a_{n+1}, b_{n+1}]$. On prend $\varphi(n+1) = m$.

Donc $a_n \leq u_{\varphi(n)} \leq b_n$ d'où $\lim u_{\varphi(n)} = l$.

Moyennes de Cesàro

Définition, propriétés des moyennes de Cesàro.

Soit (u_n) une suite. La suite des moyennes de Cesàro de u_n est

$$\sigma_n = \frac{a_1 + a_2 + \cdots + a_n}{n}$$

Si $u_n \rightarrow l \in \overline{\mathbb{R}}$, alors $\sigma_n \rightarrow l$.

Preuve :

- l fini : Découpage pour $n < N$ et $n \geq N$ et inégalité triangulaire.
- l infini : majoration.

Manipulations asymptotiques

Manipulations asymptotiques élémentaires.

- \sim : relation d'équivalence
 - ▶ produit, quotient, exposant
 - ▶ **pas** de somme, de composition, ...
- $o(1) \Leftrightarrow$ tend vers 0, $O(1) \Leftrightarrow$ borné
- O et o transitifs
- O et o mangent les constantes
- $u_n \sim v_n$ ssi $u_n = v_n + o(v_n)$
- Si $u_n \sim v_n$ (ou O, o), alors $u_{\varphi(n)} \sim v_{\varphi(n)}$ (ou O, o)
- o et \sim sont des cas particuliers de O .

Comparaison asymptotiques usuelles

Comparaison asymptotiques usuelles, stirling

Soit $k \in \mathbb{R}_+^*$, $q > 1$, au voisinage de l'infini :

$$n^k = o(q^n)$$

$$q^n = o(n!)$$

$$n! \sim \sqrt{2\pi n} \frac{n^n}{e^n}$$

$$\ln(n!) \sim n \ln n$$

$$\sum_{k=1}^n \frac{1}{n} = \ln n + \gamma + o(1)$$

Fonctions K -Lipschitziennes

Qu'est qu'une fonction K -lipschitzienne

Une fonction $f : A \rightarrow \mathbb{R}$ est K -lipschitzienne si

$$\forall x, y \in A, |f(x) - f(y)| \leq K|x - y|$$

Lipschitz sur un segment
implique uniformément continue.

Théorème des bornes atteintes

Théorème des bornes atteintes et démonstration.

Si f est $C^0([a, b])$, alors f est bornée et atteint ses bornes.

Preuve :

Notons $M = \sup f$, quitte à avoir $M \in \overline{\mathbb{R}}$. $M \in \text{adh}_{\overline{\mathbb{R}}}(f([a, b]))$, donc il existe une suite (x_n) à valeur dans $[a, b]$ tel que $f(x_n) \rightarrow M$.

Par Bolzano-Weiestrass, il existe φ tel que $x_{\varphi(n)} \rightarrow l$ avec $l \in [a, b]$ et donc nécessairement $M \in \mathbb{R}$.

Théorème de Heine

Énoncé et démonstration du théorème de Heine.

Toute fonction continue sur un segment est uniformément continue.

Preuve :

Soit $f \in C^0([a, b])$. Supposons par l'absurde que f n'est pas uniformément continue.

$$\exists \varepsilon > 0, \forall \delta > 0, \exists x, y \in [a, b] \\ |x - y| < \delta \text{ et } |f(x) - f(y)| \geq \varepsilon$$

On prend $(x_n), (y_n) \in [a, b]^{\mathbb{N}}$ tel que

$$\forall n \in \mathbb{N}, |x_n - y_n| < \frac{1}{n} \\ |f(x_n) - f(y_n)| \geq \varepsilon$$

Ces suites sont bornées donc par Bolzano-Weiestrass, il existe une extractrice φ tel que $x_{\varphi(n)} \rightarrow l \in [a, b]$.

Or $|x_{\varphi(n)} - y_{\varphi(n)}| \rightarrow 0$ donc $y_{\varphi(n)} \rightarrow l$.

Mais par continuité de f ,

$$\lim_{n \rightarrow \infty} f(x_{\varphi(n)}) = \lim_{n \rightarrow \infty} f(y_{\varphi(n)}) \\ = f(l)$$

Donc il existe $N \in \mathbb{N}$ tel que

$$|f(x_{\varphi(n)}) - f(y_{\varphi(n)})| < \varepsilon$$

Qui est absurde.

Fonctions trigonometriques réciproques

Domaine de définition et
dérivées des fonctions
trigonometrique réciproques.

$$\begin{aligned} \arccos &: [-1, 1] \rightarrow [0, \pi] \\ \arccos' &:]-1, 1[\rightarrow [-1, -\infty[\\ x &\mapsto -\frac{1}{\sqrt{1-x^2}} \end{aligned}$$

$$\begin{aligned} \arcsin &: [-1, 1] \rightarrow \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \\ \arcsin' &:]-1, 1[\rightarrow [1, +\infty[\\ x &\mapsto \frac{1}{\sqrt{1-x^2}} \end{aligned}$$

$$\begin{aligned} \arctan &: \mathbb{R} \rightarrow \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[\\ \arctan' &: \mathbb{R} \rightarrow]0, 1] \\ x &\mapsto \frac{1}{1+x^2} \end{aligned}$$

Propriété des extrémum locaux

Que peut on dire si $f : I \rightarrow \mathbb{R}$ et dérivable et admet un extrémum local en $a \in I \setminus \{\inf I, \sup I\}$.

Soit $f : I \rightarrow \mathbb{R}$ dérivable qui admet un extrémum local en a , un point intérieur à I , alors $f'(a) = 0$.

Preuve : par hypothèse, pour un maximum (un minimum se traite de même)

$$\exists V \in \mathcal{V}(a), \forall x \in V, f(x) \leq f(a)$$

Études

$$\lim_{x \rightarrow a} \frac{f(x) - f(a)}{x - a}$$

Si $x < a$:

Si $x > a$:

$$\overbrace{\frac{f(x) - f(a)}{x - a}}^{\leq 0} \geq 0 \quad \overbrace{\frac{f(x) - f(a)}{x - a}}^{\leq 0} \leq 0$$

$\underbrace{x - a}_{< 0}$
 $\underbrace{x - a}_{> 0}$

Donc $f'(a) = 0$ (les deux limites sont égales par la dérivabilité de f en a).

Théorème de Rolle, théorème des accroissements finis

Énoncé et preuve des théorèmes de Rolle et des accroissements finis.

Soit $f \in C^0([a, b])$ dérivable sur $]a, b[$

Rolle Si $f(a) = f(b)$, alors

$$\exists c \in]a, b[, f'(c) = 0$$

TAF

$$\exists c \in]a, b[, f'(c) = \frac{f(b) - f(a)}{b - a}$$

Preuve :

- Rolle : théorème des bornes atteintes, propriétés des extrémum locaux avec une disjonction de cas si les extrémums sont aux bornes.
- TAF : Rolle en pente, on corrige par la pente pour se ramener à Rolle.

Inégalité des accroissements finis et de Taylor-Lagrange

Inégalité des accroissements finis et de Taylor-Lagrange.

Inégalité des accroissements finis

Soit $f : I \rightarrow \mathbb{R}$ dérivable et $a \in I$, pour tout $x \in I$

$$|f(x) - f(a)| \leq \sup_{[a,x]} |f'| \cdot |x - a|$$

Inégalité de Taylor-Lagrange

Soit $f : I \rightarrow \mathbb{R}$ qui est D^{n+1} et $a \in I$, pour tout $x \in I$

$$\left| f(x) - \sum_{k=0}^n f^{(k)}(a) \frac{(x-a)^k}{k!} \right| \leq \sup_{[a,x]} |f^{(n+1)}| \cdot \frac{|x-a|^{n+1}}{(n+1)!}$$

Preuve :

On prend les théorème et on majore le paramètre.

Intégration de l'inverse d'un trinôme

Méthode d'intégration pour l'inverse d'un trinôme du second degré.

On prend $ax^2 + bx + c$ un trinôme du second degré, on vas intégrer $\frac{1}{ax^2+bx+c}$.

- $\Delta > 0$: décomposition en éléments simples
- $\Delta = 0$:

$$\begin{aligned}\int \frac{dx}{ax^2 + bx + c} &= \int \frac{dx}{a(x - r)^2} \\ &= -\frac{1}{a(x - r)}\end{aligned}$$

- $\Delta < 0$: on passe à la forme canonique

$$\begin{aligned}ax^2 + bx + c \\ = a \left[\left(x + \frac{b}{2a} \right)^2 + \frac{|\Delta|}{4a^2} \right]\end{aligned}$$

Et on se ramène à $\int \frac{du}{u^2+1} = \arctan u$.

$$\begin{aligned}\int \frac{1}{ax^2 + bx + c} \\ = \frac{2}{\sqrt{|\Delta|}} \arctan \left(\frac{2ax + b}{\sqrt{|\Delta|}} \right)\end{aligned}$$

Développements limités

$$\frac{1}{1-x} = ?$$

$$\operatorname{ch}(x) = ?$$

$$\operatorname{sh}(x) = ?$$

$$\frac{1}{1+x} = ?$$

$$(1+x)^\alpha = ?$$

$$\ln(1+x) = ?$$

$$\frac{1}{\sqrt{1-x^2}} = ?$$

$$e^x = ?$$

$$\arcsin(x) = ?$$

$$e^{-x} = ?$$

$$\arccos(x) = ?$$

$$\cos(x) = ?$$

$$\arctan(x) = ?$$

$$\sin(x) = ?$$

$$\tan(x) = ?$$

$$\frac{1}{1-x} = 1 + x + x^2 + o(x^2)$$

$$= \sum_{k=0}^n x^k + o(x^n)$$

$$\frac{1}{1+x} = 1 - x + x^2 + o(x^2)$$

$$= \sum_{k=0}^n (-x)^k + o(x^n)$$

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + o(x^3)$$

$$= \sum_{k=0}^n \frac{(-x)^{k+1}}{k+1} + o(x^n)$$

$$e^x = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + o(x^3)$$

$$= \sum_{k=0}^n \frac{x^k}{k!} + o(x^n)$$

$$e^{-x} = 1 - x + \frac{x^2}{2} - \frac{x^3}{6} + o(x^3)$$

$$= \sum_{k=0}^n \frac{(-x)^k}{k!} + o(x^n)$$

$$\cos(x) = 1 - \frac{x^2}{2} + \frac{x^4}{24} + o(x^5)$$

$$= \sum_{k=0}^n (-1)^k \frac{x^{2k}}{(2k)!} + o(x^{2k})$$

$$\sin(x) = x - \frac{x^3}{6} + \frac{x^5}{120} + o(x^6)$$

$$= \sum_{k=0}^n \frac{(-1)^k x^{2k+1}}{(2k+1)!} + o(x^{2k+1})$$

$$\operatorname{ch}(x) = 1 + \frac{x^2}{2} + \frac{x^4}{24} + o(x^5)$$

$$= \sum_{k=0}^n \frac{x^{2k}}{(2k)!} + o(x^{2k})$$

$$\operatorname{sh}(x) = x + \frac{x^3}{6} + \frac{x^5}{120} + o(x^6)$$

$$= \sum_{k=0}^n \frac{x^{2k+1}}{(2k+1)!} + o(x^{2k+1})$$

$$(1+x)^\alpha = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2} x^2 + o(x^2)$$

$$= \sum_{k=1}^n \frac{x^k}{k!} \prod_{p=0}^{k-1} (\alpha - p) + o(x^n)$$

$$\frac{1}{\sqrt{1-x^2}} = 1 + \frac{1}{2} x^2 + \frac{3}{8} x^4 + o(x^4)$$

$$= \sum_{k=1}^n \frac{1}{2^{2k}} \binom{2k}{k} x^{2k} + o(x^{2k})$$

$$\arcsin(x) = x + \frac{1}{2} \frac{x^3}{3} + \frac{3}{8} \frac{x^5}{5} + o(x^5)$$

$$= \sum_{k=1}^n \frac{\binom{2k}{k} x^{2k+1}}{2^{2k} (2k+1)} + o(x^{2n+1})$$

$$\arccos(x) = -x - \frac{1}{2} \frac{x^3}{3} - \frac{3}{8} \frac{x^5}{5} + o(x^5)$$

$$= \sum_{k=1}^n -\frac{\binom{2k}{k} x^{2k+1}}{2^{2k} (2k+1)} + o(x^{2n+1})$$

$$\arctan(x) = x - \frac{x^3}{3} + \frac{x^5}{5} + o(x^5)$$

$$= \sum_{k=1}^n \frac{(-1)^k x^{2k+1}}{2k+1} + o(x^{2n+1})$$

$$\tan(x) = x + \frac{1}{3} x^3 + \frac{2}{15} x^5 + \frac{17}{315} x^7 + o(x^8)$$

Étude local et asymptotique de fonctions

Méthode pour étudié le
comportement local et
asymptotique d'une fonction.

Local au voisinage de $a \in \mathbb{R}$

- Équivalent en a : premier terme
- Tangente en a : $DL_1(a)$
- Signe de f en a : premier terme non nul.
- Position relative par rapport à la tangente : signe du premier terme non nul après l'ordre 1.

Asymptotique au voisinage de $\pm\infty$

- Asymptote oblique : $DL_1(\pm\infty)$
- Position relative : signe du terme suivant.

Rappelle :

f admet une asymptote oblique
d'équation $ax + b$ si

$$\lim_{x \rightarrow \pm\infty} f(x) - ax - b = 0$$

Suites récurrentes

Méthode pour les suites récurrentes de la forme $u_{n+1} = f(u_n)$.

Soit f une fonction et $(u_n) \in \mathbb{R}^{\mathbb{N}}$ tel que $u_{n+1} = f(u_n)$.

1. Intervalle stable : on cherche I tel que $f(I) \subseteq I$.
2. Variations de (u_n)
 - Signe de $f(x) - x$ sur I
 - $+$: (u_n) est croissante
 - $-$: (u_n) est décroissante
 - Sinon affiner I
 - Monotonie de f
 - Si f est croissante sur I , (u_n) est monotone
 - Si f est décroissante sur I , (u_{2n}) et (u_{2n+1}) sont monotone.
3. On montre l'existence de la limite (limite croissante)
4. On la détermine : il s'agit de l'un des points fixes de I (idéalement il n'y en a qu'un).

Dans le cas des fonctions décroissantes, on cherche les limites des deux sous-suites, points fixes de $f \circ f$.

Propriétés de convexité

Définition et propriétés de convexité.

Soit $f : I \rightarrow \mathbb{R}$, f est dite convexe si

$$\begin{aligned} \forall x, y \in I, \forall \lambda \in [0, 1] \\ f(\lambda x + (1 - \lambda)y) \\ \leq \lambda f(x) + (1 - \lambda)f(y) \end{aligned}$$

Propriétés :

- Soit $f : I \rightarrow \mathbb{R}$ convexe,

$$\forall x_1, \dots, x_n \in I$$

$$\forall \lambda_1, \dots, \lambda_n \in [0, 1], \lambda_1 + \dots + \lambda_n = 1 \Rightarrow$$

$$f\left(\sum_{i=1}^n \lambda_i x_i\right) \leq \sum_{i=1}^n \lambda_i f(x_i)$$

- Soit Φ convexe, $\forall f \in C^0([a, b])$

$$\begin{aligned} \Phi\left(\frac{1}{b-a} \int_a^b f(x) dx\right) \\ \leq \frac{1}{b-a} \int_a^b \Phi(f(x)) dx \end{aligned}$$

- Soit $f : I \rightarrow \mathbb{R}$, $a \in I$, on note

$$\begin{aligned} \tau_a : I \setminus \{a\} &\rightarrow \mathbb{R} \\ x &\mapsto \frac{f(x) - f(a)}{x - a} \end{aligned}$$

les taux d'accroissements en a de f .

f est convexe ssi $\forall a \in I, \tau_a$ est croissante.

- Soit $f : I \rightarrow \mathbb{R}$, on appelle droite d'appuis en x_0 de f une droite $y = ax + b$ tel que

- $\forall x \in I, ax + b \leq f(x)$
- $f(x_0) = ax_0 + b$

Si f convexe, f admet des droites d'appuis en tout points.

Propriétés élémentaires sur les séries

Propriétés élémentaires sur les séries.

- Soit $(u_n) \in \mathbb{K}^{\mathbb{N}}$ et $S_n = \sum_{k=0}^n u_k$, on dit que $\sum u_n$ converge si (S_n) converge.
- Si $\sum u_n$ converge alors

$$(u_n) \xrightarrow{n \rightarrow +\infty} 0$$

- La suite (u_n) converge ssi la série $\sum (u_{n+1} - u_n)$ converge.
- L'ensemble \mathcal{S} des séries convergentes est un sev de l'espace des suites, et l'application

$$\begin{aligned} \varphi : \mathcal{S} &\rightarrow \mathbb{K} \\ (u_n) &\mapsto \sum_{n=0}^{+\infty} u_n \end{aligned}$$

est linéaire.

- Si $(u_n) \in \mathbb{R}_+^{\mathbb{N}}$ alors $\sum u_n$ converge ssi (S_n) est majoré (théorème de la limite monotone).

Théorème de comparaison des séries positives

Énoncé et démonstration du théorème de comparaison des séries positives.

Soient $(u_n), (v_n) \in \mathbb{R}_+^{\mathbb{N}}$ alors

1. Si $\forall n \geq n_0, u_n \leq v_n$ et $\sum v_n$ converge alors $\sum u_n$ converge.
2. Si $u_n = O_{n \rightarrow +\infty}(v_n)$ et $\sum v_n$ converge alors $\sum u_n$ converge.
3. Si $u_n \underset{n \rightarrow +\infty}{\sim} v_n$ alors $\sum u_n$ converge ssi $\sum v_n$ converge.

Démonstration :

1. (S_n) est majoré par (\tilde{S}_n) qui est fini.
2. (S_n) est majoré par $M \cdot \tilde{S}_n$ qui est fini.
3. $u_n \sim v_n$ implique $u_n = O(v_n)$ et $v_n = O(u_n)$.

Comparaison série intégrale

Propriétés et methode de comparaison série intégrale.

Pour $f \in C_{\text{pm}}^0([a, +\infty[, \mathbb{R}_+)$,
décroissante, $\forall n \geq [a] + 1 = N_0$

$$\begin{aligned} f(n) &\geq \int_n^{n+1} f(t) dt \\ &\leq \int_{n-1}^n f(t) dt \end{aligned}$$

D'où

$$\begin{aligned} \sum_{n=N_0}^N f(n) &\geq \int_{N_0}^{N+1} f(t) dt \\ &\leq \int_{N_0-1}^N f(t) dt \end{aligned}$$

Ainsi $\sum f(n)$ converge ssi $\int_{N_0}^{+\infty} f$ converge.

Et de plus (à redémontrer) :

$$\begin{aligned} \sum \left(\int_{n-1}^n f(t) dt - f(n) \right) \\ \sum \left(f(n) - \int_n^{n+1} f(t) dt \right) \end{aligned}$$

sont à terme général positif et convergent car

$$\begin{aligned} f(n) &\leq \int_{n-1}^n f \leq f(n+1) \\ 0 &\leq \int_{n-1}^n f - f(n) \leq f(n+1) - f(n) \end{aligned}$$

Et $\sum f(n+1) - f(n)$ est positive et converge (série télescopique) car f converge (positive et décroissante).

Dans le cas f non monotone :

Si $f \in C^1$ et $\int_n^{+\infty} |f'|$ converge

$$\begin{aligned} \int_k^{k+1} f &= \underbrace{[(t-k-1)f(t)]_k^{k+1}}_{f(k)} \\ &\quad - \int_k^{k+1} (t-k-1)f'(t) dt \\ \int_1^{N+1} f &= \sum_{k=1}^N f(k) \\ &\quad + \sum_{k=1}^N \int_k^{k+1} (k+1-t)f'(t) dt \end{aligned}$$

Or pour tout $k \geq 1$

$$\left| \int_k^{k+1} (k+1-t)f'(t) dt \right| \leq \int_k^{k+1} |f'|$$

Qui est le terme général d'une série convergente d'où

$$\begin{aligned} \sum f(n) &\text{ converge} \\ \text{ssi } \left(\int_1^N f \right)_N &\text{ converge} \\ \text{ssi } \int_1^{+\infty} f &\text{ converge} \end{aligned}$$

Séries de Bertrand

Définitions et propriétés des séries de Bertrand.

Soit $\alpha, \beta \in \mathbb{R}$, la série $\sum \frac{1}{n^\alpha (\ln n)^\beta}$ est appelée série de Bertrand.

Cette série converge ssi $\alpha > 1$ ou $\alpha = 1$ et $\beta > 1$.

Démonstration :

- Cas $\alpha > 1$ comparaison avec les séries de Riemann, en prenant $\gamma \in]1, \alpha[$.
- Cas $\alpha < 1$ même chose avec $\gamma \in]\alpha, 1]$.
- Cas $\alpha = 1$, comparaison série intégrale avec $t \mapsto \frac{1}{t(\ln t)^\beta}$.

Recherche d'équivalent d'une suite

Méthodes de recherche
d'équivalents.

Si on cherche un équivalent
d'une suite (u_n)

- Étudier la série $\sum(u_{n+1} - u_n)$
ou $\sum(u_n - u_{n+1})$, sommes
partielles ou restes (voir
théorème de sommation des
relations de comparaison).
- Chercher $\alpha \in \mathbb{R}^*$ tel que $u_{n+1}^\alpha - u_n^\alpha \xrightarrow{n \rightarrow +\infty} l \in \mathbb{R}^*$, pour avoir

$$u_n^\alpha - u_0^\alpha = \sum_{k=0}^{n-1} u_{k+1}^\alpha - u_k^\alpha \underset{n \rightarrow +\infty}{\sim} nl$$

Absolue convergence

Définitions et démonstration du théorème de l'absolue convergence d'une série.

Une série $\sum u_n$ (dans \mathbb{R} ou \mathbb{C}) est dite absolument convergente si $\sum |u_n|$ converge. Si $\sum u_n$ est absolument convergente, alors elle est convergente.

Démonstration : on étudie $((u_n)_+)$ et $((u_n)_-)$ pour le cas réel, puis $(\operatorname{Re}(u_n))$ et $(\operatorname{Im}(u_n))$ pour le cas imaginaire, à chaque fois on majore par le module et on applique les théorèmes de comparaison des séries positives.

Théorème des séries alternées

Énoncer et démonstration du théorème des séries alternées.

Si $(u_n) \in \mathbb{R}_+^{\mathbb{N}}$ décroissante tel que $u_n \xrightarrow{n \rightarrow +\infty} 0$, alors $\sum u_n$ converge et $R_n = \sum_{k=n+1}^{+\infty} u_k = S - S_n$ est du signe du premier terme et $|R_n| \leq |u_{n+1}|$.

Démonstration : on montre que les suites S_{2n} et S_{2n+1} sont adjacentes et on étudie R_{2n} et R_{2n+1} .

Transformation d'Abel

Définition et applications de la transformation d'Abel.

Il s'agit d'une sorte d'IPP sur les séries. Soit (a_n) et (b_n) deux suites, la transformation d'Abel est utile si on a des hypothèses sur $S_n = \sum_{k=0}^n a_k$. On pose $S_{-1} = 0$.

$$\begin{aligned} \sum_{k=0}^n a_k b_k &= \sum_{k=0}^n (S_k - S_{k-1}) b_k \\ &= \sum_{k=0}^n S_k b_k - \sum_{k=0}^n S_{k-1} b_k \\ &= S_n b_n - \sum_{k=0}^{n-1} S_k (b_{k+1} - b_k) \end{aligned}$$

Applications :

$$\begin{aligned} \sum \frac{\sin(n\theta)}{n^\alpha} \\ \sum \frac{\cos(n\theta)}{n^\alpha} \\ \sum \frac{e^{in\theta}}{n^\alpha} \end{aligned}$$

Remarque : on peut aussi écrire $a_k = R_{k-1} - R_k$, qui peut être intéressant si $\sum a_n$ converge.

Règle de Raabe-Duhamel

Énoncé et démonstration de la règle de Raab-Duchamel.

Soit $(a_n) \in (\mathbb{R}_+^*)^{\mathbb{N}}$, $\frac{a_{n+1}}{a_n} \xrightarrow{n \rightarrow +\infty} 1$ et

$$\frac{a_{n+1}}{a_n} = 1 - \frac{\alpha}{n} + O_{n \rightarrow +\infty} \left(\frac{1}{n^{1+h}} \right), \quad h > 0$$

On considère $n^\alpha a_n = u_n$, on veut montrer que $u_n \xrightarrow{n \rightarrow +\infty} l \in \mathbb{R}_+^*$, c'est dire que $(\ln(u_n))$ a une limite réelle. On étudie $\sum \ln(u_{n+1}) - \ln(u_n)$.

$$\begin{aligned} \ln(u_{n+1}) - \ln(u_n) &= \ln\left(\frac{a_{n+1}}{a_n}\right) + \alpha \ln\left(\frac{n+1}{n}\right) \\ &= \ln\left(1 - \frac{\alpha}{n} + O\left(\frac{1}{n^{1+h}}\right)\right) + \alpha \ln\left(1 + \frac{1}{n}\right) \\ &= \frac{\alpha}{n} - \frac{\alpha}{n} + O\left(\frac{1}{n^{1+h}}\right) + O\left(\frac{1}{n^2}\right) \\ &= O\left(\frac{1}{n^{\min(2, 1+h)}}\right) \end{aligned}$$

Donc par le théorème de comparaison des séries à terme positifs (en valeur absolue)

$\sum \ln(u_{n+1}) - \ln(u_n)$ converge, d'où (u_n) converge.

Ainsi $n^\alpha a_n \xrightarrow{n \rightarrow +\infty} e^l$, donc $a_n \sim \frac{e^l}{n^\alpha}$, $\sum a_n$ converge ssi $\alpha > 1$.

Théorème de sommutation des relations de comparaison pour les séries

Énoncés des théorèmes de sommation des relations de comparaison pour les séries.

Pour les restes de séries convergentes :

Si $(u_n) \in \mathbb{K}^{\mathbb{N}}$, $(a_n) \in \mathbb{R}_+^{\mathbb{N}}$ et $\sum a_n$ converge.

1. Si $u_n = O(a_n)$, alors $\sum u_n$ converge absolument et

$$\sum_{k=n+1}^{+\infty} u_k = O\left(\sum_{k=n+1}^{+\infty} a_k\right)$$

2. Si $u_n = o(a_n)$, alors $\sum u_n$ converge absolument et

$$\sum_{k=n+1}^{+\infty} u_k = o\left(\sum_{k=n+1}^{+\infty} a_k\right)$$

3. Si $u_n \sim a_n$, alors

$$\sum_{k=n+1}^{+\infty} u_k \sim \sum_{k=n+1}^{+\infty} a_k$$

Démonstration : on repasse par les définitions de o et O : $\exists N \in \mathbb{N}$, $\forall n \geq N$, $|u_n| \leq K a_n$, avec $K > 0$ fixé pour O et $K = \varepsilon > 0$ pour o . Pour \sim , on a $u_n - a_n = o(a_n)$.

Pour les sommes partielles de séries divergentes :

Si $(u_n) \in \mathbb{K}^{\mathbb{N}}$, $(a_n) \in \mathbb{R}_+^{\mathbb{N}}$ et $\sum a_n$ diverge.

1. Si $u_n = O(a_n)$, alors $\sum u_n$ converge absolument et

$$\sum_{k=0}^n u_k = O\left(\sum_{k=0}^n a_k\right)$$

2. Si $u_n = o(a_n)$, alors $\sum u_n$ converge absolument et

$$\sum_{k=0}^n u_k = o\left(\sum_{k=0}^n a_k\right)$$

3. Si $u_n \sim a_n$, alors

$$\sum_{k=0}^n u_k \sim \sum_{k=0}^n a_k$$

Démonstration : même que pour l'autre, on à juste à découper la somme entre avant et après un certain rang (pour o et O).

Équivalents de référence : séries de Riemann

Équivalent des restes ou sommes partielles des séries de Riemann (à redémontrer).

Par comparaison série intégrale :

- Pour $1 \geq \alpha > 0$

$$\int_1^{n+1} \frac{dt}{t^\alpha} \leq 1 + \sum_{k=1}^n \frac{1}{k^\alpha} \leq \int_2^n \frac{dt}{t^\alpha}$$

$$S_n(\alpha) = \sum_{k=1}^n \frac{1}{k^\alpha} \underset{n \rightarrow +\infty}{\sim} \frac{n^{1-\alpha}}{1-\alpha}$$

- Pour $\alpha > 0$

$$\int_{n+1}^{+\infty} \frac{dt}{t^\alpha} \leq \sum_{k=n+1}^{+\infty} \frac{1}{k^\alpha} \leq \int_n^{+\infty} \frac{dt}{t^\alpha}$$

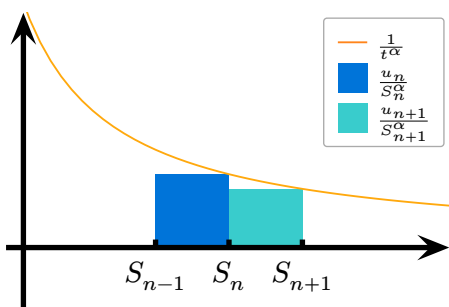
$$R_n(\alpha) = \sum_{k=n+1}^{+\infty} \frac{1}{k^\alpha} \underset{n \rightarrow +\infty}{\sim} \frac{1}{\alpha-1} \cdot \frac{1}{n^{\alpha-1}}$$

Exercice : Nature de la série terme général sur somme partielle

Démonstration de la CNS sur α de la convergence de la série $\sum \frac{u_n}{S_n^\alpha}$ (avec $\sum u_n$ divergente).

Soit $(u_n) \in (\mathbb{R}_+^*)^{\mathbb{N}}$, $\sum u_n$ diverge, et $\alpha \in \mathbb{R}$. On note $S_n = \sum_{k=1}^n u_k$.

- Si $\alpha > 1$:



Donc pour $t \in [S_{n-1}, S_n]$

$$\frac{1}{t^\alpha} \geq \frac{1}{S_n^\alpha}$$

$$\sum_{k=1}^n \frac{u_k}{S_k^\alpha} \leq \int_{S_0}^{S_n} \frac{dt}{t^\alpha} = \frac{1}{\alpha-1} \left(\frac{1}{S_0^{\alpha-1}} - \frac{1}{S_n^{\alpha-1}} \right)$$

Or $S_n \xrightarrow{n \rightarrow +\infty} +\infty$ donc

$$\sum_{n=1}^{+\infty} \frac{u_n}{S_n^\alpha} \leq \frac{1}{\alpha-1} \cdot \frac{1}{S_0^{\alpha-1}}$$

- Si $\alpha = 1$:

Si $\frac{u_n}{S_n} \not\rightarrow 0$ la série diverge grossièrement, et sinon

$$\begin{aligned} \frac{u_n}{S_n} &\sim -\ln\left(1 - \frac{u_n}{S_n}\right) \\ &\sim \ln(S_n) - \ln(S_{n-1}) \end{aligned}$$

Qui est le terme général d'une série télescopique divergente.

- Si $\alpha \leq 1$, on compare avec $\alpha = 1$, car à partir d'un certain rang $S_n \geq 1$.

Familles sommables

Définition et propriétés élémentaires des familles sommables.

Soit I un ensemble non vide.

Pour $(u_i) \in \mathbb{R}_+^I$, on définit

$$\sum_{i \in I} u_i = \sup \left\{ \sum_{j \in J} u_j, J \subseteq I \text{ fini} \right\} \\ \in \mathbb{R}_+ \cup \{+\infty\}$$

Pour une famille $(u_i) \in \mathbb{K}^I$, on dit qu'elle est sommable si

$$\sum_{i \in I} |u_i| < +\infty$$

Si $(u_i)_{i \in I}$ est sommable, alors elle contient un nombre au plus dénombrable d'éléments non nuls (Démonstration : on étudie $J_n = \{i \in I \mid u_i \geq \frac{1}{n}\}$)

Théorème de sommation par paquets

Énoncer et éléments de démonstration du théorème de sommation par paquets.

Soit $(u_i)_{i \in I} \in \mathbb{R}^I$, et $I = \bigsqcup_{n \in \mathbb{N}} I_n$ une partition. La famille (u_i) est sommable ssi

$$(*) : \begin{cases} \forall n \in \mathbb{N}, (u_i)_{i \in I_n} \text{ sommable} \\ \sum \left(\sum_{i \in I_n} |u_i| \right) \text{ converge vers } S \end{cases}$$

Dans ce cas

$$\sum_{i \in I} u_i = \sum_{n=0}^{+\infty} \left(\sum_{i \in I_n} u_i \right)$$

Démonstration :

- Cas positif :
 - ▶ On suppose $(*)$, on prend une sous famille fini J de I , on a donc une famille $(J_n = I_n \cap J)_n$, on note $N = \max(n \in \mathbb{N} \mid J_n \neq \emptyset)$ qui existe car J fini.

$$\begin{aligned} \sum_{j \in J} u_j &= \sum_{n=0}^N \left(\sum_{j \in J_n} u_j \right) \\ &\leq \sum_{n=0}^{+\infty} \left(\sum_{i \in I_n} u_i \right) = S \end{aligned}$$

- ▶ Caractérisation de la borne supérieure, majoration et sous ensembles finis.
- Cas général : D'abord en valeurs absolues, puis parties positives, négatives, réelles et imaginaires.

Critère de convergence d'intégrales usuelles

Critère de convergence d'intégrales usuelles :

$$\int_1^{+\infty} \frac{dt}{t^\alpha}$$

$$\int_0^1 \frac{dt}{t^\alpha}$$

$$\int_2^{+\infty} \frac{dt}{t^\alpha (\ln t)^\beta}$$

$$\int_0^{\frac{1}{2}} \frac{dt}{t^\alpha (\ln t)^\beta}$$

-
- $\int_1^{+\infty} \frac{dt}{t^\alpha}$ converge vers $\frac{1}{\alpha-1}$ ssi $\alpha > 1$.
 - $\int_0^1 \frac{dt}{t^\alpha}$ converge vers $\frac{1}{1-\alpha}$ ssi $\alpha < 1$.
 - $\int_2^{+\infty} \frac{dt}{t^\alpha (\ln t)^\beta}$ converge ssi $\alpha > 1$ ou $\alpha = 1$ et $\beta > 1$
 - $\int_0^{\frac{1}{2}} \frac{dt}{t^\alpha (\ln t)^\beta}$ converge ssi $\alpha < 1$ ou $\alpha = 1$ et $\beta > 1$

Fonction gamma

Définition, convergence et démonstration de la fonction Γ .

On définit

$$\Gamma(x) = \int_0^{+\infty} e^{-t} t^{x-1} dt$$

- Qui converge pour $x > 0$.
- Pour $x > 0$

$$\Gamma(x+1) = x\Gamma(x)$$

- $\Gamma(1) = 1$

$t \mapsto e^{-t} t^{x-1}$ est C_{pm}^0 sur $]0, +\infty[$.

- Sur $[1, +\infty[$

$$\begin{aligned} e^{-t} t^{x-1} &= o_{t \rightarrow +\infty} \left(e^{-\frac{t}{2}} \right) \\ &= o_{t \rightarrow +\infty} \left(\frac{1}{t^2} \right) \end{aligned}$$

Or $\int_1^{+\infty} e^{-\frac{t}{2}} dt$ converge, donc par le théorème de comparaison d'intégrales de fonctions positives, $\int_1^{+\infty} e^{-t} t^{x-1} dt$ converge.

- Sur $]0, 1]$

$$e^{-t} t^{x-1} \underset{t \rightarrow 0_+}{\sim} \frac{1}{t^{1-x}}$$

Or $\int_0^1 \frac{dt}{t^{1-x}}$ converge ssi $1-x < 1$ d'où $x > 0$, et on conclut par le même théorème.

$$\begin{aligned} \Gamma(x+1) &= \int_0^{+\infty} e^{-t} t^x dt \\ &= [-e^{-t} t^x]_0^{+\infty} + x \int_0^{+\infty} e^{-t} t^{x-1} dt \\ &= x\Gamma(x) \end{aligned}$$

Intégrales de Wallis

Définition, propriétés et démonstration des intégrales de Wallis.

On pose pour $n \in \mathbb{N}$

$$\begin{aligned} W_n &= \int_0^{\frac{\pi}{2}} (\cos t)^n dt \\ &= \int_0^{\frac{\pi}{2}} (\sin \theta)^n d\theta \quad (\theta = \frac{\pi}{2} - t) \end{aligned}$$

Relation de récurrence

$$\begin{aligned} W_{n+2} &= \int_0^{\frac{\pi}{2}} (\sin t)^{n+2} dt \\ &= \underbrace{\left[-\cos(t) \sin(t)^{n+1} \right]_0^{\frac{\pi}{2}}}_0 \\ &\quad + (n+1) \int_0^{\frac{\pi}{2}} (\sin t)^n \underbrace{(\cos t)^2}_{1 - (\sin t)^2} dt \\ &= (n+1)W_n - (n+1)W_{n+2} \\ &= \frac{n+1}{n+2} W_n \end{aligned}$$

Formules explicites

$$W_0 = \frac{\pi}{2}$$

$$W_1 = 1$$

$$W_{2n} = \frac{(2n)!}{2^{2n} (n!)^2} \frac{\pi}{2}$$

$$W_{2n+1} = \frac{2^{2n} (n!)^2}{(2n+1)!}$$

Équivalents

Pour $t \in [0, \frac{\pi}{2}]$

$$0 \leq (\sin t)^{n+2} \leq (\sin t)^{n+1} \leq (\sin t)^n$$

$$0 \leq W_{n+2} \leq W_{n+1} \leq W_n$$

$$\frac{n+1}{n+2} \leq \frac{W_{n+1}}{W_n} \leq 1$$

D'où

$$W_{n+1} \underset{n \rightarrow +\infty}{\sim} W_n$$

$$W_{2n}^2 \underset{n \rightarrow +\infty}{\sim} W_{2n+1}^2$$

$$\underset{n \rightarrow +\infty}{\sim} W_{2n} W_{2n+1} = \frac{\pi}{4n+2}$$

Ainsi

$$W_{2n+1} \underset{n \rightarrow +\infty}{\sim} \sqrt{\frac{\pi}{4n+2}}$$

$$W_{2n} \underset{n \rightarrow +\infty}{\sim} \sqrt{\frac{\pi}{4n}}$$

Lemme de Riemann-Lebesgue

Énoncé et démonstration du lemme de Riemann-Lebesgue.

Si I est un Intervalle de \mathbb{R} , et $f \in C_{\text{pm}}^0(I, \mathbb{K})$ intégrable sur I , alors

$$\begin{aligned}\int_I f(t) e^{i\lambda t} dt &\xrightarrow{\lambda \rightarrow \infty} 0 \\ \int_I f(t) \cos(\lambda t) dt &\xrightarrow{\lambda \rightarrow \infty} 0 \\ \int_I f(t) \sin(\lambda t) dt &\xrightarrow{\lambda \rightarrow \infty} 0\end{aligned}$$

Démonstration

- Si f est C^1 sur un segment : par IPP, on dérive f , f' étant continue sur un segment elle est uniformément continue sur ce segment (théorème de Heine), et est donc bornée (théorème des bornes atteintes).
- On montre d'abord pour I segment.
 - ▶ On traite le cas f constante.
 - ▶ On généralise à f en escalier.
 - ▶ Par densité des fonctions en escalier on étend aux fonctions continues.
- On étend finalement aux intervalles quelconques.

Hölder

Inégalité de Hölder et démonstration.

Soit $p, q \in \mathbb{R}_+^*$ tels que $\frac{1}{p} + \frac{1}{q} = 1$.

Pour $x_1, \dots, x_n, y_1, \dots, y_n \in \mathbb{R}_+$

$$\sum_{i=1}^n x_i y_i \leq \left(\sum_{i=1}^n x_i^p \right)^{\frac{1}{p}} \left(\sum_{i=1}^n y_i^q \right)^{\frac{1}{q}}$$

Démonstration

- Pour tout $x, y \in \mathbb{R}_+$

$$xy \leq \frac{1}{p} x^p + \frac{1}{q} y^q$$

Le cas nul se traite facilement, puis on utilise la concavité de \ln sur \mathbb{R}_+^* :

$$\begin{aligned} \ln \left(\frac{1}{p} x^p + \frac{1}{q} y^q \right) &\geq \frac{1}{p} \ln(x^p) + \frac{1}{q} \ln(y^q) \\ &= \ln(xy) \end{aligned}$$

$$\frac{1}{p} x^p + \frac{1}{q} y^q \geq xy$$

- On traite d'abord le cas où l'un des vecteurs (X ou Y) est nul.
- On traite ensuite le cas où

$$\sum_{i=1}^n x_i^p = 1 \quad \text{et} \quad \sum_{j=1}^n y_j^q = 1$$

Pour tout $i \in \llbracket 1, n \rrbracket$

$$x_i y_i \leq \frac{1}{p} x_i^p + \frac{1}{q} y_i^q$$

$$\begin{aligned} \sum_{i=1}^n x_i y_i &\leq \underbrace{\frac{1}{p} \sum_{i=1}^n x_i^p}_1 + \underbrace{\frac{1}{q} \sum_{i=1}^n y_i^q}_1 \\ &\leq 1 = \left(\sum_{i=1}^n x_i^p \right)^{\frac{1}{p}} \left(\sum_{i=1}^n y_i^q \right)^{\frac{1}{q}} \end{aligned}$$

- Enfin dans le cas général, on pose pour $i \in \llbracket 1, n \rrbracket$

$$\tilde{x}_i = \frac{x_i}{\sum_{i=1}^n x_i} \quad \tilde{y}_i = \frac{y_i}{\sum_{i=1}^n y_i}$$

Et ça marche.

Norme

Définition d'une norme sur un \mathbb{K} -ev E .

Une norme sur un \mathbb{K} -ev E est une application $N : E \rightarrow \mathbb{R}_+$ tel que

1. Homogénéité : $\forall \lambda \in \mathbb{K}, x \in E$

$$N(\lambda x) = |\lambda|N(x)$$

2. Inégalité triangulaire : $\forall x, y \in E$

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

3. Séparation : $\forall x \in E$

$$N(x) = 0 \Rightarrow x = 0$$

Norme euclidienne

Définition et propriétés des normes euclidiennes.

Pour E un \mathbb{R} -ev un produit scalaire est une forme bilinéaire symétrique définie positive.

Pour un produit scalaire $\langle \cdot | \cdot \rangle$ on a l'Inégalité de Cauchy-Schwartz :

$$\forall x, y \in E$$

$$\langle x|y \rangle^2 \leq \langle x|x \rangle \cdot \langle y|y \rangle$$

Avec cas d'égalité si (x, y) liée.

D'un produit scalaire dérive une norme (euclidienne)

$$\|\cdot\| : \begin{cases} E \rightarrow \mathbb{R}_+ \\ x \mapsto \sqrt{\langle x|x \rangle} \end{cases}$$

Démonstration

- Si $x = 0$ ou $y = 0$: évident.
Sinon pour $x, y \in E \setminus \{0\}, t \in \mathbb{R}$:

$$\begin{aligned} & \langle x + ty | x + ty \rangle \\ &= t^2 \langle y|y \rangle + 2t \langle x|y \rangle + \langle x|x \rangle \\ &= P(t) \end{aligned}$$

Comme $\langle y|y \rangle > 0$, $\deg P = 2$. De plus par positivité de $\langle \cdot | \cdot \rangle$:

$$\begin{aligned} \Delta &= 4 \langle x|y \rangle^2 - 4 \langle x|x \rangle \cdot \langle y|y \rangle \leq 0 \\ \langle x|y \rangle^2 &\leq \langle x|x \rangle \cdot \langle y|y \rangle \end{aligned}$$

Avec cas d'égalité si $\Delta = 0$, c'est à dire $x + ty = 0$.

- Vérifions les axiomes

1. Soit $\lambda \in \mathbb{R}, x \in E$

$$\begin{aligned} \|\lambda x\| &= \sqrt{\langle \lambda x | \lambda x \rangle} \\ &= |\lambda| \sqrt{\langle x|x \rangle} \\ &= |\lambda| \|x\| \end{aligned}$$

2. Soit $x \in E$ tel que $\|x\| = 0$

$$\begin{aligned} \sqrt{\langle x|x \rangle} &= 0 \\ \langle x|x \rangle &= 0 \\ x &= 0 \end{aligned}$$

3. Soit $x, y \in E$

$$\begin{aligned} & \|x + y\|^2 \\ &= \langle x + y | x + y \rangle \\ &= \|x\|^2 + \|y\|^2 + 2 \langle x|y \rangle \\ &\leq \|x\|^2 + \|y\|^2 + 2 \underbrace{|\langle x|y \rangle|}_{\text{C-S}} \\ &\leq \|x\|^2 + \|y\|^2 + 2 \|x\| \|y\| \\ &= (\|x\| + \|y\|)^2 \end{aligned}$$

Avec égalité ssi $\langle x|y \rangle \geq 0$ et égalité dans C-S : ssi x, y positivement liés.

Norme produit

Définition de la norme produit.

Soit $(E_1, \|\cdot\|_1), \dots, (E_d, \|\cdot\|_d)$ des \mathbb{K} -evn.

On définit la norme produit sur $\prod_{k=1}^d E_k$ comme

$$N : \begin{cases} \prod_{k=1}^d E_k \rightarrow \mathbb{R}_+ \\ \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} \mapsto \max_{k \in \llbracket 1, n \rrbracket} \|x_k\|_k \end{cases}$$

Distance

Définition de distance.

Soit X un ensemble non vide. On appelle distance une application $d : X^2 \rightarrow \mathbb{R}_+$ tel que

1. Symétrie : $\forall x, y \in X$

$$d(x, y) = d(y, x)$$

2. Inégalité triangulaire :

$$\forall x, y, z \in X$$

$$d(x, z) \leq d(x, y) + d(y, z)$$

3. Séparation : $\forall x, y \in X$

$$d(x, y) = 0 \Rightarrow x = y$$

Dans un evn $(E, \|\cdot\|)$ on peut définir la distance sur E associé à la norme $\|\cdot\|$:

$$d : \begin{cases} E^2 & \rightarrow \mathbb{R}_+ \\ (x, y) & \mapsto \|x - y\| \end{cases}$$

Boules et sphères

Définition, propriétés des boules et sphères.

Soit E un espace métrique, $a \in E$ et $r \in \mathbb{R}_+$. On définit les ensembles suivants

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

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

$$\mathbb{S}(a, r) = \{x \in E \mid d(a, x) = r\}$$

Si E est un \mathbb{K} -evn alors on a de plus la convexité de $B(a, r)$ et $B_f(a, r)$.

Points extrémaux d'un convexe

Définition des points extrémaux d'un convexe et points extrémaux d'une boule.

Soit $(E, \|\cdot\|)$ un evn, $K \subseteq E$ convexe. On dit que $x \in K$ est extrémal si

$$\forall y, z \in K, \forall t \in]0, 1[, \\ x = (1 - t)y + tz \Rightarrow x = y = z$$

Si $\|\cdot\|$ dérive d'un produit scalaire, alors pour tout $a \in E$ et $r \in \mathbb{R}_+$, l'ensemble des points extrémaux de $B_f(a, r)$ est $\mathbb{S}(a, r)$.

Démonstration

Pour $r = 1$ et $a = 0$: (auxquels on peut se ramener)

- Soit $x \in B(0, 1)$

$$x = (1 - \|x\|)0 + \|x\| \frac{x}{\|x\|}$$

D'où x pas extrémal (on traite le cas $x = 0$ séparément).

- Soit $x \in \mathbb{S}(0, 1)$, $y, z \in B_f(0, 1)$, $t \in]0, 1[$ tel que

$$x = (1 - t)y + tz \\ \|x\| = 1 \leq (1 - t) \underbrace{\|y\|}_{\leq 1} + t \underbrace{\|z\|}_{\leq 1}$$

On a égalité dans l'inégalité triangulaire : y et z positivement liés (car produit scalaire) et $\|y\| = \|z\|$ d'où $y = z = x$.

Topologie, espace topologique

Définition d'une topologie.

Soit X un ensemble, $T \subseteq \mathcal{P}(X)$ est une topologie sur X si

1. $\{\emptyset, X\} \subseteq T$
2. Pour toute famille $(\Omega_i)_i \in T^I$

$$\bigcup_{i \in I} \Omega_i \in T$$

3. Pour tout $\Omega_1, \dots, \Omega_n \in T$

$$\bigcap_{k=1}^n \Omega_k \in T$$

Les éléments de T sont appelés ouverts de X .

X muni de T est appelé espace topologique.

Topologie sur un espace métrique

Définitions des ouverts / fermés d'un espace métrique.

Soit (E, d) un espace métrique.

On dit que $\Omega \subseteq E$ est un ouvert de E si

$$\forall x \in \Omega, \exists \delta > 0, B(x, \delta) \subseteq \Omega$$

De manière équivalente

$$\forall x \in \Omega, \Omega \in \mathcal{V}(x)$$

L'ensemble T des ouverts de E forme une topologie :

1. \emptyset et E sont ouverts.
2. T est stable par union quelconque.
3. T est stable par intersection finie.

On définit de plus les fermés : le complémentaire d'un ouvert.

Démonstration

1. Évident.
2. Soit $(\Omega_i)_{i \in I} \in T^I$ une famille d'ouverts. Soit $x \in W = \bigcup_{i \in I} \Omega_i$.

On dispose de $i \in I$ tel que $x \in \Omega_i$, ainsi on dispose de plus de $\delta > 0$ tel que

$$B(x, \delta) \subseteq \Omega_i \subseteq W$$

Donc $W \in T$: c'est un ouvert.

3. Soit $F_1, \dots, F_n \in T$, soit $x \in W = \bigcap_{k=1}^n F_k$. Pour tout $k \in \llbracket 1, n \rrbracket$ on dispose de $\delta_k > 0$ tel que

$$B(x, \delta_k) \subseteq F_k$$

$$\delta = \min_{k \in \llbracket 1, n \rrbracket} \delta_k$$

Ainsi on a pour tout $k \in \llbracket 1, n \rrbracket$:

$$B(x, \delta) \subseteq B(x, \delta_k) \subseteq F_k$$

Donc

$$B(x, \delta) \subseteq W$$

Limites de suites

Définitions équivalentes de limites d'une suite.

Soit (E, d) un espace métrique, $u = (u_n)_n \in E^{\mathbb{N}}$. On dit que $l \in E$ est limite de la suite u si l'une des définitions suivantes équivalentes s'applique :

1. $\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, d(u_n, l) < \varepsilon.$
2. $\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, u_n \in B(l, \varepsilon).$
3. $(d(u_n, l))_n \xrightarrow{n \rightarrow \infty} 0.$
4. $\forall V \in \mathcal{V}(l), \exists N \in \mathbb{N}, \forall n \geq N, u_n \in V.$

Si la limite existe, alors elle est unique.

Démonstration

- Équivalence : l'écrire.
- Si $l = \lim_{n \rightarrow \infty} u_n$, prendre $l' \neq l$ et montrer que $(d(l', u_n))_n \not\xrightarrow{n \rightarrow \infty} 0.$

Valeurs d'adhérence d'une suite

Définitions et propriétés sur les valeurs d'adhérence d'une suite.

Soit (E, d) un espace métrique, $u = (u_n)_n \in E^{\mathbb{N}}$ une suite.

On dit que $l \in E$ est une valeur d'adhérence de u s'il existe φ extractrice tel que $(u_{\varphi(n)})_n \xrightarrow{n \rightarrow \infty} l$.

Une suite qui a deux valeurs d'adhérence diverge.

Comparaison de normes

Définitions de comparaison de normes, propriétés.

Soit E un \mathbb{K} -ev, $\|\cdot\|_1$ et $\|\cdot\|_2$ deux normes sur E .

On dit que $\|\cdot\|_2$ est plus fine de $\|\cdot\|_1$ s'il existe $\alpha > 0$ tel que

$$\forall x \in E, \|x\|_1 \leq \alpha \|x\|_2$$

Dans ce cas :

1. Pour tout $a \in E$ et $r > 0$

$$B_2(a, r) \subseteq B_1(a, \alpha r)$$

2. Si $\Omega \subseteq E$ est ouvert pour $\|\cdot\|_1$ est ouvert pour $\|\cdot\|_2$
3. Toute suite bornée pour $\|\cdot\|_1$ l'est pour $\|\cdot\|_2$.
4. Toute suite convergente pour $\|\cdot\|_1$ l'est pour $\|\cdot\|_2$.

On dit que $\|\cdot\|_1$ et $\|\cdot\|_2$ sont équivalentes si chacune est plus fine que l'autre. C'est une relation d'équivalence.

Valeurs propres, espaces propres

Définitions, caractérisation, démonstration autour des valeurs propres et des espaces propres.

Soit $u \in \mathcal{L}(E)$, $\lambda \in \mathbb{K}$, il y a équivalence entre

1. $\exists x_0 \in E \setminus \{0\}, u(x_0) = \lambda x_0$
2. $\ker(u - \lambda \text{id}) \neq \{0\}$
3. $u - \lambda \text{id} \notin \text{GL}(E)$

On dit alors que λ est une valeur propre de u , on appelle sous-espace propre de u pour la valeur propre λ

$$E_\lambda(u) = \{x \in E \mid u(x) = \lambda x\}$$

Démonstration

$$\begin{aligned} & \exists x_0 \in E \setminus \{0\}, u(x_0) = \lambda x_0 \\ & \Leftrightarrow \exists x_0 \in \ker(u - \lambda \text{id}) \setminus \{0\} \\ & \Leftrightarrow u - \lambda \text{id} \notin \text{GL}(E) \quad \left(\begin{smallmatrix} \text{dimension} \\ \text{finie} \end{smallmatrix} \right) \end{aligned}$$

Somme directe des sous-espaces propres

Démonstration du fait que les sous-espaces propres d'un endomorphisme sont en somme directe.

Soit $u \in \mathcal{L}(E)$, $\lambda_1, \dots, \lambda_p \in \mathbb{K}$ ses valeurs propres deux à deux distinctes.

Soit $(x_1, \dots, x_p) \in \prod_{k=1}^p E_{\lambda_k}(u)$ tels que $\sum_{k=1}^p x_k = 0$.

Par recurrence on montre que pour tout $P(X) \in \mathbb{K}[X]$.

$$0 = \sum_{k=1}^p P(\lambda_k) x_k$$

En particulier avec $P = L_i$ pour $i \in \llbracket 1, n \rrbracket$ on a

$$0 = \sum_{k=1}^p L_i(\lambda_k) x_k = x_i$$

On appelle spectre de u

$$\text{Sp}(u) = \{\lambda \in \mathbb{K} \mid \lambda \text{ valeur propre}\}$$

Qui est finit ($|\text{Sp}(u)| \leq n = \dim E$).

Polynôme caractéristique d'un endomorphisme

Définitions, propriétés élémentaires et démonstrations autour du polynôme caractéristique d'un endomorphisme.

Matrices

Soit $A \in M_n(\mathbb{K})$, on définit le polynôme caractéristique de A comme

$$\chi_A(X) = \det(XI_n - A)$$

Et on a

$$\chi_A(X) = \sum_{k=0}^n a_k X^k$$

$$a_n = 1 \quad (\chi_A \text{ unitaire})$$

$$a_{n-1} = -\text{tr}(A)$$

$$a_0 = (-1)^n \det(A)$$

Endomorphismes

Soit $u \in \mathcal{L}(E)$, e base de E , $A = \mathcal{M}_e(u)$. On définit

$$\chi_u(X) = \chi_A(X)$$

Ceci ne dépend pas de la base e choisie.

De plus

$$\text{Sp}(u) = Z_{\mathbb{K}}(\chi_u)$$

Démonstration

$$\chi_A(X) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \underbrace{\prod_{j=1}^n (X\delta_{\sigma(j)j} - A_{\sigma(j)j})}_{P_{\sigma}(X)}$$

Pour tout $\sigma \in \mathfrak{S}_n$, $P_{\sigma} \in \mathbb{K}_n[X]$

donc $\chi_A \in \mathbb{K}_n[X]$. De plus

$$\deg(P_{\sigma}) = |\{k \in \llbracket 1, n \rrbracket \mid \sigma(k) = k\}|$$

$$\deg(P_{\sigma}) = n \Leftrightarrow \sigma = \text{id}$$

Donc $\deg \chi_A = n$ et $\text{cd } \chi_A = 1$.

Si $\sigma \neq \text{id}$, $\deg(P_{\sigma}) \leq n-2$, donc a_{n-1} est le terme en X^{n-1} de P_{id} .

$$P_{\text{id}} = \prod_{j=1}^n (X - A_{jj})$$

$$a_{n-1} = -\sum_{j=1}^n A_{jj} = -\text{tr}(A)$$

$$a_0 = \chi_A(0) = \det(0 - A)$$

$$= (-1)^n \det(A)$$

Soient e, e' deux bases de E , $A = \mathcal{M}_e(u)$, $A' = \mathcal{M}_{e'}(u)$, $P = P_{e' \rightarrow e}$.

$$A' = PAP^{-1}$$

$$\begin{aligned} \chi_{A'}(X) &= \det(XI_n - A') \\ &= \det(XPI_nP^{-1} - PAP^{-1}) \\ &= \det(P) \det(XI_n - A) \det(P^{-1}) \\ &= \chi_A(X) \end{aligned}$$

Multiplicités d'une valeur propre

Définitions des multiplicités d'une valeur propre.

Soit $\lambda \in \mathbb{K}$ une valeur propre de l'endomorphisme u .

- On appelle multiplicité algébrique (m_λ), ou juste multiplicité de λ sa multiplicité en tant que racine de χ_u .
- On appelle multiplicité géométrique de λ la dimension de son espace propre.

On a toujours

$$\dim E_\lambda(u) \leq m_\lambda$$

Démonstration

Soit (e_1, \dots, e_d) base de E_λ complété en $e = (e_1, \dots, e_n)$ base de E .

$$\mathcal{M}_e(u) = \left(\begin{array}{c|c} \lambda I_d & B \\ \hline 0 & C \end{array} \right)$$

$$\chi_u = \chi_{\mathcal{M}_e(u)}$$

$$\begin{aligned} &= \left| \begin{array}{c|c} (X - \lambda)I_d & -B \\ \hline 0 & XI_{n-d} - C \end{array} \right| \\ &= (X - \lambda)^d \chi_C(X) \end{aligned}$$

Propriétés diverses du polynôme caractéristique

Cas particuliers de calculs du polynôme caractéristique, et lien avec les endomorphisme induit.

- Pour tout $T \in T_n(\mathbb{K})$

$$\chi_T = \prod_{k=1}^n T_{kk}$$

- Pour tout $M = \left(\begin{array}{c|c} A & B \\ \hline 0 & C \end{array} \right) \in M_n(\mathbb{K})$, $A \in M_r(\mathbb{K})$, $C \in M_{n-r}(\mathbb{K})$, $B \in M_{r,n-r}(\mathbb{K})$

$$\chi_M(X) = \chi_A(X)\chi_C(X)$$

- Soient $u \in \mathcal{L}(E)$, F sev stable par u , \tilde{u} l'endomorphisme induit par u sur F , on a toujours

$$\chi_{\tilde{u}} \mid \chi_u$$

Démonstration

- L'écrire.
- L'écrire.
- Soit $e = (e_1, \dots, e_n)$ base de F complétée en base de E .

$$\mathcal{M}_e(u) = \left(\begin{array}{c|c} A & B \\ \hline 0 & C \end{array} \right)$$

Avec $A = \mathcal{M}_{\tilde{e}}(\tilde{u})$.

Diagonalisabilité

Définition et premier critère de diagonalisabilité.

On dit que $u \in \mathcal{L}(E)$ est diagonalisable s'il existe une base e de E tel que $\mathcal{M}_e(u)$ est diagonale.

Une tel base est par définition formée de vecteurs propres de u .

De plus

$$\begin{aligned}
 & u \text{ diagonalisable} \\
 & \Leftrightarrow E = \bigoplus_{\lambda \in \text{Sp}(u)} E_\lambda(u) \\
 & \Leftrightarrow \sum_{\lambda \in \text{Sp}(u)} \dim E_\lambda(u) = \dim E
 \end{aligned}$$

En particulier

- Les homothéties sont diagonales dans toutes les bases
- Les projecteurs sont diagonalisables :

$$\underbrace{\ker(p - \text{id})}_{E_1(p)} \oplus \underbrace{\ker p}_{E_0(p)} = E$$

- Les symétries sont diagonalisables :

$$\underbrace{\ker(s - \text{id})}_{E_1(s)} \oplus \underbrace{\ker s + \text{id}}_{E_{-1}(s)} = E$$

Autre critère de diagonalisabilité

Énoncer du critère de diagonalisabilité sur χ_u et les multiplicités.

Soit $u \in \mathcal{L}(E)$

u diagonalisable

$$\Leftrightarrow \begin{cases} \chi_u \text{ scindé} \\ \forall \lambda \in \text{Sp}(u), \dim E_\lambda(u) = m_\lambda \end{cases}$$

Où m_λ est la multiplicité (algébrique) de λ .

Ainsi car $\dim E_\lambda(u) \geq 1$ pour tout $\lambda \in \text{Sp}(u)$,

$$\chi_u \text{ SARS} \Rightarrow u \text{ diagonalisable}$$

Démonstration

- Supposons u diagonalisable, notons e la base qui le diagonalise.

$$\mathcal{M}_e(u) = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix}$$

Donc χ_u est scindé

$$\begin{aligned} \chi_u(X) &= \prod_{k=1}^n (X - \alpha_k) \\ &= \prod_{k=1}^p (X - \lambda_k)^{m_{\lambda_k}} \end{aligned}$$

Ainsi

$$\begin{aligned} \deg \chi_u &= n = \sum_{k=1}^p m_{\lambda_k} \\ n &= \sum_{k=1}^p m_{\lambda_k} \geq \sum_{k=1}^p \dim E_{\lambda_k} = n \end{aligned}$$

- Supposons χ_u scindé et pour tout $\lambda \in \text{Sp}(u)$, $\dim E_\lambda(u) = m_\lambda$.

$$\chi_u = \underbrace{\prod_{\lambda \in \text{Sp}(u)} (X - \lambda)^{m_\lambda}}_{\deg = n}$$

$$n = \sum_{\lambda \in \text{Sp}(u)} m_\lambda = \sum_{\lambda \in \text{Sp}(u)} \dim E_\lambda(u)$$

Donc u est diagonalisable.

Trigonalisabilité

Définition et premiers critères de la trigonalisabilité.

Soit $u \in \mathcal{L}(E)$. On dit que u est trigonalisable s'il existe une base $e = (e_1, \dots, e_n)$ de E tel que $\mathcal{M}_e(u) \in T_n^+(\mathbb{K})$

Dans ce cas

- $u(e_1) = t_{11}e_1$, donc e_1 est un vecteur propre de u .
- Notons $F_k = \text{Vect}(e_1, \dots, e_k)$ le drapeau.

$$\forall k \in \llbracket 1, n \rrbracket, u(F_k) \subset F_k$$

- $\chi_u(X) = \prod_{k=1}^n (X - t_{kk})$ scindé.

La réciproque est aussi vraie :

χ_u scindé $\Rightarrow u$ trigonalisable.

Si $F \neq \{0\}$ est un sev stable par u et u trigonalisable, alors \tilde{u} (induit par u sur F) est trigonalisable (car $\chi_{\tilde{u}} \mid \chi_u$ scindé).

Si \mathbb{K} est algébriquement clos, toute matrice ou endomorphisme est trigonalisable.

Démonstration

Par récurrence sur $n = \dim E$.

Toute matrice de taille 1 est supérieure.

Supposons pour un $n \in \mathbb{N}$

$$\forall A \in M_n(\mathbb{K}),$$

$$\chi_A \text{ scindé} \Rightarrow A \text{ trigonalisable}$$

Soit $A \in M_{n+1}(\mathbb{K})$ tel que χ_A scindé.

χ_A a au moins une racine, donc A admet une valeur propre λ .

On dispose de $X_0 \in \mathbb{K}^{n+1}$ tel que

$$AX_0 = \lambda X_0$$

Ainsi on peut construire la base $e' = (X_0, \dots, X_n)$ de \mathbb{K}^{n+1} . Notons $P = P_{\text{can} \rightarrow e'}$.

$$A = P \left(\begin{array}{c|ccc} \lambda & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \tilde{A} & \\ 0 & & & \end{array} \right) P^{-1}$$

Avec $\tilde{A} \in M_n(\mathbb{K})$ et $\chi_A = \chi_{\tilde{A}}(X - \lambda)$ d'où $\chi_{\tilde{A}}$ scindé.

Par hypothèse de récurrence \tilde{A} est trigonalisable et on peut donc construire $P_0 \in \text{GL}_n(\mathbb{K})$ tel que

$$A = P \left(\begin{array}{ccc} \alpha_1 & & * \\ & \ddots & \\ & & \alpha_{n+1} \end{array} \right) P^{-1}$$

Caractérisation des endomorphismes nilpotents

Caractérisation des endomorphisme nilpotents.

Soit $u \in \mathcal{L}(E)$, il y a équivalence entre

1. u nilpotent
2. u trigonalisable en une matrice strictement supérieure.
3. u trigonalisable et $\text{Sp}(u) = \{0\}$
4. $\chi_u = X^n$

Démonstration

- (4 \Rightarrow 3) $\chi_u = X^n$ est scindé donc u est trigonalisable et $\text{Sp}(u) = Z(X^n) = \{0\}$.
- (3 \Leftrightarrow 2) Évident.
- (3 \Rightarrow 4) On dispose de e base de E tel que

$$\mathcal{M}_e(u) = \begin{pmatrix} 0 & & * \\ & \ddots & \\ & & 0 \end{pmatrix}$$

$$\text{Donc } \chi_u = X^n$$

- (2 \Rightarrow 1) On dispose de e base de E tel que $\mathcal{M}_e(u) \in T_n^{++}(\mathbb{K})$, notons $F_k = \text{Vect}(e_1, \dots, e_k)$.

$$u(F_k) \subseteq u(F_{k-1})$$

$$u^n(F_n = E) \subseteq F_0 = \{0\}$$

$$u^n = 0$$

- (1 \Rightarrow 2) u est nilpotent d'indice d .

$$\{0\} \subsetneq \ker u \subsetneq \dots \subsetneq \ker u^d = E$$

Construisons une base adaptée

$$\left(\underbrace{e_1, \dots, e_{i_1}}_{\text{base de } \ker u}, \dots, \underbrace{e_{i_2}, \dots, e_{i_d}}_{\text{base de } \ker u^2} \right)$$

Pour tout $x \in \ker u^k$:

$$u(x) \in \ker u^{k-1}$$

Ainsi pour tout $k \in \llbracket 1, n \rrbracket$ si $i_j + 1 \leq k \leq i_{j+1}$

$$e_k \in \ker u^j$$

$$u(e_k) \in \ker u^{j-1}$$

$$u(e_k) \in \text{Vect}(e_1, \dots, e_{i_{j-1}})$$

Premier lien entre polynôme minimal et polynôme caractéristique

Lien entre racines du polynôme minimal et celles du polynôme caractéristique.

Soit $u \in \mathcal{L}(E)$, $P \in \mathbb{K}[X]$
annulateur de u .

$$\text{Sp}(u) \subseteq Z_{\mathbb{K}}(P)$$

$$Z(\chi_u) = \text{Sp}(u) = Z_{\mathbb{K}}(\Pi_u)$$

Démonstration

- Soit $\lambda \in \text{Sp}(u)$ et $x \in E_{\lambda}(u) \setminus \{0\}$:

$$P(X) = \sum_{k=0}^d a_k X^k$$

$$\begin{aligned} P(u)(x) &= \sum_{k=0}^d u^k(x) = \sum_{k=0}^d \lambda^k x \\ &= P(\lambda)x = 0 \end{aligned}$$

Or $x \neq 0$, donc $P(\lambda) = 0$.

- Π_u annule u d'où $\text{Sp}(u) \subseteq Z_{\mathbb{K}}(\Pi_u)$
- Soit $\lambda \in \mathbb{K}$ racine de Π_u

$$\Pi_u = (X - \lambda)Q(X)$$

$$0 = (u - \lambda \text{id}) \circ Q(u)$$

Donc $\text{im } Q(u) \subseteq \ker(u - \lambda \text{id})$.

Mais $Q(u) \neq 0$ car Π_u minimal, donc

$$\dim(\text{im } Q(u)) \geq 1$$

$$\text{im } Q(u) \subseteq \ker(u - \lambda \text{id}) = E_{\lambda}(u)$$

$$\lambda \in \text{Sp}(u)$$

Théorème des noyaux

Énoncé et démonstrations du théorème des noyaux.

Soit $u \in \mathcal{L}(E)$ (\mathbb{K} -ev de dimension finie), $P \in \mathbb{K}[X]$.

Si $P = \prod_{k=1}^N P_k$ avec P_1, \dots, P_N deux à deux premiers entre eux, alors

$$\ker P(u) = \bigoplus_{k=1}^N \ker P_k(u)$$

Si de plus P annule u alors

$$E = \ker P(u) = \bigoplus_{k=1}^N \ker P_k(u)$$

$$\mathcal{M}_e(u) = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_N \end{pmatrix}$$

Où e est la base construite par concaténation de bases des $\ker P_k(u)$.

Démonstration

Par récurrence sur N .

Pour $P = P_1 P_2$ avec $P_1 \wedge P_2 = 1$:

$$P_1 V_1 + P_2 V_2 = 1$$

$$P_1(u) \circ V_1(u) + P_2(u) \circ V_2(u) = \text{id} \quad (*)$$

En évaluant on trouve

$$\ker P_1(u) \cap \ker P_2(u) = \{0\}$$

De plus

$$P_1(u) \circ P_2(u) = P_2(u) \circ P_1(u) = P(u)$$

$$\text{Donc } \begin{cases} \ker P_1(u) \subseteq \ker P(u) \\ \ker P_2(u) \subseteq \ker P(u) \end{cases}$$

$$\ker P_1(u) \oplus \ker P_2(u) \subseteq \ker P(u)$$

Soit $x \in \ker P(u)$, par (*) on a

$$x = \underbrace{V_1(u) \circ P_1(u)(x)}_{x_2} + \underbrace{V_2(u) \circ P_2(u)(x)}_{x_1}$$

$$\begin{aligned} P_1(u)(x_1) &= (P_1 V_2 P_2)(u)(x) \\ &= (V_1 P)(u)(x) \\ &= 0 \end{aligned}$$

$$\begin{aligned} P_2(u)(x_2) &= (P_2 V_1 P_1)(u)(x) \\ &= (V_2 P)(u)(x) \\ &= 0 \end{aligned}$$

$$x = \underbrace{x_1}_{\in \ker P_1(u)} + \underbrace{x_2}_{\in \ker P_2(u)}$$

D'où $\ker P(u) = \ker P_1(u) \oplus \ker P_2(u)$.

Supposons maintenant le résultat pour tout P_1, \dots, P_N respectant les conditions.

Soient $P = P_1 \cdots P_{N+1} \in \mathbb{K}[X]$ avec P_1, \dots, P_{N+1} deux à deux premiers entre eux.

Donc $Q = P_1 P_2 \cdots P_N$ et P_{N+1} sont premiers entre eux.

Ainsi

$$\begin{aligned} \ker P(u) &= \ker(P_{N+1} Q)(u) \\ &= \underbrace{\ker Q(u) \oplus \ker P_{N+1}(u)}_{\text{cas } N=2} \\ &= \underbrace{\bigoplus_{k=1}^N \ker P_k(u) \oplus \ker P_{N+1}(u)}_{\text{H.R.}} \\ &= \bigoplus_{k=1}^{N+1} \ker P_k(u) \end{aligned}$$

Démonstration annexe du théorème des noyaux

Démonstration secondaire du théorème des noyaux dans le cas d'un polynôme annulateur.

Soit $u \in \mathcal{L}(E)$.

On suppose $P = \prod_{k=1}^N P_k$ annulateur de u , P_1, \dots, P_N premiers entre eux deux à deux. On pose

$$Q_k = \prod_{\substack{i=1 \\ i \neq k}}^N P_i$$

Qui sont premiers dans leur ensemble.

$$\sum_{k=1}^N V_k Q_k = 1$$

$$\sum_{k=1}^N \underbrace{V_k(u) \circ Q_k(u)}_{\Pi_k} = \text{id} \quad (1)$$

On remarque que

$$P_k(u) \circ \Pi_k = (V_k P_k Q_k)(u) = (V_k P)(u) = 0$$

$$\text{Donc } \text{im } \Pi_k \subseteq \ker P_k(u)$$

Et pour $k \neq i$, $P \mid Q_i Q_k$ d'où

$$P \mid (V_k P_k)(V_i P_i)$$

$$\Pi_i \circ \Pi_k = 0$$

Donc par (1)

$$\sum_{i=1}^N \Pi_k \circ \Pi_i = \Pi_k \circ \Pi_k = \Pi_k$$

Donc les Π_k sont des projecteurs.

Soit $x \in \ker P_k(u)$, pour tout $i \neq k$, $\Pi_i(x) = 0$. Par (1)

$$x = \Pi_k(x)$$

$$x \in \text{im } \Pi_k$$

Ainsi

$$\ker P_k(u) = \text{im } \Pi_k$$

$$\ker P_i(u) \subseteq \ker \Pi_k$$

Les Π_k projettent sur $\ker P_k$.

Théorème des noyaux

Soient $(x_1, \dots, x_N) \in \prod_{k=1}^N \ker P_k(u)$ tels que $\sum_{k=1}^N x_k = 0$.

Pour tout $i \in \llbracket 1, N \rrbracket$

$$\Pi_i \left(\sum_{k=1}^N x_k \right) = x_i = 0$$

Donc les $\ker P_k(u) = \text{im } \Pi_k$ sont en somme directe.

Soit $x \in \ker P(u) = E$, par (1)

$$x = \sum_{k=1}^N \Pi_k(x) \in \sum_{k=1}^N \ker P_k(u)$$

D'où

$$E = \bigoplus_{k=1}^N \ker P_k(u)$$

Et de plus

$$\text{im } \Pi_k = \ker P_k(u)$$

$$\ker \Pi_k = \bigoplus_{\substack{i=1 \\ i \neq k}}^N \ker P_i(u)$$

$$\Pi_k \in \mathbb{K}[u]$$

Critère de Diagonalisabilité

Démonstration d'une CNS de diagonalisabilité.

Soit $u \in \mathcal{L}(E)$, il y a équivalence entre

1. u diagonalisable.
2. u annule un polynôme SARS.
3. Π_u est SARS

Démonstration

- (2 \Leftrightarrow 3)

$$\begin{aligned} \exists P \in \mathbb{K}[X], P \text{ SARS et } P(u) = 0 \\ \Leftrightarrow \exists P \in \mathbb{K}[X], P \text{ SARS et } \Pi_u \mid P \\ \Leftrightarrow \Pi_u \text{ SARS} \end{aligned}$$

- (3 \Rightarrow 1) Π_u SARS donc

$$\Pi_u = \prod_{\lambda \in \text{Sp}(u)}^N (X - \lambda)$$

Par le TDN

$$\begin{aligned} E &= \bigoplus_{\lambda \in \text{Sp}(u)} \ker(u - \lambda \text{id}) \\ &= \bigoplus_{\lambda \in \text{Sp}(u)} E_\lambda(u) \end{aligned}$$

Donc u diagonalisable.

- (1 \Rightarrow 3) u diagonalisable

$$\mathcal{M}_e(u) = \underbrace{\begin{pmatrix} \lambda_1 & & & \\ & \ddots & & \\ & & \lambda_1 & \\ & & & \ddots \\ & & & & \lambda_n \\ & & & & & \ddots \\ & & & & & & \lambda_n \end{pmatrix}}_M$$

$$P(X) = \prod_{k=1}^N (X - \lambda_k) \text{ SARS}$$

$$\begin{aligned} P(M) &= \begin{pmatrix} P(\lambda_1) & & & \\ & \ddots & & \\ & & P(\lambda_1) & \\ & & & \ddots \\ & & & & P(\lambda_n) \\ & & & & & \ddots \\ & & & & & & P(\lambda_n) \end{pmatrix} \\ &= 0 \end{aligned}$$

Donc $\Pi_u \mid P$ SARS.

Diagonalisabilité d'un endomorphisme induit

Diagonalisabilité d'un endomorphisme induit.

Soit $u \in \mathcal{L}(E)$, F un sev stable par u .

Notons \tilde{u} l'endomorphisme induit par u sur F .

- $\Pi_{\tilde{u}} \mid \Pi_u$
- Si u diagonalisable, alors \tilde{u} aussi.

Démonstration

- $\Pi_u(\tilde{u}) = 0$ donc $\Pi_{\tilde{u}} \mid \Pi_u$.
- Si u diagonalisable, Π_u est SARS, donc $\Pi_{\tilde{u}}$ aussi (car divise) donc \tilde{u} est diagonalisable.

Sous-espaces cycliques

Définition de sous-espace cyclique et base associé.

Pour un $u \in \mathcal{L}(E)$ et $x_0 \in E$ on appelle sous-espace cyclique engendré par x_0 (pour u)

$$F_{x_0} = \text{Vect}(u^k(x_0))_{k \in \mathbb{N}}$$

Cet espace admet comme base

$$(x_0, u(x_0), \dots, u^{d-1}(x_0))$$

Où $d = \deg \Pi_{u, x_0}$ le polynôme minimal ponctuel, l'unique polynôme unitaire minimal tel que

$$\text{Pour } \theta_{x_0} : \begin{cases} \mathbb{K}[X] & \rightarrow E \\ P & \mapsto P(u)(x_0) \end{cases}$$

$$\ker \theta_{x_0} = \Pi_{u, x_0} \mathbb{K}[X]$$

Démonstration

$\theta_{x_0} \in \mathcal{L}(E)$, donc $\ker \theta_{x_0}$ est un sev, donc un sous-groupe de $(\mathbb{K}[X], +)$.

Soit $P \in \ker \theta_{x_0}, Q \in \mathbb{K}[X]$

$$\begin{aligned} \theta_{x_0}(QP) &= Q(u)(P(u)(x_0)) \\ &= Q(u)(0) = 0 \end{aligned}$$

Donc $\ker \theta_{x_0}$ est un idéal de $\mathbb{K}[X]$, qui est principal d'où Π_{u, x_0} existe. Notons $d_{x_0} = \deg \Pi_{u, x_0}$.

Par existence et unicité de la division euclidienne on a

$$\mathbb{K}[X] = \mathbb{K}_{d_{x_0}-1}[X] \oplus \ker \theta_{x_0}$$

Donc $\theta_{x_0}|_{\mathbb{K}_{d_{x_0}-1}[X]}$ isomorphisme de $\mathbb{K}_{d_{x_0}-1}[X] \rightarrow \text{im } \theta_{x_0} = F_{x_0}$.

Donc F_{x_0} a pour base

$$\begin{aligned} &(\theta_{x_0}(1), \theta_{x_0}(X), \dots, \theta_{x_0}(X^{d_{x_0}-1})) \\ &= (x_0, u(x_0), \dots, u^{d-1}(x_0)) \end{aligned}$$

Endomorphismes cycliques

Définition, propriétés, démonstration autour des endomorphismes cycliques.

Soit $u \in \mathcal{L}(E)$, on dit que u est cyclique si l'une des conditions équivalentes suivantes est vérifiée

1. $\exists x_0 \in E, \text{Vect}(u^k(x_0))_{k \in \mathbb{N}} = E.$
2. $\exists x_0 \in E, (x_0, u(x_0), \dots, u^{n-1}(x_0))$ base de $E.$

Propriétés en vrac (sans démonstration)

- Si u cyclique, tout endomorphisme induit l'est aussi.
- Si u cyclique, u admet un nombre fini de sev stables.
- Si \mathbb{K} est infini et u admet un nombre fini de sev stables, alors u est cyclique.

Démonstration équivalence

- $(2 \Rightarrow 1)$ Évident.
- $(1 \Rightarrow 2)$ $F_{x_0} = \text{Vect}(u^k(x_0))_{k \in \mathbb{N}}$ est le sous-espace engendré par x_0 pour u , donc

$$(x_0, u(x_0), \dots, u^{d-1}(x_0))$$

Où $d = \deg \Pi_{u, x_0}$ en est une base.

Or $F_{x_0} = E$ par hypothèse, donc $\dim F_{x_0} = n$ et $d = n.$

Vision matricielle de la cyclicité

Lien entre endomorphisme cyclique et matrices de compagnon.

Soit $u \in \mathcal{L}(E)$, u est cyclique ss'il existe une base e de E et P unitaire de degré n tel que $\mathcal{M}_e(u) = C_P$.

Dans ce cas $\Pi_u = P$.

Démonstration

Soit $u \in \mathcal{L}(E)$ cyclique pour $x_0 \in E$. Notons $e = (x_0, u(x_0), \dots, u^{n-1}(x_0))$ la base associé.

On dispose alors de $a_0, \dots, a_{n-1} \in \mathbb{K}$ tels que

$$u^n(x_0) - \sum_{k=0}^{n-1} a_k u^k(x_0) = 0$$

$$P = X^n - \sum_{k=0}^{n-1} a_k X^k$$

$$P(u)(x_0) = 0$$

Et alors

$$\begin{aligned} \mathcal{M}_e(u) &= \begin{matrix} & x_0 & & & \\ & u(x_0) & & & \\ & \vdots & & & \\ & u^{n-1}(x_0) & & & \end{matrix} \begin{pmatrix} u(x_0) & \cdots & u^n(x_0) \\ 0 & & a_0 \\ 1 & \ddots & a_1 \\ & \ddots & 0 \\ & & 1 & a_{n-1} \end{pmatrix} \\ &= C_P \end{aligned}$$

Réciproquement :

Soit $u \in \mathcal{L}(E)$ et $e = (e_1, \dots, e_n)$ base de E tel que

$$\mathcal{M}_e(u) = \left(\begin{array}{ccc|c} 0 & & & a_0 \\ 1 & \ddots & & a_1 \\ & \ddots & 0 & \vdots \\ & & 1 & a_{n-1} \end{array} \right)$$

Alors pour $k \in \llbracket 1, n-1 \rrbracket$

$$u(e_k) = u(e_{k+1})$$

$$\text{Donc } e = (e_1, u(e_1), \dots, u^{n-1}(e_1))$$

Donc u est cyclique.

Ainsi :

$$P(u)(x_0) = u^n(x_0) - \underbrace{\sum_{k=0}^{n-1} a_k u^k(x_0)}_{u^n(x_0)} = 0$$

Donc pour tout $m \in \llbracket 0, n-1 \rrbracket$

$$P(u)(u^m(x_0)) = u^m(P(u)(x_0)) = 0$$

Ainsi $P(u)$ annule une base, d'où $\Pi_u \mid P$.

Or $\deg \Pi_{u, x_0} = n$ car u cyclique et $\Pi_{u, x_0} \mid \Pi_u$, donc

$$n \leq \deg \Pi_u \leq \deg P = n$$

Et comme Π_u et P sont unitaires

$$\Pi_u = P$$

Matrice compagnon

Définition de matrice compagnon.

Soit $P = X^d \sum_{k=0}^{d-1} a_k X^k \in \mathbb{K}[X]$ un polynôme unitaire. On appelle matrice compagnon de P la matrice

$$C_P = \left(\begin{array}{ccc|c} 0 & & & -a_0 \\ 1 & \ddots & & -a_1 \\ & \ddots & 0 & \vdots \\ & & 1 & -a_{d-1} \end{array} \right)$$

Ainsi (en développant selon la dernière colonne)

$$\chi_{C_P}(X) = P(X)$$

Exercice : vecteur dont le polynôme minimal ponctuel est le polynôme minimal

Soit $u \in \mathcal{L}(E)$, montrer qu'il existe $x \in E$ tel que $\Pi_{u,x} = \Pi_u$.

En déduire que u cyclique ssi $\deg \Pi_u = n$.

Soit $u \in \mathcal{L}(E)$.

On pose

$$\Pi_u = \prod_{k=1}^N P_k^{d_k}$$

Avec P_1, \dots, P_N irréductibles deux à deux distincts.

Démonstration \mathbb{K} quelconque

Par le TDN

$$E = \bigoplus_{k=1}^N \ker \underbrace{P_k^{d_k}(u)}_{F_k}$$

$$\ker P_k^{d_k-1}(u) \subseteq \ker P_k^{d_k}(u) = F_k$$

Supposons par l'absurde qu'on ai égalité pour un k .

$$E = \bigoplus_{j \neq k} \ker P_j^{d_j}(u) \oplus \ker P_k^{d_k-1}(u)$$

$$= \ker \underbrace{\left(P_k^{d_k-1} \prod_{j \neq k} P_j^{d_j} \right)}_{\substack{\text{ne peut annuler } u \\ \text{car } \Pi_u \text{ minimal}}}(u)$$

Donc $\ker P_k^{d_k-1}(u) \subsetneq \ker P_k^{d_k}(u)$.

Pour tout $k \in \llbracket 1, N \rrbracket$ on dispose de

$$x_k \in F_k \setminus \ker P_k^{d_k-1}(u)$$

$$\text{Donc } \begin{cases} P_k^{d_k}(u)(x_k) = 0 \\ P_k^{d_k-1}(x_k) \neq 0 \end{cases}$$

$$\text{Donc } \begin{cases} \Pi_{u,x_k} \mid P_k^{d_k} \\ \Pi_{u,x_k} \nmid P_k^{d_k-1} \end{cases}$$

$$\text{Donc } \underbrace{\Pi_{u,x_k}}_{\text{car } P_k \text{ irréductible}} = P_k^{d_k}$$

On pose $x = \sum_{k=1}^N x_k$, alors pour tout $P \in \Pi_{u,x} \mathbb{K}[X]$

$$P(u)(x) = 0$$

$$\Leftrightarrow \sum_{k=1}^N P(u)(x_k) = 0$$

$$\Leftrightarrow \underbrace{\forall k \in \llbracket 1, N \rrbracket, P(u)(x_k) = 0}_{\text{somme directe}}$$

$$\Leftrightarrow \forall k \in \llbracket 1, N \rrbracket, P_k^{d_k} = \Pi_{u,x_k} \mid P$$

$$\Leftrightarrow \prod_{k=1}^N P_k^{d_k} = \Pi_u \mid P$$

$$\Leftrightarrow P \in \Pi_u \mathbb{K}[X]$$

Donc $\Pi_u \mid \Pi_{u,x} \mid \Pi_u$.

Démonstration \mathbb{K} infini

Pour tout $x \in E$, $\Pi_{u,x} \mid \Pi_u$ donc

$$\Pi_{u,x} \in D = \{\text{Diviseurs unitaires de } \Pi_u\}$$

$$|D| = \prod_{k=1}^N (d_k + 1)$$

$$D' = \{\Pi_{u,y} \mid y \in E\} \subseteq D$$

Et $x \in \ker \Pi_{u,x}(u)$ d'où

$$E = \bigcup_{x \in E} \ker \Pi_{u,x}(u)$$

$$= \bigcup_{\substack{P \in D' \\ \text{union finie de sev}}} \ker P(u)$$

Donc on dispose de $Q = \Pi_{u,y} \in D'$ tel que (cf. exercice union de sev dans un corps infini)

$$E = \ker Q(u)$$

Par minimalité de Π_u , $\Pi_{u,y} = \Pi_u$.

CNS de cyclicité

On sait que si u cyclique, alors on dispose de e base de E tel que

$$\mathcal{M}_e(u) = C_{\Pi_u}$$

Avec $\Pi_u \in \mathbb{K}[X]$ unitaire de degré n .

Supposons maintenant que $\deg \Pi_u = n$.

On dispose de $x_0 \in E$ tel que $\Pi_{u,x_0} = \Pi_u$, d'où

$$\deg \Pi_{u,x_0} = n = \dim \underbrace{\text{Vect}(u^k(x_0))}_{F_{x_0}}_{k \in \mathbb{N}}$$

D'où $F_{x_0} = E$ et u cyclique.

Théorème de Cayley-Hamilton

Énoncé et démonstration du théorème de Cayley-Hamilton.

Soit $u \in \mathcal{L}(E)$, on a $\chi_u(u) = 0$ c'est à dire $\Pi_u \mid \chi_u$.

Démonstration

Soit $x_0 \in E \setminus \{0\}$, on veut montrer $\chi_u(u)(x_0) = 0$.

On pose $F_{x_0} = \text{Vect}(u^k(x_0))_{k \in \mathbb{N}}$ sev de E stable par u .

Soit \tilde{u} endomorphisme induit par u sur F_{x_0} , qui est donc cyclique.

Soit $d \in \mathbb{N}$ tel que

$$e_0 = (x_0, u(x_0), \dots, u^{d-1}(x_0))$$

Soit une base de F_{x_0} .

$$\mathcal{M}_{e_0}(\tilde{u}) = C_P = \left(\begin{array}{ccc|c} 0 & & & a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & a_{n-2} \\ & & 1 & a_{n-1} \end{array} \right)$$

Où

$$\tilde{u}^d(x_0) = u^d(x_0) = \sum_{k=0}^{d-1} a_k u^k(x_0)$$

$$P(X) = X^d - \sum_{k=0}^{d-1} a_k X^k$$

$$P(u)(x_0) = 0$$

Or $P = \chi_{C_P} = \chi_{\tilde{u}} \mid \chi_u$ donc

$$\chi_u(u)(x_0) = Q(u)(P(u)(x_0)) = 0$$

Exercice : propriétés des endomorphismes cycliques

1. Soit $u \in \mathcal{L}(E)$ diagonalisable, CNS pour u cyclique.
2. Soit $u \in \mathcal{L}(E)$ nilpotent, CNS pour u cyclique.
3. Soit $u \in \mathcal{L}(E)$ cyclique, montrer que pour tout $\lambda \in \text{Sp}(u)$, $\dim E_\lambda(u) = 1$.
4. Soit $u \in \mathcal{L}(E)$ cyclique, montrer que $\text{Com } u = \mathbb{K}[u]$.

1. Soit $u \in \mathcal{L}(E)$ diagonalisable.

$$\Pi_u = \prod_{k=1}^N (X - \lambda_k)$$

Où les $\lambda_1, \dots, \lambda_N$ sont deux à deux distincts (Π_u SARS).

u cyclique ssi $N = n = \dim E$.

- Si u cyclique, $\deg \Pi_u = n = N$.
- Si $\deg \Pi_u = n$

Soit $e = (e_1, \dots, e_n)$ base de vecteurs propres associés aux $\lambda_1, \dots, \lambda_n$.

Posons $x = \sum_{k=1}^n e_k$.

$$\mathcal{M}_e(x_0, u(x_0), \dots, u^{n-1}(x_0))$$

$$= \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \dots & \lambda_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \dots & \lambda_n^n \end{pmatrix}$$

Matrice de Vandermonde

inversible, d'où

$(x_0, u(x_0), \dots, u^{n-1}(x_0))$ base.

2. Soit $u \in \mathcal{L}(E)$ nilpotent d'indice q .

$$\Pi_u = X^q$$

- Si u cyclique, alors $\deg \Pi_u = q = n$.
- Si $q = n$, $u^{n-1} \neq 0$, donc on dispose de $x_0 \in E$ tel que $u^{n-1}(x_0) \neq 0$.

Et $(x_0, u(x_0), \dots, u^{n-1}(x_0))$ est libre et donc une base.

(En évaluant

$$u^i \left(\sum_{k=0}^{n-1} \lambda_k u^k(x_0) \right)).$$

3. Soit $u \in \mathcal{L}(E)$ cyclique, donc on dispose de e base de E tel que pour $\lambda \in \text{Sp}(u)$

$$\mathcal{M}_e(u - \lambda \text{id}) = \left(\begin{array}{cccc|c} -\lambda & & & & a_0 \\ 1 & -\lambda & & & a_2 \\ & 1 & \ddots & & \vdots \\ & & \ddots & -\lambda & a_{n-2} \\ & & & 1 & a_{n-1} - \lambda \end{array} \right)$$

Dont le quadrant inférieur gauche est une sous-matrice inversible de taille $n - 1$.

$$\text{rg } (u - \lambda \text{id}) \geq n - 1$$

$$1 \leq \dim E_\lambda(u) = \dim \ker(u - \lambda \text{id}) \leq 1$$

4. Soit $u \in \mathcal{L}(E)$ cyclique. On dispose de $x_0 \in E$ tel que

$$(x_0, u(x_0), \dots, u^{n-1}(x_0))$$

Est une base.

On a déjà $\mathbb{K}[u] \subseteq \text{Com}(u)$.

Soit $v \in \text{Com}(u)$. On dispose de

$\alpha_0, \dots, \alpha_{n-1} \in \mathbb{K}$ tels que

$$v(x_0) = \sum_{k=0}^{n-1} \alpha_k u^k(x_0)$$

Soit $m \in \llbracket 0, n - 1 \rrbracket$

$$v(u^m(x_0)) = u^m(v(x_0))$$

$$= u^m \left(\sum_{k=0}^{n-1} \alpha_k u^k(x_0) \right)$$

$$= \sum_{k=0}^{n-1} \alpha_k u^k(u^m(x_0))$$

Donc v et $\sum_{k=0}^{n-1} \alpha_k u^k$ coïncident sur une base, d'où $v \in \mathbb{K}[u]$.

Critère de trigonalisabilité sur le polynôme minimal

Soit $u \in \mathcal{L}(E)$, CNS de trigonalisabilité sur Π_u .

Soit $u \in \mathcal{L}(E)$, u est trigonalisable ssi Π_u scindé.

Démonstration

- Supposons u trigonalisable, donc χ_u est scindé or $\Pi_u \mid \chi_u$ donc Π_u est scindé.
- Supposons Π_u scindé.

$$\Pi_u = \prod_{k=1}^N (X - \lambda_k)^{d_k}$$

Avec $\lambda_1, \dots, \lambda_N \in \mathbb{K}$ deux à deux distincts.

Par le TDN

$$E = \bigoplus_{k=1}^N \underbrace{\ker(u - \lambda_k \text{id})^{d_k}}_{F_k}$$

Pour k fixé, F_k est stable par u et $u - \lambda_k \text{id}$, posons u_k induit par u sur F_k .

$u_k - \lambda_k \text{id}$ est nilpotent, donc on dispose de e_k base de F_k tel que

$$\mathcal{M}_{e_k}(u_k - \lambda_k \text{id}) = \begin{pmatrix} 0 & * \\ & \ddots \\ & & 0 \end{pmatrix}$$

$$\mathcal{M}_{e_k}(u_k) = A_k = \begin{pmatrix} \lambda_k & * \\ & \ddots \\ & & \lambda_k \end{pmatrix}$$

Notons e la base concaténant les bases e_1, \dots, e_N .

$$\mathcal{M}_e(u) = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_N \end{pmatrix}$$

Où les A_1, \dots, A_N sont triangulaires.

- (Autre méthode) Par récurrence sur n .

Cas $n = 1$ évident.

Supposons le résultat pour $n \in \mathbb{N}$. Soit $u \in \mathcal{L}(E)$ où $\dim E = n + 1$ et Π_u scindé.

Π_u admet au moins une racine λ , on dispose donc de $x \in E$ vecteur propre associé.

On forme la base $(\lambda, e_1, \dots, e_{n-1})$ de E .

$$\mathcal{M}_e(u) = A = \left(\begin{array}{c|ccc} \lambda & * & \dots & * \\ \hline 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{array} \right)$$

Or

$$\begin{aligned} 0 &= \mathcal{M}_e(\Pi_u(u)) = \Pi_u(A) \\ &= \left(\begin{array}{c|ccc} \Pi_u(\lambda) & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \Pi_u(A_1) & \\ 0 & & & \end{array} \right) \end{aligned}$$

D'où $\Pi_u(A_1) = 0$ donc $\Pi_{A_1} \mid \Pi_u$ et Π_{A_1} scindé, donc par hypothèse de récurrence A_1 est trigonalisable.

Exercice : polynôme caractéristique divisant une puissance du polynôme minimal

Soit $u \in \mathcal{L}(E)$, $n = \dim E$. Montrer que $\chi_u \mid \Pi_u^n$

Par récurrence forte sur n .

Cas $n = 1$ évident.

Supposons le résultat pour tout $m \in \llbracket 1, n-1 \rrbracket$.

Si u est cyclique, $\Pi_u = \chi_u$ d'où $\chi_u \mid \Pi_u^n$.

Sinon on prend $x_0 \in E \setminus \{0\}$, $k = \deg \Pi_{u, x_0} < n$ donc $(x_0, u(x_0), \dots, u^{k-1}(x_0))$ est libre, on la complète en une base e de E .

$$\mathcal{M}_e(u) = \left(\begin{array}{c|c} C_{\Pi_{u, x_0}} & * \\ \hline 0 & A \end{array} \right)$$

Donc

$$\chi_u = \underbrace{\chi_{C_{\Pi_{u, x_0}}} \chi_A}_{\Pi_{u, x_0}}$$

$$\chi_u \mid \Pi_u \chi_A$$

Or par hypothèse de récurrence $\chi_A \mid \Pi_A^{n-k}$ et

$$0 = \mathcal{M}_e(\Pi_u(u)) = \left(\begin{array}{c|c} \Pi_u(C_{\Pi_{u, x_0}}) & * \\ \hline 0 & \Pi_u(A) \end{array} \right)$$

$$\text{Donc } \Pi_A \mid \Pi_u$$

Ainsi

$$\chi_u \mid \Pi_u \Pi_A^{n-k} \mid \Pi_u^{n-k+1} \mid \Pi_u^n$$

Décomposition en sous espaces caractéristiques

Définition et démonstration de la décomposition en sous-espaces caractéristiques.

Soit $u \in \mathcal{L}(E)$ tel que χ_u scindé, l'espace E se décompose en somme directe de sev stables par u :

$$E = \bigoplus_{k=1}^N F_k$$

Où pour tout $k \in \llbracket 1, N \rrbracket$, u_k induit par u sur F_k vérifie

$$u_k = \lambda_k \text{id} + n_k$$

Où n_k est nilpotent et $\lambda_k \in \text{Sp}(u)$.

Dé plus $\dim F_k = m_k$ et $F_k = \ker(u - \lambda_k \text{id})^{m_k}$.

Cas diagonalisable

Si u est diagonalisable

$$\dim F_k = m_k = \dim E_{\lambda_k}(u)$$

$$E_{\lambda_k}(u) = \ker(u - \lambda_k \text{id})$$

$$\subseteq \ker(u - \lambda_k \text{id})^{m_k} = F_k$$

$$E_{\lambda_k}(u) = F_k$$

Démonstration

Soit $u \in \mathcal{L}(E)$ tel que χ_u scindé.

$$\chi_u = \prod_{k=1}^N (X - \lambda_k)^{m_k}$$

Où $\text{Sp}(u) = \{\lambda_1, \dots, \lambda_N\}$.

Par le TDN on a

$$E = \bigoplus_{k=1}^N \underbrace{\ker(u - \lambda_k \text{id})^{m_k}}_{F_k}$$

Les F_k sont stables par u , on peut donc poser u_k induit par u sur F_k .

On note $n_k = u_k - \lambda_k \text{id} \in \mathcal{L}(F_k)$ qui est nilpotent d'ordre inférieur à m_k .

Soit e_k base de F_k tel que

$$\mathcal{M}_{e_k}(n_k) = N_k \in T_{\dim F_k}^{++}(\mathbb{K}).$$

Ainsi $\mathcal{M}_{e_k}(u_k) = \lambda_k I_{\dim F_k} + N_k$.

En concaténant les bases $(e_k)_k$ en une base e de E on trouve

$$\mathcal{M}_e(u) = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_N \end{pmatrix}$$

$$\forall k \in \llbracket 1, N \rrbracket, A_k = \begin{pmatrix} \lambda_k & & * \\ & \ddots & \\ & & \lambda_k \end{pmatrix}$$

D'où

$$\prod_{k=1}^N (X - \lambda_k)^{m_k} = \chi_u = \prod_{k=1}^N (X - \lambda_k)^{\dim F_k}$$

$$m_k = \dim F_k$$

Sous-espaces caractéristiques et polynôme minimal

Lien entre la décomposition en sous-espaces caractéristiques et le polynôme minimal.

Soit $u \in \mathcal{L}(E)$ tel que χ_u scindé, à fortiori, Π_u est scindé.

$$\begin{aligned}\Pi_u &= \prod_{k=1}^N (X - \lambda_k)^{d_k} \\ \chi_u &= \prod_{k=1}^N (X - \lambda_k)^{m_k}\end{aligned}$$

On peut décomposer par le TDN sur Π_u et en les espaces caractéristiques

$$\begin{aligned}E &= \bigoplus_{k=1}^N \overbrace{\ker(u - \lambda_k \text{id})^{m_k}}^{F_k} \\ &= \bigoplus_{k=1}^N \underbrace{\ker(u - \lambda_k \text{id})^{d_k}}_{G_k}\end{aligned}$$

Or $d_k \leq m_k$ (car $\Pi_u \mid \chi_u$), d'où

$$\begin{aligned}G_k &= \ker(u - \lambda_k \text{id})^{d_k} \\ &\subseteq \ker(u - \lambda_k \text{id})^{m_k} = F_k\end{aligned}$$

Mais $\bigoplus_{k=1}^N G_k = \bigoplus_{k=1}^N F_k$ donc $G_k = F_k$.

Soit $q_k \leq d_k$ l'indice de nilpotence de $n_k = (u - \lambda_k \text{id})|_{F_k}$.

$$\begin{aligned}F_k &\subseteq \ker(u - \lambda_k \text{id})^{q_k} \\ &\subseteq \ker(u - \lambda_k \text{id})^{d_k} = F_k\end{aligned}$$

Posons $Q = \prod_{k=1}^N (X - \lambda_k)^{q_k}$

$$\begin{aligned}E &= \bigoplus_{k=1}^N \ker(u - \lambda_k)^{d_k} \\ &= \bigoplus_{k=1}^N \ker(u - \lambda_k)^{q_k}\end{aligned}$$

Donc par le TDN $\ker Q(u) = E$, $\Pi_u \mid Q$ donc $d_k \leq q_k \leq d_k$.

Exercice : valuation X-adique du polynôme minimal.

Soit $u \in \mathcal{L}(E)$, $\Pi_u = X^d Q$ avec $X \nmid Q$.

1. Montrer que

$$d = \min\{k \in \mathbb{N}^* \mid \ker u^k = \ker u^{k+1}\}$$

2. Montrer que

$$E = \ker u^d \oplus \operatorname{im} u^d$$

Soit $u \in \mathcal{L}(E)$, $\Pi_u = X^d Q$ avec $X \nmid Q$.

1. Notons

$$q = \min\{k \in \mathbb{N}^* \mid \ker u^k = \ker u^{k+1}\}$$

Soit \tilde{u} l'induit par u sur $\ker u^q$.

$$\begin{cases} \tilde{u}^q = 0 \\ \tilde{u}^{q-1} \neq 0 \end{cases} \quad \text{Donc} \quad \Pi_{\tilde{u}} = X^q$$

$$\begin{aligned} X^q \mid \Pi_{\tilde{u}} \mid \Pi_u = X^d Q \\ q \leq d \end{aligned}$$

Donc $\ker u^q = \ker u^d$

$$\ker u^d \circ Q(u) = E$$

$$\operatorname{im} Q(u) \subseteq \ker u^d = \ker u^q$$

$$\ker u^q \circ Q(u) = E$$

$$\begin{aligned} X^d Q \mid X^q Q \\ q \geq d \end{aligned}$$

2. On a (TDN)

$$E = \ker u^d \oplus \ker Q(u)$$

Soit $y \in \operatorname{im} u^d$, on dispose donc de $x \in E$ tel que $y = u^d(x)$.

$$y = u^d(x)$$

$$Q(u)(y) = (X^d Q)(u)(x) = 0$$

$$\operatorname{im} u^d \subseteq \ker Q(u)$$

Or par le théorème du rang

$$\begin{aligned} \dim \operatorname{im} u^d &= \dim E - \dim \ker u^d \\ &= \dim \ker Q(u) \end{aligned}$$

D'où $\operatorname{im} u^d = \ker Q(u)$.

Décomposition de Dunford

Définition et démonstration de la décomposition de Dunford.

Soit $u \in \mathcal{L}(E)$ tel que χ_u scindé.

On dispose de $d, n \in \mathcal{L}(E)$ tel que

- $u = d + n$
- d diagonalisable
- n nilpotent
- $d \circ n = n \circ d$

De plus cette décomposition est unique.

Elle peut entre autre servir pour les puissances de matrices :

$$= P \begin{pmatrix} (\lambda_1 I_{m_1} + N_1)^k & & \\ & \ddots & \\ & & (\lambda_n I_{m_n} + N_n)^k \end{pmatrix}$$

Démonstration

On reprend la décomposition en sous-espaces caractéristiques

$$\Pi_u = \prod_{k=1}^N (X - \lambda_k)^{d_k}$$

$$\chi_u = \prod_{k=1}^N (X - \lambda_k)^{m_k}$$

$$E = \bigoplus_{k=1}^N \underbrace{\ker (u - \lambda_k \text{id})^{m_k}}_{F_k}$$

$$\forall k \in \llbracket 1, n \rrbracket, F_k = \ker (u - \lambda_k \text{id})^{d_k}$$

On note u_k l'endomorphisme induit par u sur F_k .

$$F_k = \ker (u - \lambda_k \text{id}_E)^{m_k}$$

$$\text{D'où } (u_k - \lambda_k \text{id}_{F_k})^{m_k} = 0_{\mathcal{L}(F_k)}$$

Posons

$$n_k = u_k - \lambda_k \text{id}_{F_k}$$

$$\text{Donc } u_k = \lambda_k \text{id}_{F_k} + n_k$$

Où n_k est nilpotent d'ordre d_k (cf démonstration sous-espaces caractéristiques).

On pose alors $d, n \in \mathcal{L}(E)$ tel que

$$\forall k \in \llbracket 1, n \rrbracket,$$

$$d|_{F_k} = \lambda_k \text{id}_{F_k}$$

$$n|_{F_k} = n_k$$

Donc d diagonalisable et n nilpotent d'ordre $\max_{k \in \llbracket 1, n \rrbracket} (d_k)$.

Matriciellement

$$\mathcal{M}_e(d) = \begin{pmatrix} \lambda_1 I_{m_k} & & \\ & \ddots & \\ & & \lambda_N I_{m_k} \end{pmatrix} \in D_n(\mathbb{K})$$

$$\mathcal{M}_e(n) = \begin{pmatrix} N_1 & & \\ & \ddots & \\ & & N_N \end{pmatrix} \in T_n^{++}(\mathbb{K})$$

$$DN = \begin{pmatrix} \lambda_1 N_1 & & \\ & \ddots & \\ & & \lambda_N N_N \end{pmatrix} = ND$$

Unicité

On prend p_1, \dots, p_N les projecteurs associés à la décomposition (cf. démonstration du TDN)

$$E = \bigoplus_{k=1}^N F_k = \bigoplus_{k=1}^N \ker (u - \lambda_k \text{id})^{d_k}$$

On avait montrer que $p_1, \dots, p_N \in \mathbb{K}[u]$.

On a

$$d = \sum_{k=1}^N \lambda_k p_k \in \mathbb{K}[u]$$

$$n = u - d \in \mathbb{K}[u]$$

Soient $d', n' \in \mathcal{L}(E)$ respectent les conditions.

Comme $u = d' + n'$, d' commute avec u et n' aussi, donc d' commute avec $d \in \mathbb{K}[u]$ et n' avec $n \in \mathbb{K}[u]$.

Ainsi d' et d sont codiagonalisables, d'où $d' - d$ est diagonalisable.

Et $n - n'$ est nilpotent (binôme de Newton).

Or $d' + n' = d + n$ d'où

$$\underbrace{d' - d}_{\text{diagonalisable}} = \underbrace{n - n'}_{\text{nilpotent}}$$

D'où $d' - d = 0$ et $n' - n = 0$.

Codiagonalisabilité

Définition et critère de codiagonalisabilité.

Soient $(u_i)_i \in \mathcal{L}(E)^I$ une famille d'endomorphismes.

On dit que les $(u_i)_i$ sont codiagonalisables s'il existe une base e de E tels que pour tout $i \in I$, $\mathcal{M}_e(u_i) \in D_n(\mathbb{K})$.

Démonstration : deux endomorphismes

Soient $u, v \in \mathcal{L}(E)$ diagonalisables tels que $u \circ v = v \circ u$.

$$E = \bigoplus_{k=1}^N E_{\lambda_k}(u) \quad \text{où} \quad \text{Sp}(u) = \{\lambda_1, \dots, \lambda_N\}$$

Comme $u \circ v = v \circ u$, les $E_{\lambda_k}(u)$ sont stables par v .

Soit v_k l'induit de v sur $E_{\lambda_k}(u)$, qui est diagonalisable car v l'est.

Pour chaque $k \in \llbracket 1, N \rrbracket$ on dispose de e_k base de vecteurs propres de v_k (donc de v et u).

En concaténant on obtient une base qui convient.

Démonstration famille quelconque

Par récurrence sur $n = \dim E$.

Cas $n = 1$ évident.

Supposons la propriété pour tout \mathbb{K} -ev de dimension inférieur à n .

Soit $(u_i)_i \in \mathcal{L}(E)^I$ diagonalisables commutant avec $\dim E = n + 1$.

Si tout les u_i sont des homothéties n'importe quelle base convient.

Sinon on dispose de $j \in I$ tel que u_j n'est pas une homothétie.

$$E = \bigoplus_{k=1}^N E_{\lambda_k}(u_j) \quad \text{où} \quad \text{Sp}(u_j) = \{\lambda_1, \dots, \lambda_N\}$$

Pour tout $i \in I$, les $E_{\lambda_k}(u_j)$ sont stables par u_i car $u_i \circ u_j = u_j \circ u_i$.

Notons $u_{i,k}$ l'induit de u_i sur $E_{\lambda_k}(u_j)$ qui est de dimension inférieur à n car u_j n'est pas une homothétie.

Les $(u_{i,k})_i$ sont donc diagonalisables et commutent entre eux, on peut appliquer l'hypothèse de récurrence.

On dispose donc de e_k base de $E_{\lambda_k}(u_j)$ formée de vecteurs propres commun aux $(u_i)_i$. Il suffit alors de les concaténer.

Commutant d'un endomorphisme diagonalisable

Propriétés sur le commutant d'un endomorphisme diagonalisable.

Soit $u \in \mathcal{L}(E)$ diagonalisable.

- Pour tout $v \in \mathcal{L}(E)$, $v \in \text{Com}(u)$ ssi les espaces propres de u sont stables par v .
- $\dim \text{Com}(u) = \sum_{\lambda \in \text{Sp}(u)} (\dim E_{\lambda}(u))^2$

Démonstration

- L'implication directe est évidente.

Supposons $v \in \mathcal{L}(E)$ qui stabilise les espaces propres de u .

Pour $\lambda \in \text{Sp}(u)$ soit $x \in E_{\lambda}(u)$, d'où $v(x) \in E_{\lambda}(u)$.

$$\begin{aligned} v(u(x)) &= v(\lambda x) = \lambda v(x) \\ u(v(x)) &= \lambda v(x) \end{aligned}$$

Or u diagonalisable, donc on dispose d'une base de vecteurs propres de u .

Ainsi $u \circ v$ et $v \circ u$ coïncident sur une base d'où l'égalité.

- On note $\text{Sp}(u) = \{\lambda_1, \dots, \lambda_N\}$.

On considère

$$\theta : \begin{cases} \text{Com}(u) & \rightarrow & \prod_{k=1}^N \mathcal{L}(E_{\lambda_k}(u)) \\ v & \mapsto & (v|_{E_{\lambda_1}(u)}, \dots, v|_{E_{\lambda_N}(u)}) \end{cases}$$

Qui est linéaire.

Soit $v \in \ker \theta$: pour tout $k \in \llbracket 1, N \rrbracket$

$$v(E_{\lambda_k}(u)) = 0$$

$$\text{Or } E = \bigoplus_{k=1}^N E_{\lambda_k}(u)$$

$$\text{Donc } v = 0$$

Soit $(v_1, \dots, v_k) \in \prod_{k=1}^N \mathcal{L}(E_{\lambda_k}(u))$.

Pour $k \in \llbracket 1, N \rrbracket$, on note e_k base de $E_{\lambda_k}(u)$.

On définit $v \in \mathcal{L}(E)$ qui coïncide avec v_k sur tout les vecteurs de e_k .

Ainsi $\theta(v) = (v_1, \dots, v_k)$, et θ isomorphisme.

$$\begin{aligned} \dim \text{Com}(u) &= \sum_{k=1}^N \dim \mathcal{L}(E_{\lambda_k}(u)) \\ &= \sum_{k=1}^N (\dim E_{\lambda_k}(u))^2 \end{aligned}$$

Exercice : le bicommutant

Soit $u \in \mathcal{L}(E)$ diagonalisable. On définit le bicommutant de u

$$B(u) = \left\{ w \in \mathcal{L}(E) \mid \begin{array}{l} \forall v \in \text{Com}(u) \\ v \circ w = w \circ v \end{array} \right\}$$

Montrer que $B(u) = \mathbb{K}[u]$.

Comme $u \in \text{Com}(u)$ on remarque

$$\mathbb{K}[u] \subseteq B(u) \subseteq \text{Com}(u)$$

On construit e concatenation de bases des $E_{\lambda_k}(u)$ pour $k \in \llbracket 1, N \rrbracket$ et $\text{Sp}(u) = \{\lambda_1, \dots, \lambda_N\}$.

Soit $w \in B(u) \subseteq \text{Com}(u)$ donc les $(E_{\lambda_k})_k$ sont stables par w .

$$M = \mathcal{M}_e(w) = \begin{pmatrix} M_1 & & \\ & \ddots & \\ & & M_N \end{pmatrix}$$

Pour tout $v \in \text{Com}(u)$, $w \circ v = v \circ w$.

$$A = \mathcal{M}_e(v) = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_N \end{pmatrix}$$

Or $AM = MA$ donc

$$\forall k \in \llbracket 1, N \rrbracket, A_k M_k = M_k A_k$$

Ainsi M_k est une matrice qui commute avec toutes les autres.

On montre facilement grâce à E_{ij} que $M_k = \alpha_k I_{m_k}$.

Par interpolation de Lagrange on dispose de $P \in \mathbb{K}_{N+1}(X)$ tel que $P(\lambda_k) = \alpha_k$. Or

$$\mathcal{M}_e(u) = \begin{pmatrix} \lambda_1 I_{m_1} & & \\ & \ddots & \\ & & \lambda_N I_{m_N} \end{pmatrix}$$

$$\begin{aligned} \mathcal{M}_e(P(u)) &= \begin{pmatrix} P(\lambda_1) I_{m_1} & & \\ & \ddots & \\ & & P(\lambda_N) I_{m_N} \end{pmatrix} \\ &= \begin{pmatrix} \alpha_1 I_{m_1} & & \\ & \ddots & \\ & & \alpha_N I_{m_N} \end{pmatrix} \\ &= \mathcal{M}_e(w) \end{aligned}$$

D'où $w \in \mathbb{K}[u]$.

Projecteurs spectraux d'un endomorphisme diagonalisable

Définition et propriétés des projecteurs spectraux d'un endomorphisme diagonalisable.

Soit $u \in \mathcal{L}(E)$ diagonalisable.

$$\chi_u = \prod_{k=1}^N (X - \lambda_k)^{m_k}$$

$$\Pi_u = \prod_{k=1}^N (X - \lambda_k)$$

Soient p_1, \dots, p_N les projecteurs associés à la décomposition

$$E = \bigoplus_{k=1}^N \underbrace{\ker(u - \lambda_k \text{id})}_{E_{\lambda_k}(u)}$$

On a alors pour tout $i, j \in \llbracket 1, N \rrbracket$

$$p_i|_{E_{\lambda_j}(u)} = \delta_{ij} \lambda_i \text{id}$$

Dans la base e diagonalisant u et pour tout $P \in \mathbb{K}[X]$ on a

$$\mathcal{M}_e(P(u)) = \begin{pmatrix} P(\lambda_1)I_{m_1} & & \\ & \ddots & \\ & & P(\lambda_N)I_{m_N} \end{pmatrix}$$

$$\mathcal{M}_e(p_k) = \begin{pmatrix} 0 & & & \\ & \ddots & & \\ & & I_{m_k} & \\ & & & \ddots \\ & & & & 0 \end{pmatrix}$$

Donc $p_k = L_k(u) \in \mathbb{K}_{N-1}[u]$ avec L_k polynôme de Lagrange associés aux $(\lambda_i)_i$.

Ainsi pour tout $q \in \mathbb{N}$

$$u = \sum_{k=1}^N \lambda_k p_k$$

$$u^q = \sum_{k=1}^N \lambda_k^q p_k \in \mathbb{K}_{N-1}[u]$$

Sous-espaces stables d'un endomorphisme diagonalisable

Propriétés sur les sous-espaces stables d'un endomorphisme diagonalisable.

Soit $u \in \mathcal{L}(E)$ diagonalisable,
 $\text{Sp}(u) = \{\lambda_1, \dots, \lambda_N\}$.

1. Si G sev stable par u alors

$$G = \bigoplus_{k=1}^N G \cap E_{\lambda_k}(u)$$

2. Réciproquement si G_1, \dots, G_N sont des sevs de $E_{\lambda_1}(u), \dots, E_{\lambda_N}(u)$ respectivement alors

$$G = \bigoplus_{k=1}^N G_k$$

Est un sev stable par u .

Démonstration

1. Soit \tilde{u} induit par u sur G donc diagonalisable.

$$\begin{aligned} G &= \bigoplus_{\lambda \in \text{Sp}(\tilde{u})} E_{\lambda}(\tilde{u}) \\ &= \bigoplus_{k=1}^N \ker(\tilde{u} - \lambda_k \text{id}_G) \\ &= \bigoplus_{k=1}^N G \cap \underbrace{\ker(u - \lambda_k \text{id})}_{E_{\lambda_k}(u)} \end{aligned}$$

2. L'écrire.

Existence d'une droite ou d'un plan stable dans un espace vectoriel réel

Démonstration de l'existence d'une droite ou d'un plan stable dans un espace vectoriel réel.

Soit E un \mathbb{R} -ev et $u \in \mathcal{L}(E)$, u admet une droite ou un plan stable.

$$\Pi_u = \prod_{k=1}^N P_k^{m_k}$$

Avec P_1, \dots, P_N irréductibles deux à deux distincts.

- Si l'un des P_k est de degré 1.

$$P_k = X - \lambda$$

Et λ est racine de Π_u et est donc une valeur propre de u d'où l'existence d'une droite stable.

- Si l'un des P_k est de degré 2.

$$P_k = X^2 - aX - b$$

Supposons par l'absurde que $\ker P_k(u) = \{0\}$.

$$\Pi_u(u) = P_k(u) \circ Q(u) = 0$$

D'où $Q(u) = 0$ qui est absurde car Π_u est minimal.

On dispose donc de $x \in \ker P_k(u) \setminus \{0\}$.

$$u^2(x) = au(x) + bx$$

D'où $F = \text{Vect}(x, u(x))$ stable par u .

Si $u(x) = \alpha x$, $\alpha \in \mathbb{R}$.

$$\alpha^2 x = (a\alpha + b)x$$

$$\alpha \mid X^2 - aX - b$$

Absurde donc F est un plan.

Endomorphismes simples

Soit $u \in \mathcal{L}(E)$, il y a équivalence entre

1. Les seuls sev stables de u sont E et $\{0\}$.
2. χ_u irréductible.
3. u est dit simple.

1. $(2 \Rightarrow 1)$ Par contraposé

Soit F sev stable par u de dimension dans $\llbracket 1, n-1 \rrbracket$, et \tilde{u} l'endomorphisme induit.

$$\chi_{\tilde{u}} \mid \chi_u$$

Avec $\chi_{\tilde{u}} = \dim F \neq \deg \chi_u$ d'où χ_u non irréductible.

2. $(1 \Rightarrow 2)$ Par contraposé : Soit $x \in E \setminus \{0\}$ on note

$$F_x = \text{Vect}(u^k(x_0))_{k \in \mathbb{N}}$$

Qui est stable par u .

Si $\deg \Pi_{u,x} = \dim F_x \leq n-1$, alors u possède un sev stable non trivial.

Sinon $\Pi_{u,x} \mid \Pi_u \mid \chi_u$ tous unitaires de degré n , donc égaux. Ainsi

$$\Pi_{u,x} = \chi_u = PQ$$

$$y = Q(u)(x)$$

$$\Pi_{u,y} = P$$

D'où F_y stable non trivial.

Endomorphismes semi-simples

Définition et propriétés des endomorphismes semi-simples.

Soit $u \in \mathcal{L}(E)$, il y a équivalence entre

1. Tout sev stable par u admet un supplémentaire stable.
2. Π_u est sans carrés

$$\Pi_u = \prod_{k=1}^N P_k$$

Avec P_1, \dots, P_N irréductibles deux à deux distincts.

3. u est semi-simple.

Démonstration

1. $(1 \Rightarrow 2)$ On pose

$$\Pi_u = \prod_{k=1}^N P_k^{d_k}$$

Pour $i \in \llbracket 1, N \rrbracket$, $F = \ker P_k(u)$ admet un supplémentaire stable G .

Soient u_F, u_G induit par u sur F et G .

$$\Pi_{u_F} = P_i$$

Car annule et irréductible.

De plus

$$\begin{aligned} P(u) &= 0 \\ \Leftrightarrow \begin{cases} \forall x \in F, P(u)(x) = 0 \\ \forall x \in G, P(u)(x) = 0 \end{cases} \\ \Leftrightarrow \Pi_{u_F} \mid P \text{ et } \Pi_{u_G} \mid P \\ \Leftrightarrow \Pi_{u_F} \vee \Pi_{u_G} \mid P \\ \text{Donc } \Pi_u &= \Pi_{u_F} \vee \Pi_{u_G} \end{aligned}$$

Ainsi

$$\begin{aligned} \Pi_{u_G} \mid \prod_{k=1}^N P_k^{d_k} \\ \Pi_u &= \Pi_{u_G} \vee P_i \end{aligned}$$

Mais

$$\begin{aligned} G \cap F &= \{0\} \\ G \cap \ker P_1(u) &= \{0\} \\ 0 \neq P_i(u_G) &\in \text{GL}(E) \\ P_i &\nmid \Pi_{u_G} \end{aligned}$$

Ainsi comme $\Pi_u = P_i \vee \Pi_{u_G}$

$$d_i = 1$$

2. $(2 \Rightarrow 1)$ Cas Π_u irréductible.

On suppose Π_u irréductible de degré d .

Donc pour tout $x \in E \setminus \{0\}$

$$\begin{aligned} \Pi_{u,x} \mid \Pi_u \text{ d'où } \Pi_u &= \Pi_{u,x} \\ \text{et } \dim F_x &= d \end{aligned}$$

Soit F sev stable par u , si $F = E$, $G = 0$ convient.

On dispose alors de $x_1 \in E \setminus F$.

Comme F et F_{x_1} sont stables par u , $F \cap F_{x_1}$ l'est.

Supposons par l'absurde qu'il existe $x \in F \cap F_{x_1} \setminus \{0\}$.

$$\underbrace{F_x}_{\dim d} \subseteq \underbrace{\overbrace{F_{x_1} \cap F}^{\dim d}}_{\dim \leq d}$$

$$F_{x_1} \subseteq F$$

$$x_1 \in F$$

Qui est absurde : $F \oplus F_{x_1} \subseteq E$.

Supposons construits x_1, \dots, x_k tels que

$$\underbrace{F \oplus \left(\bigoplus_{i=1}^k F_{x_i} \right)}_{F_k \text{ stable}} \subseteq E$$

Si $F_k = E$ on a fini.

Sinon on choisit $x_{k+1} \in E \setminus F_k$ et on répète.

$$F_{x_{k+1}} \cap F_k = \{0\}$$

$$F_k \oplus F_{x_{k+1}} \subseteq E$$

$$F \oplus \left(\bigoplus_{i=1}^{k+1} F_{x_i} \right) \subseteq E$$

Qui se termine en au plus $\lfloor \frac{n}{d} \rfloor$ étapes.

3. $(2 \Rightarrow 1)$ Cas général.

$$\Pi_u = \prod_{k=1}^N P_k$$

Par le TDN

$$E = \bigoplus_{k=1}^N \ker P_k(u)$$

Soit F sev stable par u , \tilde{u} induit par u sur F . Par TDN

$$\begin{aligned} F &= \bigoplus_{k=1}^N \ker P_k(\tilde{u}) \\ &= \bigoplus_{k=1}^N \underbrace{(\ker P_k(\tilde{u})) \cap F}_{F_k} \end{aligned}$$

F_k sev de $E_k = \ker P_k(u)$ stable par u_k induit par u sur E_k .

De plus $\Pi_{u_k} = P_k$ (annule et irréductible).

Donc par le premier cas on trouve G_k sev de E_k stable par u tel que

$$E_k = G_k \oplus F_k$$

Enfin

$$E = \bigoplus_{k=1}^N E_k$$

$$= \underbrace{\left(\bigoplus_{k=1}^N (F_k) \right)}_{F \text{ stable par } u} \oplus \underbrace{\left(\bigoplus_{k=1}^N G_k \right)}_{G \text{ stable par } u}$$

Exercice : critère de diagonalisabilité sur l'existence de supplémentaires stables

Soit $u \in \mathcal{L}(E)$ tel que χ_u scindé. Montrer que u est diagonalisable ssi tout sev stable par u admet un supplémentaire stable.

- Supposons u diagonalisable, soit F un sev stable par u .

On dispose donc de $f = (f_1, \dots, f_d)$ base de F et $e = (e_1, \dots, e_n)$ base de vecteurs propres de E .

On peut donc compléter la base f par des vecteurs de e :

$(f_1, \dots, f_d, e_{i_1}, \dots, e_{i_{n-d}})$ base de E

Ainsi $G = \text{Vect}(e_{i_1}, \dots, e_{i_{n-d}})$ est un supplémentaire de F stable par u .

- Supposons que tout sev stable par u admettent un supplémentaire stable.

$$F = \bigoplus_{\lambda \in \text{Sp}(u)} E_\lambda(u)$$

Est un sev stable, et admet donc G comme supplémentaire stable. Notons \tilde{u} l'induit sur G de u .

$$\Pi_{\tilde{u}} \mid \Pi_u \text{ scindé}$$

Donc \tilde{u} admet une valeur propre λ et un vecteur propre $x \in F \cap G = \{0\}$ qui est absurde. Donc $G = \{0\}$ et $F = E : u$ est diagonalisable.

Endomorphismes de produit de matrices

Propriétés sur les endomorphismes de la forme $M \mapsto AM$ et $M \mapsto MA$ de $\mathcal{L}(M_n(\mathbb{K}))$.

Soit $A \in M_n(\mathbb{K})$. Posons

$$L_A : \begin{cases} M_n(\mathbb{K}) \rightarrow M_n(\mathbb{K}) \\ M \mapsto AM \text{ ou } MA \end{cases} \in \mathcal{L}(M_n(\mathbb{K}))$$

Pour tout $P \in \mathbb{K}[X]$ et $M \in M_n(\mathbb{K})$

$$P(L_A)(M) = \begin{cases} P(A)M \\ MP(A) \end{cases} = L_{P(A)}(M)$$

De plus $L_B = 0 \Rightarrow L_B(I_n) = B = 0$
d'où

$$P(L_A) = 0 \Leftrightarrow P(A) = 0$$

C'est à dire $\Pi_{L_A} = \Pi_A$

On en déduit

- L_A est nilpotent ssi A l'est et est de même ordre.
- L_A est diagonalisable ssi A l'est.
- $\text{Sp}(A) = \text{Sp}(L_A)$

De plus pour $\lambda \in \text{Sp}(A)$

$$\dim E_\lambda(L_A) = n \dim E_\lambda(A)$$

Démonstration

- Pour $L_A(M) = AM$

Soit $M = (C_1, \dots, C_n) \in M_n(\mathbb{K})$

$$\begin{aligned} M \in E_\lambda(L_A) &\Leftrightarrow AM = \lambda M \\ &\Leftrightarrow \forall j \in \llbracket 1, n \rrbracket, AC_j = \lambda C_j \\ &\Leftrightarrow \{C_1, \dots, C_n\} \subseteq E_\lambda(A) \end{aligned}$$

Ainsi $E_\lambda(L_A) \simeq E_\lambda(A)^n$.

- Pour $L_A(M) = MA$

$$\text{Soit } M = \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix} \in M_n(\mathbb{K})$$

$$\begin{aligned} M \in E_\lambda(L_A) &\Leftrightarrow MA = \lambda M \\ &\Leftrightarrow \forall i \in \llbracket 1, n \rrbracket, AL_i = \lambda L_i \\ &\Leftrightarrow \{L_1, \dots, L_n\} \subseteq E_\lambda(A) \end{aligned}$$

Ainsi $E_\lambda(L_A) \simeq E_\lambda(A)^n$.

Endomorphisme différence de produits de matrices

Propriétés sur l'endomorphisme

$$\varphi : M \mapsto AM - MB \text{ in } \mathcal{L}(M_n(\mathbb{K}))$$

Soit $A, B \in M_n(\mathbb{K})$, tel que χ_A scindé et B admet au moins une valeur propre. (\mathbb{K} algébriquement clos suffit).

Posons

$$\varphi : \begin{cases} M_n(\mathbb{K}) & \rightarrow & M_n(\mathbb{K}) \\ M & \mapsto & AM - MB \end{cases} \in \mathcal{L}(M_n(\mathbb{K}))$$

Il y a équivalence entre

1. $\text{Sp}(A) \cap \text{Sp}(B) = \emptyset$.
2. $\chi_A(B) \in \text{GL}_n(\mathbb{K})$.
3. φ injectif.
4. φ est un automorphisme.

De plus on a

$$\bullet \text{Sp}(\varphi) = \{\lambda - \mu, (\lambda, \mu) \in \text{Sp}(A) \times \text{Sp}(B)\}$$

Démonstration

- (3 \Leftrightarrow 4) Argument dimensionnel.

- (1 \Rightarrow 2) Pour tout $\lambda \in \text{Sp}(A)$

$$\lambda \notin \text{Sp}(B)$$

$$\ker(B - \lambda I_n) = E_\lambda(B) = \{0\}$$

$$B - \lambda I_n \in \text{GL}_n(\mathbb{K})$$

Ainsi

$$\chi_A(B) = \prod_{\lambda \in \text{Sp}(A)} (B - \lambda I_n)^{m_\lambda} \in \text{GL}_n(\mathbb{K})$$

- (2 \Rightarrow 3) Soit $M \in \ker \varphi$

$$AM = MB$$

$$\forall k \in \mathbb{N}, A^k M = MB^k$$

$$0 = \chi_A(A)M = \underbrace{\chi_A(B)}_{\in \text{GL}_n(\mathbb{K})} M$$

$$M = 0$$

- (3 \Rightarrow 1) Par contraposé, supposons qu'on dispose de $\lambda \in \text{Sp}(A) \cap \text{Sp}(B)$.

On sait que $\chi_B = \chi_{B^\top}$ donc toute valeur propre de B est valeur propre de B^\top .

Soit X, Y vecteurs propres non nuls de A et B^\top .

$$\begin{aligned} \varphi(XY^\top) &= AXY^\top - XY^\top B \\ &= AXY^\top - X(B^\top Y)^\top \\ &= \lambda XY^\top - \lambda XY^\top \\ &= 0 \end{aligned}$$

Or $XY^\top \neq 0$ d'où φ non injective.

- Soit $\lambda \in \text{Sp}(A), \mu \in \text{Sp}(B)$. X, Y vecteurs propres non nuls de A et B^\top .

$$\begin{aligned} \varphi(XY^\top) &= AXY^\top - XY^\top B \\ &= \lambda XY^\top - \mu XY^\top \\ &= (\lambda - \mu)XY^\top \end{aligned}$$

D'où $\lambda - \mu \in \text{Sp}(\varphi)$

- Soit $\alpha \in \text{Sp}(\varphi)$, M vecteur propre non nul associé.

$$\begin{aligned} \varphi(M) &= AM - MB = \alpha M \\ \underbrace{(A - \alpha I_n)}_{\tilde{A}} M - MB &= 0 \end{aligned}$$

Avec $\chi_{\tilde{A}}$ scindé (pour toute valeur propre λ de A , $\lambda - \alpha$ est valeur propre de \tilde{A})

Posons $\varphi' : N \mapsto \tilde{A}N - NB$

$$\varphi'(M) = 0$$

Donc φ' non injectif d'où

$$\{\mu\} \subseteq \text{Sp}(\tilde{A}) \cap \text{Sp}(B) \neq \emptyset$$

Ainsi $\alpha + \mu \in \text{Sp}(A)$.

Endomorphisme commutateur de matrices

Propriétés sur les endomorphismes de la forme $M \mapsto AM - MA \in \mathcal{L}(M_n(\mathbb{K}))$.

Soit $A \in \mathcal{M}_n(\mathbb{K})$ tel que χ_A scindé.

$$\varphi_A : \begin{cases} M_n(\mathbb{K}) & \rightarrow M_n(\mathbb{K}) \\ M & \mapsto AM - MA \end{cases} \in \mathcal{L}(M_n(\mathbb{K}))$$

On a les propriétés de $M \mapsto AM - MB$, et de plus

- Si A est nilpotent alors φ_A l'est.
- Si A est diagonalisable alors φ_A aussi.

Démonstration

- Supposons A nilpotent d'ordre q . Posons

$$\begin{aligned} M_n(\mathbb{K}) & \rightarrow M_n(\mathbb{K}) \\ L_A : M & \mapsto AM \\ R_A : M & \mapsto MA \end{aligned}$$

On sait que L_A et R_A sont nilpotents d'ordre q car A l'est.

De plus $L_A \circ R_A = AMA = R_A \circ L_A$ d'où

$$\varphi_A = L_A - R_A$$

$$\varphi_A^{2q} = \sum_{k=0}^{2q} \binom{2q}{k} (-1)^k R_A^k \circ L_A^{2q-k} = 0$$

- Supposons A diagonalisable.

On sait que L_A et R_A commutent et sont diagonalisables, donc ils sont codiagonalisables :

$$\varphi_A = L_A - R_A$$

Est diagonalisable.

Endomorphismes nilpotents cycliques

Caractérisation des sev stables par un endomorphisme nilpotent cyclique.

Soit $u \in \mathcal{L}(E)$ nilpotent cyclique.

Les seuls sev de E stables par u sont les $(\ker u^k)_{k \in \llbracket 0, n \rrbracket}$.

Démonstration

Ils sont stables comme \ker d'un endomorphisme commutant avec u .

Soit F sev stable par u . Soit \tilde{u} induit par u sur F qui est nilpotent car $\tilde{u}^n = 0$.

Or l'ordre de nilpotence de \tilde{u} est majoré par $d = \dim F : \tilde{u}^d = 0$.

Donc $F \subseteq \ker u^d$.

De plus par les noyaux itérées

$$\underbrace{\ker u}_{\dim 1} \subsetneq \cdots \subsetneq \underbrace{\ker u^d}_{\dim d} \subsetneq \cdots \subsetneq \underbrace{\ker u^n}_{\dim n}$$

D'où $F = \ker u^d$.

Produit de Kronecker et diagonalisabilité

Diagonalisabilité du produit de Kronecker de matrices (dimension $2n$).

Soit $L = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{K})$ et $A \in M_n(\mathbb{K})$. On pose le produit de Kronecker

$$M = L \otimes A = \begin{pmatrix} \alpha A & \beta A \\ \gamma A & \delta A \end{pmatrix} \in M_{2n}(\mathbb{K})$$

Alors

- Si L est diagonalisable, M est diagonalisable ssi A l'est.
- Si $L = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, M est diagonalisable ssi $A = 0$.

Démonstration

- On suppose L diagonalisable :

$$L = P \begin{pmatrix} \lambda & \\ & \mu \end{pmatrix} P^{-1} \quad P = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{K}) \\ P^{-1} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

On remarque

$$Q = P \otimes I_n = \begin{pmatrix} aI_n & bI_n \\ cI_n & dI_n \end{pmatrix}$$

$$Q' = P \otimes I_n = \begin{pmatrix} a'I_n & b'I_n \\ c'I_n & d'I_n \end{pmatrix}$$

$$QQ' = \begin{pmatrix} I_n & \\ & I_n \end{pmatrix} = I_{2n}$$

$$Q'MQ = \begin{pmatrix} a'I_n & b'I_n \\ c'I_n & d'I_n \end{pmatrix} \begin{pmatrix} \alpha A & \beta A \\ \gamma A & \delta A \end{pmatrix} \begin{pmatrix} aI_n & bI_n \\ cI_n & dI_n \end{pmatrix} \\ = \begin{pmatrix} \lambda A & \\ & \mu A \end{pmatrix}$$

Donc M est diagonalisable ssi A l'est.

- Pour $L = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

$$M^k = \begin{pmatrix} A^k & kA^k \\ 0 & A^k \end{pmatrix} \quad (\text{récurrence})$$

Donc pour tout $P \in \mathbb{K}[X]$

$$P(M) = \begin{pmatrix} P(A) & AP'(A) \\ 0 & P(A) \end{pmatrix}$$

Si M est diagonalisable, Π_M est SARS.

$$\Pi_M(M) = 0 \Leftrightarrow \begin{cases} \Pi_M(A) = 0 \\ A\Pi_M(A) = 0 \end{cases}$$

Comme $\Pi_M(A) = 0$, A est diagonalisable.

Or Π_M est SARS : $\Pi_M \wedge \Pi_{M'} = 1$ donc $P' \wedge \Pi_A = 1$ car $\Pi_A \mid \Pi_M$.

Donc $\Pi_{M'}(A) \in \text{GL}_n(\mathbb{K})$ et $A\Pi_{M'}(A) = 0$ d'où $A = 0$.

Cotrigonalisation

Critère de Cotrigonalisabilité d'une famille d'endomorphismes.

Soit $(u_i)_i \in \mathcal{L}(E)^I$ une famille d'endomorphismes trigonalisables qui commutent.

Il existe une base e de E tel que pour tout $i \in I$, $\mathcal{M}_e(u_i)$ soit triangulaire supérieure.

Démonstration : structure

On voudra toujours

1. Trouver un vecteur propre commun
2. Faire une récurrence sur la dimension.

Faisons d'abord la 2^e étape dans le cas général :

Supposons que toute famille $(u_i)_i \in \mathcal{L}(E)^I$ d'endomorphismes trigonalisables qui commutent admette un vecteur propre commun.

Cas $n = 1$ évident.

Supposons la propriété sur tout \mathbb{K} -ev de dimension strictement inférieur à n .

Soit e_1 vecteur propre commun aux éléments de $(u_i)_i$ associé aux valeurs propres $(\lambda_i)_i \in \mathbb{K}^I$.

On complète e_1 en la base (e_1, \dots, e_n) . Pour tout $i \in I$

$$\mathcal{M}_e(u_i) = \left(\begin{array}{c|c} \lambda_i & * \\ \hline 0 & A_i \end{array} \right) \quad \chi_{u_i} = \chi_{A_i}(X - \lambda)$$

Or χ_{u_i} scindé donc χ_A scindé : χ_A est trigonalisable.

De plus les $(A_i)_i$ commutent car mes $(u_i)_i$ aussi.

Par hypothèse de récurrence on conclut.

Démonstration : deux endomorphismes

Soit $u, v \in \mathcal{L}(E)$ trigonalisables qui commutent.

Soit $\lambda \in \text{Sp}(u)$, $E_\lambda(u) \neq \{0\}$ est stable par v .

Notons \tilde{v} induit par v sur $E_\lambda(u)$, qui est encore trigonalisable, et admet donc un vecteur propre e_1 .

Puis récurrence.

Démonstration : famille finie

Par récurrence sur d cardinal de la famille.

Cas 1 et 2 endomorphismes traités.

On suppose que toute famille de cardinal inférieur à d admet un vecteur propre commun.

Soit $u_1, \dots, u_{d+1} \in \mathcal{L}(E)$ trigonalisables qui comutent.

Soit x vecteur propre commun aux u_1, \dots, u_d associé aux valeurs propres $\lambda_1, \dots, \lambda_d \in \mathbb{K}$.

$$\{x\} \in F = \bigcap_{k=1}^d \underbrace{E_{\lambda_k}(u_k)}_{\text{stable par } v} \neq \emptyset$$

Donc F est stable par v , on peut donc y induire \tilde{v} qui est trigonalisable et admet donc e_1 vecteur propre commun aux

u_1, \dots, u_{d+1} .

Démonstration : famille infinie

Soit $(u_i)_i \in \mathcal{L}(E)^I$ une famille quelconque d'endomorphismes trigonalisables qui commutent.

$\text{Vect}(u_i)_{i \in I}$ est un sev de $\mathcal{L}(E)$ et admet donc une base u_{i_1}, \dots, u_{i_d} .

C'est une famille finie, donc cotrigonalisable dans une base e .

Et pour tout $i \in I$, $u_i \in \text{Vect}(u_{i_1}, \dots, u_{i_d})$ donc $\mathcal{M}_e(u_i)$ est triangulaire supérieur (comme combinaison linéaire de matrices qui le sont).

Exercice : polynôme caractéristique d'une somme d'endomorphismes

Soit E un \mathbb{C} -ev de dimension finie, $u, v \in \mathcal{L}(E)$ qui commutent, tel que v est nilpotent.

Montrer que $\chi_{u+v} = \chi_u$ (Exercice 106).

Deux perspectives

1. Comme E est un \mathbb{C} -ev, u et v sont trigonalisables, et commutent, donc sont cotrigonalisable.

Ainsi on dispose de e base de E tel que

$$\mathcal{M}_e(u) = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

$$\mathcal{M}_e(v) = \begin{pmatrix} 0 & & * \\ & \ddots & \\ & & 0 \end{pmatrix}$$

$$\mathcal{M}_e(u+v) = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

$$\chi_{u+v} = \chi_u$$

Exercice : commutateur qui vaut l'un des opérande

Soit E un \mathbb{K} -ev (car $\mathbb{K} = 0$) et $u, v \in \mathcal{L}(E)$ tels que $uv - vu = u$.

1. Montrer que u est nilpotent.
2. Montrer que si $\mathbb{K} = \mathbb{C}$, u et v sont cotrigonalisable.

1. Deux méthodes :

- On considère

$$\varphi_v : \begin{cases} \mathcal{L}(E) & \rightarrow & \mathcal{L}(E) \\ w & \mapsto & wv - vw \end{cases}$$

$$\varphi_v(u^k) = ku^k$$

Donc si $u^k \neq 0$, $k \in \text{Sp}(\varphi_v)$ qui est fini, donc on dispose de $k \in \mathbb{N}^*$ tel que $u^k = 0$.

- On remarque

$$P(u)v - vP(u) = uP'(u)$$

En particulier pour $P = \Pi_u$

$$0 = u\Pi'_u(u)$$

$$\underbrace{\Pi_u}_{\deg d} \mid \underbrace{X\Pi'_u}_{\deg d}$$

$$X\Pi'_u = c\Pi_u$$

Donc

$$dX^d + \sum_{k=0}^{d-1} ka_k X^k = cX^d + \sum_{k=0}^{d-1} ca_k X^k$$

$$c = d$$

$$\forall k \in \llbracket 0, d-1 \rrbracket, da_k = ka_k$$

$$\forall k \in \llbracket 0, d-1 \rrbracket, a_k = 0$$

$$\Pi_u = X^d$$

2. Comme u est nilpotent,

$$\text{Sp}(u) = \{0\}.$$

$$(uv - vu)(\ker u) = u(\ker u)$$

$$u(v(\ker u)) = 0$$

$$v(\ker u) \subseteq \ker u$$

Donc $\ker u$ est stable par v , posons \tilde{v} induit sur $\ker u$. Or \tilde{v} admet un vecteur propre commun $x \in \ker u = E_0(u)$.

Ainsi par récurrence sur la dimension de E :

Supposons la propriété pour tout \mathbb{C} -ev de dimension inférieur strictement à n .

Soit e_1 vecteur propre commun à u et v associé aux valeurs propres 0 et λ .

Soit $e' = (e_1, e'_2, \dots, e'_n)$ base de E .

$$\mathcal{M}_{e'}(u) = \begin{pmatrix} 0 & * \\ 0 & A \end{pmatrix}$$

$$\mathcal{M}_{e'}(v) = \begin{pmatrix} \lambda & * \\ 0 & B \end{pmatrix}$$

Et $AB - BA = A$ car $uv - vu = u$ donc on dispose de

(e_2, \dots, e_n) qui cotrigonalisent A et B .

Exercice : critère de nilpotence sur la trace des puissances

Soit E un \mathbb{K} -ev de dimension n ($\mathbb{K} \subseteq \mathbb{C}$).

1. Soit $u \in \mathcal{L}(E)$, montrer que u est nilpotent ssi pour tout $k \in \mathbb{N}^*$, $\text{tr}(u^k) = 0$.
2. Soit $u \in \mathcal{L}(E)$ tel que pour tout $k \in \mathbb{N}^*$

$$\text{tr } u^k = \sum_{i=1}^n \lambda_i^k \quad \lambda_1, \dots, \lambda_n \in \mathbb{C}$$

Montrer que

$$\chi_u = \prod_{k=1}^n (X - \lambda_k)$$

Dans les deux cas, $\mathbb{K} \subseteq \mathbb{C}$, donc u est trigonalisable dans \mathbb{C} .

$$\mathcal{M}_e(u) = \begin{pmatrix} \mu_1 & & * \\ & \ddots & \\ & & \mu_n \end{pmatrix} = D$$

$$\forall k \in \mathbb{N}, \quad \text{tr } u^k = \text{tr } D^k = \sum_{i=1}^n \mu_i^k$$

Posons $\{\mu_1, \dots, \mu_n\} = \{\alpha_1, \dots, \alpha_d\}$ deux à deux distincts.

$$\chi_u = \prod_{k=1}^d (X - \alpha_k)^{m_k}$$

$$\text{tr } u^k = \sum_{i=1}^d m_i \alpha_i^k \quad (*)$$

1. Par l'absurde : on suppose $d \geq 2$ et $\alpha_1 = 0$ (éventuellement $m_1 = 0$).

Par (*) :

$$\forall P \in X\mathbb{K}[X], \quad \sum_{k=1}^d m_k P(\alpha_k) = 0$$

Ainsi par interpolation de lagrange : pour $i \in \llbracket 2, d \rrbracket$,

$$P(\alpha_i) = 1$$

$$\forall j \neq i, \quad P(\alpha_j) = 0$$

$$P(\alpha_i) = P(0) = 0 \text{ d'où } X \mid P$$

$$\sum_{k=1}^d m_k P(\alpha_k) = m_i = 0$$

2. Pour tout $k \in \mathbb{N}^*$

$$\sum_{i=1}^n \mu_i^k = \sum_{i=1}^n \lambda_i^k$$

On considère $\{\lambda_1, \dots, \lambda_n\} \cup \{\mu_1, \dots, \mu_n\} = \{\beta_1, \dots, \beta_N\}$ deux à deux distincts.

Pour $i \in \llbracket 1, n \rrbracket$

$$n_i = |\{k \in \llbracket 1, n \rrbracket \mid \mu_k = \beta_i\}|$$

$$m_i = |\{k \in \llbracket 1, n \rrbracket \mid \lambda_k = \beta_i\}|$$

Donc pour tout $k \in \mathbb{N}^*$

$$\forall k \in \mathbb{N}^*, \quad \sum_{i=1}^N n_i \beta_i^k = \sum_{i=1}^N m_i \beta_i^k$$

$$\Leftrightarrow \forall k \in \mathbb{N}^*, \quad \sum_{i=1}^N (n_i - m_i) \beta_i^k = 0$$

Or $V(\beta_1, \dots, \beta_N) \neq 0$ d'où $m_i = n_i$.

Calcul de puissance de matrice : cas diagonalisable

Méthodes de calcul des puissances d'une matrice diagonalisable.

Soit $A \in M_n(\mathbb{K})$ diagonalisable.

1. Matrice diagonale :

On dispose de $P \in GL_n(\mathbb{K})$ (à calculer) tel que

$$A = P \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix} P^{-1}$$

$$A^k = P \begin{pmatrix} \alpha_1^k & & \\ & \ddots & \\ & & \alpha_n^k \end{pmatrix} P^{-1}$$

2. Lagrange : notons $d = \deg \Pi_A$

$$A^k \in \mathbb{K}[u] = \text{Vect}(I_n, A, \dots, A^{d-1})$$

Donc on dispose de $P \in \mathbb{K}_{d-1}[X]$ tel que $A^k = P(A)$.

Explicitons le :

$$\mathbb{K}^n = \bigoplus_{i=1}^N E_{\lambda_i}$$

Soit $X \in \mathbb{K}^n$

$$X = \underbrace{X_1}_{\in E_{\lambda_1}} + \dots + \underbrace{X_d}_{\in E_{\lambda_d}}$$

$$AX = \lambda_1 X_1 + \dots + \lambda_d X_d$$

$$A^k X = \lambda_1^k X_1 + \dots + \lambda_d^k X_d$$

$$P(A)X = P(\lambda_1)X_1 + \dots + P(\lambda_d)X_d$$

Ainsi avec P construit par interpolation de Lagrange afin de vérifier

$$\forall i \in \llbracket 1, d \rrbracket, P(\lambda_i) = \lambda_i^k$$

$$P \in \mathbb{K}_{d-1}[X]$$

On a alors $P(A)X = A^k X$ pour tout X , d'où $P(A) = A^k$.

Calcul de puissance de matrice : polynôme annulateur

Méthodes de calcul des puissances d'une matrice grâce à un polynôme annulateur.

Soit $A \in M_n(\mathbb{K})$, $P \in \mathbb{K}[X]$ annulateur de degré d .

$$X^k = QP + R$$

$$A^k = \underbrace{QP(A)}_0 + R(A)$$

Avec $R \in \mathbb{K}_{d-1}[X]$.

Si $P = (X - \lambda)^m$ on trouve le reste de la division euclidienne grâce à la formule de Taylor :

$$Q = \overbrace{\sum_{k=0}^{m-1} \frac{Q^{(k)}(\lambda)}{k!} (X - \lambda)^k}^{\text{reste}}$$

$$+ (X - \lambda)^m \underbrace{\sum_{k=m}^{\deg Q} \frac{Q^{(k)}(\lambda)}{k!} (X - \lambda)^{k-m}}_{\text{quotient}}$$

$$A^p = \sum_{k=0}^{m-1} \binom{p}{k} \lambda^{p-k} (A - \lambda I_n)^k$$

Équations matricielles

Méthodes de résolutions d'équations matricielles.

Soit $A \in M_n(\mathbb{K}), P \in \mathbb{K}[X]$.

On cherche à résoudre les équations de la forme

$$P(M) = A$$

Idées

- $MA = AM$ car $A \in \mathbb{K}[M]$.
- Ainsi M laisse stable
 - Les sous-espaces propres de A
 - Les sous-espaces caractéristiques de A
 - Tout les $\ker Q(A)$
- Pour Q annulateur de A , $Q \circ P$ est annulateur de M : si $Q \circ P$ est SARS, M est diagonalisable.

Résolutions cas simple

Si χ_A SARS :

$$\chi_A = \prod_{k=1}^n (X - \lambda_k)$$

$$A = R \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} R^{-1}$$

$$R = (C_1 \ \cdots \ C_n)$$

Avec C_1, \dots, C_n vecteurs propres associés aux $\lambda_1, \dots, \lambda_n$.

Si M est solution, M laisse stable tout les $E_{\lambda_k} = \text{Vect}(C_k)$

$$MC_k = \mu_k C_k$$

$$M = R \begin{pmatrix} \mu_1 & & \\ & \ddots & \\ & & \mu_n \end{pmatrix} R^{-1}$$

Or

$$P(M) = R \begin{pmatrix} P(\mu_1) & & \\ & \ddots & \\ & & P(\mu_n) \end{pmatrix} R^{-1}$$

$$= A$$

D'où $P(\mu_k) = \lambda_k$ pour tout $k \in \llbracket 1, n \rrbracket$.

Racine k-ème de matrices

Méthodes général de résolution de l'équation $M^p = A$.

Soit $A \in M_n(\mathbb{K})$ et $p \in \mathbb{N}$.

- Si A est nilpotent : il peut ne pas exister de solutions, par exemple :

Si A nilpotent d'ordre n et $p \geq 2$

$$A^n = (M^p)^n = 0$$

D'où M nilpotent

$$M^n = A^{\lceil \frac{n}{p} \rceil} = 0$$

Absurde.

- Cas $A = I_n + N$ avec N nilpotent.

Idée : DL de $(1 + x)^{\frac{1}{k}}$

$$(1 + x)^{\frac{1}{k}} = P_k(x) + o_{x \rightarrow 0}(x^{n-1})$$

$$P_k(X) = 1 + \sum_{j=1}^{n-1} \prod_{i=0}^{n-1} \left(\frac{1}{k} - i \right) \frac{x^j}{j!} \in \mathbb{R}_{n-1}[X]$$

$$\begin{aligned} 1 + x &= (P_k(x) + o_{x \rightarrow 0}(x^{n-1}))^k \\ &= Q_k(x) + o_{x \rightarrow 0}(x^{n-1}) \end{aligned}$$

Par unicité de la partie principale du DL :

$$1 + X = Q_k(X)$$

Où Q_k est P_k^k tronqué à $n - 1$ termes

$$1 + X = P_k^k(X) - X^n R_k(X)$$

$$A = I_n + N = P_k^k(N) - \underbrace{N^n R_k(N)}_0$$

D'où $P_k(N)$ est solution.

- Cas $A \in M_n(\mathbb{C})$ tel que $0 \notin \text{Sp}(A)$: Pour tout $k \in \mathbb{N}^*$:

$$\chi_A = \prod_{k=1}^q (X - \lambda_k)^{m_k}$$

$$A = P \begin{pmatrix} \lambda_1 I_{m_1} + N_1 & & \\ & \ddots & \\ & & \lambda_q I_{m_q} + N_q \end{pmatrix} P^{-1}$$

Pour tout $j \in \llbracket 1, q \rrbracket$, on dispose de \tilde{M}_j et μ_j tels que

$$\mu_j^k = \lambda_j$$

$$\tilde{M}_j^k = I_{m_j} + \frac{1}{\lambda_j} N_j$$

On définit alors

$$M_j = \mu_j \tilde{M}_j$$

$$\begin{aligned} M_j^k &= \mu_j^k I_{m_j} + \frac{\mu_j^k}{\lambda_j} N_j \\ &= \lambda_j I_{m_j} + N_j \end{aligned}$$

Ainsi

$$M = P \begin{pmatrix} M_1 & & \\ & \ddots & \\ & & M_q \end{pmatrix} P^{-1}$$

Est solution :

$$\begin{aligned} M^k &= P \begin{pmatrix} M_1^k & & \\ & \ddots & \\ & & M_q^k \end{pmatrix} P^{-1} \\ &= A \end{aligned}$$

Exercice : lien entre diagonalisabilité d'un endomorphisme et son carré

Soit $u \in \mathcal{L}(E)$ où E est un \mathbb{C} -ev, montrer que

$$u \text{ diagonalisable} \\ \Leftrightarrow \begin{cases} u^2 \text{ diagonalisable} \\ \ker u = \ker u^2 \end{cases}$$

- Supposons u diagonalisable, on dispose de e base de E tel que

$$\mathcal{M}_e(u) = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \\ \mathcal{M}_e(u^2) = \begin{pmatrix} \lambda_1^2 & & \\ & \ddots & \\ & & \lambda_n^2 \end{pmatrix}$$

D'où u^2 diagonalisable, et de plus $\ker u \subseteq \ker u^2$.

Posons $k \in \llbracket 0, n \rrbracket$ tel que

$$\lambda_1 = \dots = \lambda_k = 0 \\ \lambda_{k+1}, \dots, \lambda_n \neq 0$$

On a bien $\ker u^2 = \ker u$ (Vision matricielle).

- Supposons $0 \notin \text{Sp}(u)$, u^2 diagonalisable et $\ker u^2 = \ker u$.

$$\Pi_{u^2} = \prod_{k=1}^q (X - \lambda_k)$$

$$\Pi_{u^2}(u^2) = \prod_{k=1}^q (X - \delta_k)(X + \delta_k)(u) = 0$$

Avec $\delta_k^2 = \lambda_k$. Ainsi u est annuler par un polynôme SARRS, donc diagonalisable.

- Supposons $0 = \lambda_1 \in \text{Sp}(u)$, u^2 diagonalisable et $\ker u^2 = \ker u$.

$$E = \bigoplus_{k=1}^q \ker(u^2 - \lambda_k \text{id}) \\ = \bigoplus_{k=2}^q \ker(u^2 - \lambda_k \text{id}) \oplus \ker u^2 \\ = \bigoplus_{k=2}^q \ker(u - \delta_k \text{id})(u + \delta_k \text{id}) \\ \oplus \underbrace{\ker u^2}_{\ker u}$$

D'où u diagonalisable.

Recherche d'hyperplans stables

Méthodes de recherche
d'hyperplans stables.

Soit $A \in M_n(\mathbb{K})$, H hyperplan de \mathbb{K}^n .

On dispose de $L \in M_{1n}(\mathbb{K})$ tel que

$$H = \{X \in \mathbb{K}^n \mid LX = 0\} = \ker L$$

H est stable par A ssi

$$L^T \text{ vecteur propre de } A^T$$

Démonstration

$$AH \subseteq H \Leftrightarrow \ker L \subseteq \ker LA$$

$$\Leftrightarrow \exists \lambda \in \mathbb{K}, LA = \lambda L$$

$$\Leftrightarrow \exists \lambda \in \mathbb{K}, A^T L^T = \lambda L^T$$

Pseudo-commutativité du polynôme caractéristique

Pour $A \in M_{pn}(\mathbb{K})$ et $B \in M_{np}(\mathbb{K})$,
lien entre χ_{AB} et χ_{BA} .

Soient $A \in M_{pn}(\mathbb{K})$ et $B \in M_{np}(\mathbb{K})$.

$$AB \in M_p(\mathbb{K}) \quad BA \in M_n(\mathbb{K})$$

$$X^n \chi_{AB} = X^p \chi_{BA}$$

$$\text{Sp}(AB) \setminus \{0\} = \text{Sp}(BA) \setminus \{0\}$$

$$\forall \lambda \in \mathbb{K} \setminus \{0\},$$

$$\dim E_\lambda(AB) = \dim E_\lambda(BA)$$

Si $p = n$ (A et B sont carrés) alors

$$\chi_{AB} = \chi_{BA}$$

Démonstration

• Cas $A = J_r$:

$$A = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array} \right) \quad B = \left(\begin{array}{c|c} B_1 & B_2 \\ \hline B_3 & B_4 \end{array} \right)$$

$$AB = \left(\begin{array}{c|c} B_1 & B_2 \\ \hline 0 & 0 \end{array} \right) \quad BA = \left(\begin{array}{c|c} B_1 & 0 \\ \hline B_3 & 0 \end{array} \right)$$

$$\chi_{AB} = \chi_{B_1} X^{p-r}$$

$$\chi_{BA} = \chi_{B_1} X^{n-r}$$

• Cas général : $A = PJ_rQ$

$$AB = PJ_rQB$$

$$= P(J_rQB P)P^{-1}$$

$$BA = BPJ_rQ$$

$$= Q^{-1}(QB P J_r)Q$$

Donc

$$X^n \chi_{AB} = X^n \chi_{J_rQB P}$$

$$= X^p \chi_{QB P J_r} = X^p \chi_{BA}$$

• Pour tout $X \in E_\lambda(AB)$

$$ABX = \lambda X$$

$$BABX = \lambda BX$$

$$BX \in E_\lambda(BA)$$

Ainsi

$$\theta : \begin{cases} E_\lambda(AB) & \rightarrow E_\lambda(BA) \\ X & \mapsto BX \end{cases}$$

Est linéaire injectif, donc

$$\dim E_\lambda(BA) \geq \dim E_\lambda(AB)$$

Avec égalité par symétrie.

Réduction de matrice dans rang 1

Propriétés de réduction de matrices de rang 1.

Soit $A \in M_n(\mathbb{K})$ tel que $\text{rg } A = 1$.

1. On dispose de $L \in M_{1n}(\mathbb{K})$, $C \in M_{n1}(\mathbb{K})$ tels que $A = CL$.
2. $A^2 = (\text{tr } A)A$.
3. $X(X - \text{tr } A)$ annule A .
4. Si $\text{tr } A \neq 0$, A est diagonalisable.
5. Si $\text{tr } A = 0$, A est nilpotente.

Démonstration

1. Comme $\text{rg } A = \text{rg } (C_1 \cdots C_n) = 1$, on dispose de $k \in \llbracket 1, n \rrbracket$ tel que $\{C_1, \dots, C_n\} \subseteq \text{Vect}(C_k)$:

$$A = (C_1 \cdots C_n) = C_k(\alpha_1 \cdots \alpha_n) \\ = \underbrace{\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}}_C \underbrace{(\alpha_1 \cdots \alpha_n)}_L$$

2. $A^2 = C \underbrace{LCL}_{\text{tr } A} = (\text{tr } A)A$

3. Évident.

4. Si $\text{tr } A \neq 0$, A est annuler par $X(X - \text{tr } A)$ SARS donc A est diagonalisable.

5. Si $\text{tr } A = 0$, X^2 annule A , donc A est nilpotente.

Suites récurrentes linéaires

Propriétés, méthodes d'étude de suites récurrentes linéaires.

Pour tout $(x_0, \dots, x_{p-1}) \in \mathbb{K}^p$, pour tout $n \in \mathbb{N}$ on définit la suite $(x_n)_n \in \mathbb{K}^{\mathbb{N}}$

$$x_{n+p} = \sum_{k=0}^{p-1} a_k x_{n+k} \quad (*)$$

$$\mathcal{S} = \left\{ (x_n)_n \in \mathbb{K}^{\mathbb{N}} \mid (*) \right\}$$

$$\dim \mathcal{S} = p$$

Où \mathcal{S} est un \mathbb{K} -ev.

$$A = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ a_0 & a_1 & \cdots & a_{p-1} \end{pmatrix} = C_P^T$$

$$P = X^p - \sum_{k=0}^{p-1} a_k X^k$$

Ainsi si $X_n = \begin{pmatrix} x_n \\ \vdots \\ x_{n+p} \end{pmatrix}$

$$AX_n = X_{n+1}$$

$$X_n = A^n X_0$$

Si χ_A est SARS

$$\chi_A = \prod_{k=1}^p (X - \lambda_k)$$

$$\mathcal{S} = \text{Vect} \left((\lambda_k^n)_{n \in \mathbb{N}} \right)_{k \in \llbracket 1, p \rrbracket}$$

Démonstration

• Si $P = \chi_{C_P} = \chi_A$ est SARS

$$X^p - \sum_{k=0}^{p-1} a_k X^k = \prod_{k=1}^p (X - \lambda_k)$$

A est diagonalisable comme χ_A est SARS

$$A = Q \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_p \end{pmatrix} Q^{-1}$$

$$A^n = \sum_{k=1}^p \lambda_k^n \Pi_k$$

Où les Π_k sont les projecteurs issus de la décomposition en sous-espaces propres.

$$\begin{pmatrix} x_n \\ \vdots \\ x_{n+p} \end{pmatrix} = X_n = A^n X_0$$

$$= \sum_{k=1}^p \lambda_k^n \Pi_k X_0$$

$$x_n = \sum_{k=1}^p \lambda_k^n \gamma_k$$

$$(x_n)_n = \sum_{k=1}^p \gamma_k (\lambda_k^n)_n$$

$$\in \text{Vect} \left((\lambda_k^n)_{n \in \mathbb{N}} \right)_{k \in \llbracket 1, p \rrbracket}$$

Soit $k \in \llbracket 1, p \rrbracket$

$$\chi_A(\lambda_k) = 0$$

$$\text{Donc } \lambda_k^p = \sum_{i=0}^{p-1} a_i \lambda_k^i$$

$$\forall n \in \mathbb{N}, \lambda_k^{p+n} = \sum_{i=0}^{p-1} a_i \lambda_k^{n+i}$$

$$(\lambda_k^n)_{n \in \mathbb{N}} \in \mathcal{S}$$

• Sinon

$$P = \prod_{k=1}^q (X - \lambda_k)^{m_k}$$

Posons

$$\delta : \begin{cases} \mathbb{K}^{\mathbb{N}} & \rightarrow & \mathbb{K}^{\mathbb{N}} \\ (y_n)_n & \mapsto & (y_{n+1})_n \end{cases}$$

Ainsi on a

$$\mathcal{S} = \ker P(\delta)$$

$$= \bigoplus_{k=1}^q \ker (\delta - \lambda_k)^{m_k}$$

► Montrons que $(n^d \lambda_k^n)_n \in \ker (\delta - \lambda_k \text{id})^{m_k} \subseteq \ker P(\delta) = \mathcal{S}$:

Définissons d'abord

$$\Delta : \begin{cases} \mathbb{K}[X] & \rightarrow & \mathbb{K}[X] \\ P(X) & \mapsto & P(X+1) - P(X) \end{cases}$$

On remarque que

$$P = \sum_{k=0}^d a_k X^k$$

$$\Delta(P) = \sum_{k=0}^d a_k [(X+1)^k - X^k]$$

$$= \sum_{k=0}^d a_k \left[\sum_{i=0}^{k-1} \underbrace{X^{k-1-i} X^i}_{\deg \leq k-1} \right]$$

$$\deg \Delta(P) \leq \deg P - 1$$

Ainsi $\Delta^{d+1} P = 0$.

Alors pour tout $k \in \llbracket 1, q \rrbracket$, $P \in \mathbb{K}_{m_k-1}[X]$

$$(\delta - \lambda_k \text{id})(P(n) \lambda_k^n)_n$$

$$= ([P(n+1) - P(n)] \lambda_k^{n+1})_n$$

$$= (\Delta(P)(n) \lambda_k^{n+1})_n$$

Donc

$$(\delta - \lambda_k)^{m_k} (P(n) \lambda_k^n)_n$$

$$= (\Delta^{m_k}(P)(n) \lambda_k^{n+1})_n$$

$$= 0$$

Ainsi pour $P(X) = X^d$ avec $d \in \llbracket 0, m_k - 1 \rrbracket$,

$$(n^d \lambda_k^n)_n \in \ker (\delta - \lambda_k \text{id})^{m_k}$$

► Montrons que la famille $\left((n^d \lambda_k^n)_{n \in \mathbb{N}} \right)_{d \in \llbracket 0, m_k - 1 \rrbracket}$ est libre.

Notons $u_d = (n^d \lambda_k^n)_{n \in \mathbb{N}}$.

Supposons

$$\sum_{i=0}^{m_k-1} \gamma_i u_i = 0$$

Alors pour tout $n \in \mathbb{N}$

$$\underbrace{\left(\sum_{i=0}^{m_k-1} \gamma_i n^i \right)}_{P_k(n)} \underbrace{\lambda_k^n}_{\neq 0} = 0$$

Et P_k est un polynôme qui s'annule sur \mathbb{N} entier, et est donc nul.

Donc on dispose de bases des $\ker (\delta - \lambda_k \text{id})^{m_k}$

$$\mathcal{S} = \text{Vect} \left((n^d \lambda_k^n)_{n \in \mathbb{N}} \right)_{\substack{d \in \llbracket 0, m_k - 1 \rrbracket \\ k \in \llbracket 1, q \rrbracket}}$$

Formule de newton

Soit $n \in \mathbb{N}$, $x, a, b \in \mathbb{C}$

$$x^n - 1 = ?$$

$$a^n - b^n = ?$$

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

$$a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-k-1}$$

Formules sur les coefficients binomiaux

Soit $k, n, p \in \mathbb{N}$

$$\binom{n}{0} = ? \qquad \binom{n}{n} = ?$$

$$\sum_{k=0}^n \binom{n}{k} = ? \qquad k \binom{n}{k} = ?$$

$$\binom{n}{n-k} = ? \qquad \binom{k}{p} \binom{n}{k} = ?$$

$$\binom{n}{k} + \binom{n}{k+1} = ?$$

Soit $k, n, p \in \mathbb{N}$

$$\binom{n}{0} = \binom{n}{n} = 1$$

$$\sum_{k=0}^n \binom{n}{k} = 2^n$$

$$\binom{n}{n-k} = \binom{n}{k}$$

$$k \binom{n}{k} = n \binom{n-1}{k-1}$$

$$\binom{k}{p} \binom{n}{k} = \binom{n}{p} \binom{n-p}{k-p}$$

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Formule du crible

Formule du crible : soit

$$A_1, \dots, A_n \subseteq E$$

$$\left| \bigcup_{k=1}^n A_k \right| = ?$$

Soit $A_1, \dots, A_n \subseteq E$

$$\begin{aligned} \left| \bigcup_{k=1}^n A_k \right| &= |A_1| + |A_2| + \dots + |A_n| \\ &\quad - |A_1 \cap A_2| - \dots - |A_{n-1} \cap A_n| \\ &\quad + |A_1 \cap A_2 \cap A_3| + \dots + |A_{n-2} \cap A_{n-1} \cap A_n| \\ &\quad \vdots \\ &\quad + (-1)^n |A_1 \cap A_2 \cap \dots \cap A_n| \end{aligned}$$

$$= \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq n} \left| \bigcap_{j=1}^k A_{i_j} \right|$$

Majorant, borne supérieure, élément maximale

Soit (E, \leq) un ensemble ordonné et $A \subseteq E$, définitions de

- Majorant
- Maximum
- Borne supérieure
- Élément maximale

Soit (E, \leq) un ensemble ordonné et $A \subseteq E$.

Majorant $M \in E$ est un majorant de A si $\forall x \in A, x \leq M$

Maximum M est le maximum de A si M est un majorant de A et $M \in A$. S'il existe il est unique.

Borne supérieure B est la borne supérieure de A si B est le plus petit majorant de A :
 $\forall M \in E, (\forall x \in A, x \leq M) \Rightarrow B \leq M$. Si elle existe elle est unique.

Élément maximale M est un élément maximale de A si M n'est plus petit que personne : $\nexists x \in A, M \leq x$.
 Dans le cas d'un ensemble totalement ordonné, seul un maximum est élément maximale, dans le cas d'un ensemble non totalement ordonné, il peut en exister plusieurs.

Axiomes d'un groupe

Soit G un ensemble muni d'une opération interne $*$, quels axiomes pour que $(G, *)$ ait une structure de groupe ?

Soit G un ensemble et $*$ une opération interne, $(G, *)$ forme un groupe si

i) Associativité :

$$\forall x, y, z \in G, x * (y * z) = (x * y) * z$$

ii) Existence d'un neutre :

$$\exists e \in G, \forall x \in G, x * e = e * x = x$$

iii) Existence d'inverse :

$$\forall x \in G, \exists y \in G, x * y = y * x = e$$

Vocabulaire d'ensemble structuré

Définitions du vocabulaire
suivant

- Magma
- Semi-groupe
- Monoïde
- Groupe

Ensemble	Loi interne	Associative	Neutre	Inverse	Nom
×	×				Magma
×	×	×			Semi-groupe
×	×	×	×		Monoïde
×	×	×	×	×	Groupe

Axiomes d'un sous-groupe

Soit $(G, *)$ un groupe, quels axiome pour que $H \subseteq G$ soit un sous-groupe ?

Soit $(G, *)$ un groupe et $H \subseteq G$, H est un sous-groupe de G si

i) Présence du neutre :

$$e \in H$$

ii) Stable par $*$:

$$\forall x, y \in H, x * y \in H$$

iii) Stable par inverse :

$$\forall x \in H, x^{-1} \in H$$

Théorème de Lagrange

Énoncer le théorème de Lagrange sur les groupes.

Soit (G, \cdot) un groupe fini et H un sous-groupe de G

$$|H| \mid |G|$$

Démonstration du Théorème de Lagrange

Démonstration du théorème de Lagrange

Soit (G, \cdot) un groupe fini et H un sous-groupe.

- Relation quotienté par $H : x \mathcal{R} y$ si $yx^{-1} \in H$ (relation d'équivalence). On note G/H l'ensemble des classes d'équivalences.
- Soit $x \in G$, \bar{x} sa classe d'équivalence pour \mathcal{R} . $\bar{x} = Hx = \{hx, h \in H\}$.

Par double inclusion :

- ▶ $Hx \subseteq \bar{x}$: Soit $y \in Hx$, $y = hx$ avec $h \in H$, donc $yx^{-1} = h \in H$ d'où $y \mathcal{R} x$ et $y \in \bar{x}$.
- ▶ $\bar{x} \subseteq Hx$: Soit $y \in \bar{x}$, $yx^{-1} = h \in H$, donc $y = hx \in Hx$.
- Donc $\forall x \in G, \bar{x} = Hx \simeq H$ d'où $|\bar{x}| = |H|$.
- Enfin par le lemme du berger : $|G/H| = \frac{|G|}{|H|}$ et donc $|H| \mid |G|$.

Relation de cardinal pour un morphisme de groupe

Soient $(G_1, +)$, (G_2, \cdot) des groupes et $\varphi : G_1 \rightarrow G_2$ un morphisme, avec G_1 fini. Que peut on dire de $|G_1|$?

Soient $(G_1, +)$, (G_2, \cdot) des groupes et $\varphi : G_1 \rightarrow G_2$ un morphisme, avec G_1 fini.

$$|G_1| = |\ker \varphi| \cdot |\operatorname{im} \varphi|$$

Axiomes d'un anneau

Soit A muni de deux opérations internes $+$ et \cdot , quels axiomes pour que $(A, +, \cdot)$ soit un anneau ?

$(A, +, \cdot)$ est un anneau si :

- i) $(A, +)$ est un groupe abélien
 - a) Associativité de $+$
 - b) Existence d'un neutre additif (0_A)
 - c) Existence d'opposés ($-x$)
 - d) Commutativité de $+$
- ii) Associativité de \cdot
- iii) Existence d'un neutre multiplicatif (1_A)
- iv) Distributivité de \cdot sur $+$

$$x(y + z) = xy + xz$$

$$(x + y)z = xz + yz$$

Diviseur de zéro

Définition de diviseur de 0 dans un anneau.

Soit $(A, +, \cdot)$ un anneau, $x \in A$ est dit diviseur de 0 (à gauche) si $x \neq 0$ et $\exists y \neq 0, \quad xy = 0$

Intégrité d'un anneau

Définition d'un anneau intègre.

Un anneau $(A, +, \cdot)$ est dit intègre si

- A est commutatif
- A n'admet aucun diviseur de 0

Groupe des inversibles

Définition de groupe des inversibles d'un anneau.

Le groupe des inversibles d'un anneau $(A, +, \cdot)$, est le groupe (A^\times, \cdot) .

Idéal d'un anneau

Définition d'un idéal d'un anneau, propriétés élémentaires.

Soit $(A, +, \cdot)$ un anneau et $I \subseteq A$, I est un idéal de A si

- I est un sous-groupe additif de A
- I est stable par produit externe : $\forall x \in I, \forall a \in A, ax \in I$

Propriétés :

- Si $1 \in I$ idéal de A , alors $I = A$.
- Plus généralement s'il existe $x \in I$ inversible, $I = A$.
- Une intersection quelconque d'idéaux est un idéal.
- Une somme finie d'idéaux est un idéal.
- Si $\varphi : A_1 \rightarrow A_2$ un morphisme d'anneau avec A_1 commutatif, $\ker \varphi$ est un idéal de A_1 .
- Pour tout $b \in A$, bA est un idéal de A .
- Un idéal engendré par un ensemble est le plus petit idéal le contenant, dans le cas d'un singleton $\{a\} \subset A$, il s'agit de aA .

Axiomes d'un corps

Soit K muni de deux opérations internes $+$ et \cdot , quels axiomes pour que $(K, +, \cdot)$ soit un corps ?

$(K, +, \cdot)$ est un corps si :

- i) $(K, +)$ est un groupe abélien
 - a) Associativité de $+$
 - b) Existence d'un neutre additif (0)
 - c) Existence d'opposés ($-x$)
 - d) Commutativité de $+$
- ii) Associativité de \cdot
- iii) Commutativité de \cdot
- iv) Existence d'un neutre multiplicatif (1)
- v) Distributivité de \cdot sur $+$
- vi) Existence d'inverses (sauf pour 0)

$$\forall x \in K \setminus \{0\}, \exists x^{-1} \in K$$

$$xx^{-1} = x^{-1}x = 1$$

Corps gauche, anneau à division

Qu'est-ce qu'un "corps gauche" ou "anneau à division" ?

Un corps gauche ou anneau à division et un anneau non commutatif dont tous les éléments sont inversible sauf 0. C'est un corps dont le produit n'est pas commutatif.

Axiomes d'un sous-corps

Soit $(K, +, \times)$ un corps, axiomes pour que $L \subseteq K$ soit un sous-corps ?

$(K, +, \times)$ un corps, $L \subseteq K$ est un sous-corps si :

- i) $0 \in L$
- ii) $1 \in L$
- iii) Stable par $+$
- iv) Stable par $-$ ou stable par opposé
- v) Stable par \times
- vi) Stable par $\nabla \cdot$ ou stable par inverse

Primalité de la caractéristique d'un corps

Si $(K, +, \cdot)$ est un corps de caractéristique non nulle, que peut-on dire sur celle ci ?

$(K, +, \cdot)$ un corps, notons p sa caractéristique, si $p \neq 0$ alors p est premier

Démonstration:

Notons $p = ab$ avec $a, b \in \mathbb{N}$

$$\begin{aligned} \left(\sum_{k=1}^a 1 \right) \left(\sum_{k=1}^b 1 \right) &= \sum_{k=1}^a \sum_{k=1}^b 1 \\ &= \sum_{k=1}^{ab=p} 1 \\ &= 0 \end{aligned}$$

Or un corps n'admet pas de diviseurs de 0, donc $\sum_{k=1}^a 1 = 0$ ou $\sum_{k=1}^b 1 = 0$, d'où

$$\text{ou} \quad \begin{aligned} a &= p, b = 1 \\ p &= b, a = 1 \end{aligned}$$

Donc p est premier.

Corps des fractions

Définition du corps des fractions d'un anneau intègre.

$(A, +', \cdot)$ un anneau intègre.

- Soit $(a, b), (c, d) \in A \times A \setminus \{0\}$, on définit la relation d'équivalence suivante :

$$(a, b) \mathcal{R} (d, c) \text{ si } ad = bc$$

- On note $\frac{a}{b}$ la classe d'équivalence de (a, b) .
- On définit les opérations $+$, \times sur les fractions

$$\frac{a}{b} + \frac{c}{d} = \frac{ad +' cb}{bd}$$

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

Le corps des fractions de A est le corps

$$(A \times A \setminus \{0\}, +, \times)$$

Théorème de Gauss

Théorème de Gauss.

Soit $a, b, c \in \mathbb{N}$, si $a \mid bc$ et $a \wedge b = 1$
alors $a \mid c$

Équations diophantiennes

Résolutions d'une équation de la forme $ax + by = c$ dans \mathbb{Z} .

Soit $a, b, c \in \mathbb{Z}$

$$(E) : \quad ax + by = c$$

- Solution homogène : On cherche un couple $(u, v) \in \mathbb{Z}^2$ (Bézout) tel que

$$au + bv = c$$

- Solution particulière : il en existe si

$$a \wedge b \mid c$$

- Les solutions sont

$$S = \begin{cases} x = x_p - kb' \\ y = y_p + ka' \end{cases}$$

avec (x_p, y_p) solution particulière

$$\text{et } a' = \frac{a}{a \wedge b}, \quad b' = \frac{b}{a \wedge b}$$

Nombres de Fermat

Que sont les nombres de Fermat, et quelques propriétés.

Le n -ème nombre de Fermat est

$$F_n = 2^{2^n} + 1$$

Ils sont impaires et premier entre eux :

Soit $n < m \in \mathbb{N}$,

$$(2^{2^n} - 1) \cdot F_n \qquad \cdot F_{n+1} \cdots F_{m-1}$$

$$(2^{2^n} - 1) \cdot (2^{2^n} + 1) \qquad \cdot F_{n+1} \cdots F_{m-1}$$

$$(2^{2^{n+1}} - 1) \cdot F_{n+1} \cdots F_{m-1}$$

$$\vdots$$

$$2^{2^m} - 1 = F_m - 2$$

Donc $F_n \mid F_m - 2$, d'où $F_m \wedge F_n \mid F_m - 2$, donc $F_m \wedge F_n \mid 2$, mais ils sont impaire donc premier entre eux.

Lemme d'Euclide

Théorème du lemme d'Euclide.

Soit $p \in \mathbb{P}$, $a, b \in \mathbb{Z}$,

$$p \mid ab \Rightarrow p \mid a \text{ ou } p \mid b$$

Plus algébriquement :

$\mathbb{Z}/p\mathbb{Z}$ est un anneaux intègre :

$$ab \equiv 0 [p] \Rightarrow a \equiv 0 [p] \text{ ou } b \equiv 0 [p]$$

Formule du nombre de diviseurs

Formule du nombre de diviseurs d'un entier.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$\text{nombre de diviseurs} = \prod_{i=1}^k (\alpha_k + 1)$$

Théorème des restes chinois

Théorème des restes chinois.

Soit $n, m \in \mathbb{N}^*$ premiers entre eux

- Formulation arithmétique :

$$\begin{aligned} \forall a \in \llbracket 0, m-1 \rrbracket, \forall b \in \llbracket 0, n-1 \rrbracket, \\ \exists ! x \in \llbracket 0, nm-1 \rrbracket, \\ x \equiv a \pmod{m} \text{ et } x \equiv b \pmod{n} \end{aligned}$$

- Formulation algébrique :

$$\begin{aligned} \mathbb{Z}/mn\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \varphi : \quad x &\mapsto \begin{pmatrix} x \pmod{m} \\ x \pmod{n} \end{pmatrix} \end{aligned}$$

est un isomorphisme
d'anneaux.

- Structure de preuve : injectivité
par $\ker \varphi$ + argument de
cardinal.

Petit théorème de Fermat

Petit théorème de Fermat.

- Première formulation :

$$\forall p \in \mathbb{P}, \forall a \in \mathbb{Z},$$

$$a \wedge p = 1 \Rightarrow a^{p-1} \equiv 1 [p]$$

- Deuxième formulation (moins forte) :

$$\forall p \in \mathbb{P}, \forall a \in \mathbb{Z},$$

$$a^p \equiv a [p]$$

- Démonstration : On étudie $(\mathbb{Z}/p\mathbb{Z})^\times$:

$$\forall a \in (\mathbb{Z}/p\mathbb{Z})^\times$$

$$\text{ord}(a) \mid p-1 \text{ (Lagrange)}$$

$$\text{donc } a^{p-1} \equiv 1 [p]$$

Indicatrice d'Euler

Définition de l'indicatrice d'Euler, et propriétés.

La fonction indicatrice d'Euler est

$$\varphi : \begin{array}{ccc} \mathbb{N}^* & \rightarrow & \mathbb{N} \\ n & \mapsto & |(\mathbb{Z}/n\mathbb{Z})^\times| \end{array}$$

Quelques propriétés :

$$\varphi(p) = p - 1$$

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

$$m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$$

$$\varphi(n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1})$$

$$\frac{\varphi(n)}{n} = \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$$

$$\sum_{d \in \text{Div}(n)} \varphi(d) = n$$

Pour se convaincre de la dernière :

$$\frac{1}{n} + \frac{2}{n} + \dots + \frac{n}{n}$$

Sous formes irréductibles ($p_i \wedge q_i = 1$)

$$\frac{p_1}{q_1} + \frac{p_2}{q_2} + \dots + \frac{p_n}{q_n}$$

Il y a n fractions, les $q_i \in \text{Div}(n)$, et pour chaque q_i , on a tous les $p_i \leq q_i$, qui sont premiers avec eux :

$$\underbrace{\sum_{d \in \text{Div}(n)}}_{\substack{\text{somme sur} \\ \text{tous les} \\ \text{dénominateur}}} \underbrace{\varphi(d)}_{\substack{\text{nombre de} \\ \text{fractions pour le} \\ \text{dénominateur } d}} = \underbrace{n}_{\substack{\text{nombre de} \\ \text{fractions}}}$$

Enfin, une généralisation du petit théorème de Fermat :

$$a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 [n]$$

Théorème de Bézout

Énoncé et preuve du théorème de Bézout.

- Soient $a, b \in \mathbb{N}$ et $d = a \wedge b$ alors il existe $u, v \in \mathbb{Z}$ tel que $au + bv = d$.
- Preuve : Soit $I = \{au + bv, (u, v) \in \mathbb{Z}\}$

I est un idéal de \mathbb{Z} , donc $\exists d \in \mathbb{Z}, I = d\mathbb{Z}$ (principalité de \mathbb{Z}).
Donc $d \mid a$ et $d \mid b$.

Soit ∂ tel que $\partial \mid a$ et $\partial \mid b, \forall x \in I, \partial \mid x$, en particulier $\partial \mid d$ d'où $\partial \leq d$.

$a \wedge b = d \in I$ d'où $\exists u, v \in \mathbb{Z}, d = au + bv$

Propriétés diviseurs communs

Soit $a, b \in \mathbb{Z}$

$$x \mid a \text{ et } x \mid b \text{ ssi } ?$$

$$a \mid y \text{ et } b \mid y \text{ ssi } ?$$

$$a\mathbb{Z} + b\mathbb{Z} = ?$$

$$a\mathbb{Z} \cap b\mathbb{Z} = ?$$

Soit $a, b \in \mathbb{Z}$

$$x \mid a \text{ et } x \mid b \text{ ssi } x \mid (a \wedge b)$$

$$a \mid y \text{ et } b \mid y \text{ ssi } m \mid (a \vee b)$$

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$$

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$$

Théorème de caractérisation des matrices inversibles

Énoncé du théorème de caractérisation des matrices inversibles.

Soit $A \in M_n(\mathbb{R})$, les assertions suivantes sont équivalentes :

- A est inversible.
- $A \stackrel{L}{\sim} I_n$.
- $\text{rg } A = n$.
- Le système homogène $AX = 0$ admet une seule solution.
- $\forall Y \in \mathbb{R}^n$ le système homogène $AX = Y$ admet au plus une solution.
- $\forall Y \in \mathbb{R}^n$ le système homogène $AX = Y$ admet au moins une solution.

Polynômes associés

Définition et propriétés des polynômes associés.

Soit $P, Q \in \mathbb{K}[X]$, P et Q sont dit associé si $P \mid Q$ et $Q \mid P$.

P, Q sont associés ssi $\exists \lambda \in \mathbb{K}^*, A = \lambda B$. Toute class de polynômes associés contient un unique polynôme unitaire (à l'exception de $\{0\}$).

Propriétés des racines d'un polynôme

Propriétés des racines d'un polynôme.

Soit $P \in \mathbb{K}[X]$, $n = \deg P$

En général

1. Si $P \neq 0$, P à au plus n racines (comptées avec multiplicités).
2. L'unique polynôme qui à une infinité de racines est $P = 0$.
3. Si $Q \in \mathbb{K}_n[X]$ et $\exists \alpha_1, \dots, \alpha_{n+1} \in \mathbb{K}$ tels que $\forall k \in \llbracket 1, n+1 \rrbracket, P(\alpha_k) = Q(\alpha_k)$, alors $P = Q$.

En caractéristique nulle

4. $a \in \mathbb{K}$ est racine de P avec multiplicité m ssi

$$\forall k \in \llbracket 0, m-1 \rrbracket, P^{(k)}(a) = 0$$

$$\text{et } P^{(m)}(a) \neq 0$$

Démonstration

1. Si $\alpha_1, \dots, \alpha_N \in \mathbb{K}$ sont des racines distinctes de P , et $m_1, \dots, m_N \in \mathbb{N}^*$ leurs multiplicités.

Pour tout $k \in \llbracket 1, N \rrbracket, (X - \alpha_k)^{m_k} \mid P$

Or pour $i < j \in \llbracket 1, n \rrbracket$

$$(X - \alpha_i) - (X - \alpha_j) = \alpha_j - \alpha_i$$

Relation de Bézout ($\alpha_j - \alpha_i$ associé à 1) donc premiers entre eux deux à deux.

D'où $\prod_{k=1}^N (X - \alpha_k)^{m_k} \mid P$ et $n \geq \sum_{k=1}^N m_k$.

2. Par la propriétés précédente, si P à une infinité de racine distincte il ne peut être de degré positif (ou il serait infini) donc il est nul.
4. Par Taylor-Langrange formel, pour tout $j \in \llbracket 1, m-1 \rrbracket$

$$P = \underbrace{\sum_{k=0}^{j-1} P^{(k)}(a) \frac{(X-a)^k}{k!}}_{R_j(X) \text{ (deg} < j \text{)}} + \underbrace{\sum_{k=j}^n P^{(k)}(a) \frac{(X-a)^k}{k!}}_{(X-a)^j Q(X)}$$

D'où R_j le reste de la division euclidienne de P par $(X-a)^j$. Or a est une racine de multiplicité m ssi

$$\begin{aligned} & \begin{cases} R_m = 0 \\ R_{m+1} \neq 0 \end{cases} \\ \Leftrightarrow & \begin{cases} \forall k \in \llbracket 0, m-1 \rrbracket, \frac{P^{(k)}(a)}{k!} = 0 \\ \exists k \in \llbracket 0, m \rrbracket, \frac{P^{(k)}(a)}{k!} \neq 0 \end{cases} \\ \Leftrightarrow & \begin{cases} \forall k \in \llbracket 0, m-1 \rrbracket, (P^{(k)}(a)) = 0 \\ P^{(m)}(a) \neq 0 \end{cases} \end{aligned}$$

Multiplicité d'une racine

Définition de multiplicité d'une racine.

Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ une racine et $n \in \mathbb{N}^*$. On dit que α est de multiplicité n si (l'un ou l'autre) :

- $(X - \alpha)^n \mid P$ mais $(X - \alpha)^{n+1} \nmid P$.
- $\forall k \in \llbracket 0, n - 1 \rrbracket, P^{(k)}(\alpha) = 0$

Polynômes scindés

Définition et propriétés des polynôme scindés.

Soit $P \in \mathbb{K}[X]$, $\alpha_1, \dots, \alpha_k$ ses racines et m_1, \dots, m_k leur multiplicités.

- P est scindé si $\deg P = \sum_{i=1}^k m_k$.
- P est scindé racines simples si P scindé et $\forall i \in \llbracket 1, k \rrbracket, m_i = 1$.

Propriétés :

- Si P est scindé racines simples sur \mathbb{R} , P' aussi.
- Si P est scindé sur \mathbb{R} , P' aussi.
- Tout polynôme P est scindé sur \mathbb{C} : théorème de Gauss-d'Alembert.

Polynômes irréductibles

Définition et propriétés des polynômes irréductibles.

Soit $P \in \mathbb{K}[X]$, P est dit irréductible si ses seuls diviseurs sont P , 1 et leurs associés.

1. Dans \mathbb{C} , les polynômes irréductibles sont les monômes (théorème de Gauss-d'Alembert).
2. Dans \mathbb{R} , les polynômes irréductibles sont les monômes et les polynômes de degré 2 avec $\Delta < 0$.
3. En général, un polynôme de degré 1 est toujours irréductible.
4. Dans $\mathbb{K}[X]$, un polynôme de degré 2 ou 3 est irréductible ssi il n'admet pas de racine dans \mathbb{K} .
5. Dans $\mathbb{K}[X]$, un polynôme de degré ≥ 2 ne peut être irréductible s'il admet une racine dans \mathbb{K} .
6. ($\text{car}(\mathbb{K}) = 0$) Un polynôme $P \in \mathbb{K}[X] \subset \mathbb{L}[X]$ irréductible (\mathbb{L} extension de corps de \mathbb{K}) n'admet que des racines simples dans \mathbb{L} (et à fortiori dans \mathbb{K}).

Démonstration

2. Par les propriétés 3 et 4, on sait que ces polynômes sont irréductibles, montrons que ce sont les seuls.

Soit $P \in \mathbb{R}[X]$ irréductible de degré ≥ 2 .

$P \in \mathbb{C}[X]$ donc on dispose de $\lambda \in \mathbb{C} \setminus \mathbb{R}$ racine de P .

$$P(\bar{\lambda}) = \overline{P(\lambda)} = \overline{0} = 0$$

D'où ($\text{car } (X - \lambda) \wedge (X - \bar{\lambda}) = 1$)

$$Q = \underbrace{X^2 - 2\text{Re}(\lambda)X + |\lambda|^2}_{\in \mathbb{R}[X]} \mid P$$

Comme P est irréductible, P et Q sont associés et $\deg P = 2$.

4. Soit $P \in \mathbb{K}_3[X] \setminus \mathbb{K}_1[X]$
 - S'il est irréductible il n'admet pas de racine.
 - S'il n'est pas irréductible,

$$P = QR$$

- Soit $\deg Q = 1$, $Q = X - \alpha$ et α racine de P .
- Soit $\deg R = 1$, $R = X - \beta$ et β racine de P .

6. $0 \leq \deg P' \leq \deg P - 1$ et par irréductibilité de P dans $\mathbb{K}[X]$

$$P \wedge P' = 1$$

Or le PGCD se conserve sur les extensions de corps, ils n'ont donc pas de racine communes (dans \mathbb{K} et \mathbb{L}).

Fonctions symétriques des racines

Définition des fonctions
symétriques des racines et
formules de Viète.

Soit $\alpha_1, \dots, \alpha_k \in \mathbb{C}$ et $k \in \llbracket 0, n \rrbracket$, la k -ème fonction symétrique des élémentaire de $\alpha_1, \dots, \alpha_n$ est

$$\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} \prod_{j=1}^k \alpha_{i_j}$$

On remarque que $\sigma_0 = 1$.

Soit $P = a_0 + a_1X + \dots + a_nX^n$ scindé, on note $\alpha_1, \dots, \alpha_n$ ses racines (non distinctes).

Formule de Viète :

$$\forall k \in \llbracket 0, n \rrbracket, \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

Polynômes de Tchebycheff

Définition et propriétés des polynômes de Tchebycheff.

Le n -ème polynôme de Tchebycheff est le polynôme tel que

$$\forall \theta \in \mathbb{R}, T_n(\cos \theta) = \cos(n\theta)$$

Propriétés :

1. Formule de récurrence :

$$T_{n+1} + T_{n-1} = 2XT_n$$

2. $\deg T_n = n$, coefficient dominant : 2^{n-1} , sauf pour $n = 0$, $T_0 = 1$.

3. T_n est scindé racines simples sur \mathbb{R} :

$$T_n(X) = 2^{n-1} \prod_{k=0}^{n-1} \left(X - \cos \frac{(2k+1)\pi}{2n} \right)$$

4. Orthogonalité : si $n \neq p$

$$\int_{-1}^1 T_n(x) T_p(x) \frac{dx}{\sqrt{1-x^2}} = 0$$

5. Minimalité en norme :

$$\|P\| = \max_{t \in [-1,1]} |P(t)|$$

Si P unitaire de degré n , alors $\|P\| \geq \frac{1}{2^{n-1}}$.

Avec cas d'égalité si $P(X) = \frac{T_n(X)}{2^{n-1}}$

Preuves :

1. Formules de trigonométrie :

$$\cos((n+1)\theta) + \cos((n-1)\theta) = 2 \cos \theta \cos(n\theta)$$

$$T_{n+1}(\cos \theta) + T_{n-1}(\cos \theta) = 2(\cos \theta) T_n(\cos \theta)$$

Donc ils coïncident en une infinité de valeurs $[-1, 1]$, et sont donc égaux.

2. Par récurrence avec la relation de récurrence.

3. On résout $\cos(n\theta) = 0$, on fait attention à distingué les racines.

4. Changement de variable $x = \cos \theta$, puis formules de trigonométrie.

5. Par contraposé : On prend P unitaire de degré n tel que

$$\|P\| \leq \frac{1}{2^{n-1}}.$$

• $P = \frac{1}{2^{n-1}} T_n + Q$, $\deg Q \leq n - 1$.

• On regarde les y_k quand $T_n(y_k) = \pm 1$.

• On en déduit le signe de Q

• Par le TVI Q à n racines donc $Q = 0$.

• Donc $P(X) = \frac{T_n(X)}{2^{n-1}}$.

Propriétés des fractions rationnelles

Propriétés des fractions rationnelles

- Si on dit que $\frac{P}{Q}$ est scindé, c'est que Q est scindé.
- Si F admet une infinité de racines alors $F = 0$.
- Si F et G coïncident en une infinité de points alors $F = G$.

Décomposition en éléments simples

Formules, propriétés de la décomposition en éléments simples.

Soit $F \in \mathbb{K}(X)$, F se décompose de façon unique sous la forme

$$F = E + G \text{ avec } E \in \mathbb{K}[X] \text{ et } \deg G < 0$$

On appelle E la partie entière de F et G la partie pôlaire.

- Si $F = \frac{P}{Q}$ scindé racines simples :
soit $\alpha_1, \dots, \alpha_n$ les pôles et
 $Q(X) = (X - \alpha_k)R_k(X)$ pour
tout $k \in \llbracket 1, n \rrbracket$:

$$F = E + \frac{\lambda_1}{X - \alpha_1} + \dots + \frac{\lambda_n}{X - \alpha_n}$$

Avec

$$\lambda_k = \frac{P(\alpha)}{R_k(\alpha)} = \frac{P(\alpha)}{Q'(\alpha)}$$

- Si F est scindé pôles multiples, on fait la même chose en retranchant les décompositions à chaque fois.

Décomposition en éléments simples de $\frac{P'}{P}$:

$$P(X) = \lambda(X - \alpha_1)^{m_1} \dots \dots (X - \alpha_k)^{m_k}$$

$$\frac{P'(X)}{P(X)} = \frac{m_1}{X - \alpha_1} + \dots + \frac{m_k}{X - \alpha_k}$$

Axiomes d'un espace vectoriel

Axiomes d'un espace vectoriel.

Sois \mathbb{K} un corps, E muni de la somme interne $+$ et du produit externe \cdot est un \mathbb{K} -ev si

1. $(E, +)$ est un groupe abélien.
2. $\forall x \in E, 1 \cdot x = x$.
3. $\forall \lambda \in \mathbb{K}, \forall x, y \in E, \lambda(x + y) = \lambda x + \lambda y$.
4. $\forall \lambda, \mu \in \mathbb{K}, \forall x \in E, (\lambda + \mu)x = \lambda x + \mu x$.
5. $\forall \lambda, \mu \in \mathbb{K}, \forall x \in E, \lambda(\mu x) = (\lambda\mu)x$

Théorème de caractérisation du rang

Énoncé du théorème de
caractérisation du rang.

Soit $A \in M_{np}(\mathbb{K})$, $r \in \mathbb{N}$, les
assertions suivantes sont
équivalentes

- A équivalente par ligne à une
matrice échelonné avec r
lignes non nulles.
- $\text{rg } \varphi_A = r$
- $\text{rg } (C_1, \dots, C_p) = r$ (avec C_i la i -
ème colonne de A)
- $\text{rg } (L_1, \dots, L_n) = r$ (avec L_i la i -
ème ligne de A)
- $A \stackrel{L,C}{\sim} J_r$

On dit alors que $\text{rg } A = r$.

On a aussi

$$A \stackrel{L,C}{\sim} B \text{ ssi } \text{rg } A = \text{rg } B$$

$$\begin{aligned} \text{rg}(\varphi \circ \psi) &= \text{rg } \psi - \dim(\ker \varphi \cap \text{im } \varphi) \\ &\leq \min(\text{rg } \varphi, \text{rg } \psi) \end{aligned}$$

Formes linéaires et hyperplans

Formes linéaires et hyperplans.

Soit E un \mathbb{K} -ev

Un hyperplan de E est un sev de codimension 1, c'est à dire qui admet un supplémentaire de dimension 1.

- Si $\alpha \in E^* \setminus \{0\}$, alors $\ker \alpha$ est un hyperplan.
- Si H est un hyperplan de E , il existe une forme linéaire α unique à constante multiplicative près tel que $H = \ker \alpha$.

Deux hyperplans on toujours un supplémentaire commun.

Démonstration

- Si H_1 et H_2 sont des hyperplans, $H_1 \cup H_2 \neq E$
 - Par l'absurde : supposons $H_1 \cup H_2 = E$ sev de E
Or $H_1 \cup H_2 = (H_1 \text{ ou } H_2) = E$ (cf unions de sev) qui est absurde.

Donc on dispose de $x_0 \in E \setminus (H_1 \cup H_2)$

Ainsi $\text{Vect}(x_0)$ est un supplémentaire de H_1 et H_2

Matrices semblables

Définition de matrices semblables.

Soit $A, B \in M_n(\mathbb{K})$, A est dite semblable à B si

$$\exists P \in \text{GL}_n(\mathbb{K}), \quad B = P^{-1}AP$$

Invariants :

- $\text{rg } A = \text{rg } B$
- $\text{tr } A = \text{tr } B$
- $\det A = \det B$
- $\chi_A = \chi_B$
- $\mu_A = \mu_B$

Fonctions arithmétiques : Möbius et indicatrice d'Euler

Définition, contexte et démonstration de la fonction de Möbius et la formule d'inversion.

Pour $A = \mathcal{F}(\mathbb{N}^*, \mathbb{C})$ on définit $(*)$, pour $f, g \in A$

$$f * g = \begin{cases} \mathbb{N}^* \rightarrow \mathbb{C} \\ n \mapsto \sum_{d|n} f(d)g\left(\frac{n}{d}\right) \end{cases}$$

Qui est une loi de composition interne sur A . On montre que

- $\mathbb{1}_{\{1\}}$ est l'élément neutre.
- $(*)$ est commutatif
- $(*)$ est associatif

On définit la fonction de Möbius, on note $\mu(n) = |\{p \in \mathbb{P}, p \mid n\}|$

$$\begin{aligned} 1 &\mapsto 1 \\ \mu : n \mid \nexists p \in \mathbb{P}, p^2 \mid n &\mapsto (-1)^{\pi(n)} \\ n \mid \exists p \in \mathbb{P}, p^2 \mid n &\mapsto 0 \end{aligned}$$

On montre de plus

$$\mu * \mathbb{1}_{\mathbb{N}} = \mathbb{1}_{\{1\}}$$

Pour $n \geq 2$ on écrit $n = \prod_{j=1}^k p_j^{\alpha_j}$.
Un diviseur d s'écrit $\prod_{j=1}^k p_j^{\beta_j}$ avec $\beta_j \leq \alpha_j$. Donc

$$\mu(d) \neq 0 \Leftrightarrow \forall j \in \llbracket 1, k \rrbracket, \beta_j \in \{0, 1\}$$

Ainsi

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{\beta_1, \dots, \beta_k \in \{0, 1\}} \mu\left(\prod_{j=1}^k p_j^{\beta_j}\right) \\ &= \sum_{q=0}^k \sum_{I \subset \llbracket 1, k \rrbracket} (-1)^{|I|} \\ &= \sum_{q=0}^k (-1)^q \binom{k}{q} \\ &= 0 \end{aligned}$$

On en déduit la formule

d'inversion de Möbius : soit $f :$

$\mathbb{N}^* \rightarrow \mathbb{C}$, on pose $g : n \mapsto$

$\sum_{n|d} f(d)$ ($g = f * \mathbb{1}_{\mathbb{N}}$), on a alors pour tout $n \in \mathbb{N}$

$$f(n) = \sum_{d|n} \mu(d)g\left(\frac{n}{d}\right)$$

C'est à dire $f = g * \mu = f * \underbrace{\mathbb{1}_{\mathbb{N}} * \mu}_{\mathbb{1}_{\{1\}}}$.

De plus μ est multiplicative.

Existence et unicité des sous groupes de groupe cyclique

Soit G un groupe cyclique d'ordre n , et $d \mid n$, montrer l'existence et l'unicité d'un sous groupe d'ordre d .

Soit G cyclique d'ordre n .

Par isomorphisme à $(\mathbb{Z}/n\mathbb{Z}, +)$, on se ramène à l'étude de (\mathbb{U}_n, \cdot) .

Soit H sous groupe de \mathbb{U}_n , $|H| = d$.

Pour tout $x \in H$, $x^d = 1$ donc $H \subset \mathbb{U}_d$, par égalité des cardinaux, $H = \mathbb{U}_d$.

Polynômes cyclotomiques

Définitions et propriétés des polynômes cyclotomiques.

Pour $n \in \mathbb{N}^*$ on note

$$\begin{aligned}\mathbb{V}_n &= \{z \in \mathbb{U}_n \mid \text{ord}(z) = n\} \\ &= \left\{e^{\frac{2ki\pi}{n}}, k \in (\mathbb{Z}/n\mathbb{Z})^\times\right\}\end{aligned}$$

On définit de n -ème polynôme cyclotomique

$$\Phi_n(X) = \prod_{\xi \in \mathbb{V}_n} (X - \xi)$$

$$\deg(\Phi_n) = \varphi(n)$$

On montre

$$X^n - 1 = \prod_{d \mid n} \Phi_d$$

$$\Phi_n \in \mathbb{Z}[X]$$

$$\Phi_p \text{ irréductible}$$

Démonstration

- Pour $d \mid n$, on a

$$\mathbb{V}_d = \{z \in \mathbb{U}_n \mid \text{ord}(n) = d\}$$

Car si $z \in \mathbb{U}_n$ d'ordre d , $z \in \langle z \rangle$ sous groupe de \mathbb{U}_n de cardinal d , qui est unique car \mathbb{U}_n est cyclique. D'où $z \in \mathbb{U}_d$ et à fortiori $z \in \mathbb{V}_d$.

- On a donc

$$\mathbb{U}_n = \bigsqcup_{d \mid n} \mathbb{V}_d$$

$$\begin{aligned}X^n - 1 &= \prod_{\xi \in \mathbb{U}_n} (X - \xi) \\ &= \prod_{d \mid n} \left(\prod_{\xi \in \mathbb{V}_d} (X - \xi) \right) \\ &= \prod_{d \mid n} \Phi_d\end{aligned}$$

- On montre que la division euclidienne dans $\mathbb{Z}[X]$ par un polynôme unitaire donnent un polynôme dans $\mathbb{Z}[X]$. On refait la démonstration de la division euclidienne (récurrence).
- Récurrence forte sur n pour montrer que $\Phi_n \in \mathbb{Z}[X]$

$$X^n - 1 = \Phi_n \cdot \left(\prod_{\substack{d \mid n \\ d \neq n}} \Phi_d \right)$$

- Soit $p \in \mathbb{P}$

$$\begin{aligned}\Phi_p &= \prod_{\substack{\omega \in \mathbb{U}_p \\ \text{ord}(\omega) = p}} (X - \omega) \\ &= \frac{X^p - 1}{X - 1} = \sum_{k=0}^{p-1} X^k\end{aligned}$$

Remarquons que

$$\tau : \begin{cases} \mathbb{Q}[X] & \rightarrow & \mathbb{Q}[X] \\ P(X) & \mapsto & P(X + 1) \end{cases}$$

est un automorphisme d'anneau.

D'où $\Phi_p(X)$ irréductible ssi $\Phi_p(X + 1)$ irréductible.

$$\begin{aligned}\Phi_p(X + 1) &= \frac{(X + 1)^p - 1}{X} \\ &= X^{p-1} + \sum_{k=1}^{p-1} \underbrace{\binom{k}{p}}_{\text{divisible par } p} X^{k-1}\end{aligned}$$

et le coefficient constant est $\binom{p}{1}$ qui n'est pas divisible par p^2 , d'où par le critère d'Eisenstein, Φ_p irréductible dans $\mathbb{Q}[X]$.

Démonstration de $n =$

$\sum_{d \mid n} \varphi(d) :$

$$\begin{aligned}n &= |\mathbb{U}_n| \\ &= \sum_{d \mid n} |\mathbb{V}_d| \\ &= \sum_{d \mid n} \varphi(d)\end{aligned}$$

Groupes quotientés

Définitions et propriétés des groupes quotientés.

Soit G un groupe, H sous-groupe.

On définit la relation d'équivalence

$$\forall (x, y) \in G^2, \quad x \sim y \text{ ssi } y \in xH$$

On obtient ainsi les classes à gauche gH pour tout $g \in G$, dont l'ensemble est noté G/H .

H est dit distingué si

$$\forall g \in G, \quad gHg^{-1} = H$$

Et dans ce cas G/H à une structure de groupe muni de la multiplication sur les classes

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

Et on pose

$$f : \begin{array}{ccc} G & \rightarrow & G/H \\ g & \mapsto & gH \end{array}$$

qui est un morphisme de groupe surjectif appelé projection canonique de G sur G/H dont le noyau est H .

Cas particuliers

- Tous noyau de morphisme est un sous groupe distingué.
- Tous sous-groupe d'indice 2 ($\frac{|G|}{|H|} = 2$) est distingué.

Idéaux maximaux, anneaux quotientés

Définitions d'idéal maximale, anneau quotienté, propriétés.

Soit $(A, +, \cdot)$ un anneau et I idéal de A .

Idéal maximale

Un idéal I de A est dit maximale si pour tout J idéal de A

$$I \subsetneq J \Rightarrow J = A$$

Anneau quotienté

On définit sur A la relation d'équivalence

$$\forall (x, y) \in A^2, x \sim y \text{ ssi } x - y \in I$$

On note A/I l'ensemble des classes d'équivalences par cette relation qu'on muni d'une structure de groupe en définissant les loi suivantes

$$\overline{x} + \overline{y} = \overline{x + y}$$

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

Qui ne dépend pas du représentant choisis.

Propriétés

- I est maximale ssi tous les éléments non nuls de A/I sont inversibles.
- Si A commutatif, I maximale, alors I est premier (A/I est intègre).

Démonstration :

- On suppose I maximale. Soit $x \in A \setminus I$ c'est à dire $x \notin \overline{0_A}$, montrons que \overline{x} est inversible.

$I \subseteq xA + I = J$ est un idéal, or I maximale d'où $1_A \in A = J$, d'où l'existence de $y \in A$ et $z \in I$ tel que

$$xy + z = 1_A$$

$$\overline{xy} = \overline{1_A}$$

- On suppose les éléments non nuls de I/A inversibles.

Soit $J \supsetneq I$ idéal de A , donc il existe $x \in J$ tel que $x \notin I$.

$\overline{x} \neq \overline{0}$ donc $\overline{x}^{-1} = \overline{y}$ existe.

$$\overline{xy} = \overline{xy} = \overline{1_A}$$

$$\exists z \in I, \underbrace{xy + z}_{\in J} = 1_A$$

$1_A \in J$ donc $J = A$, I est maximale.

- Soit $x, y \in A$ tels que $xy \in I$, supposons que $x \notin I$. Donc \overline{x} inversible : on dispose de $x' \in A$ et $z \in I$ tels que

$$xx' + z = 1_A$$

$$\underbrace{\overbrace{xy x'}^{\in I}}_{\in I} + zy = y \in I$$

Signature d'une permutation

Définitions et propriétés de la signature dans \mathfrak{S}_n .

Plusieurs définitions alternatives.

- $\varepsilon : (\mathfrak{S}_n, \circ) \rightarrow (\mathbb{Z}^\times, \cdot)$ est l'unique morphisme non triviale.

Pour $\sigma \in \mathfrak{S}_n$:

$$\begin{aligned}\varepsilon(\sigma) &= \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \\ &= (-1)^{N_\sigma} \\ &= (-1)^{n - |\text{Orb}(\sigma)|}\end{aligned}$$

Où $N_\sigma = |\{(i, j) \mid i < j \text{ et } \sigma(i) > \sigma(j)\}|$.

Actions de groupe

Définitions et exemples usuels, propriétés des actions de groupes.

Soit G un groupe, X un ensemble. Une action de groupe est la donnée d'un morphisme de groupe

$$\varphi : \begin{cases} G \rightarrow \mathfrak{S}(X) \\ g \mapsto \rho_g : \begin{cases} X \rightarrow X \\ x \mapsto \rho_g(x) = g.x \end{cases} \end{cases}$$

Ainsi tout groupe fini de cardinal $n \in \mathbb{N}$ est isomorphe à un sous groupe de \mathfrak{S}_n .

Démonstration

Grâce à l'action de groupe φ

$$\varphi : \begin{cases} G \rightarrow \mathfrak{S}(G) \simeq \mathfrak{S}_n \\ a \mapsto \rho : \begin{cases} G \rightarrow G \\ g \mapsto ag \end{cases} \end{cases}$$

Qui est un morphisme de groupe (car $\rho_a \circ \rho_b = \rho_{a,b}$), injectif (car $\ker \varphi = e_G$), d'où $\varphi|_{\varphi(G)}$ isomorphisme de $G \rightarrow \varphi(G)$, avec $\varphi(G)$ sous groupe de $\mathfrak{S}(G) \simeq \mathfrak{S}_n$.

Autre action classique

On peut aussi considérer l'action de conjugaison

$$\theta : \begin{cases} G \rightarrow \mathfrak{S}(G) \\ g \mapsto \rho_g : \begin{cases} G \rightarrow G \\ x \mapsto gxg^{-1} \end{cases} \end{cases}$$

On a

$$\begin{aligned} \ker \theta &= \{g \in G \mid \theta(g) = \text{id}\} \\ &= \{g \in G \mid \forall x \in G, gxg^{-1} = x\} \\ &= \{g \in G \mid \forall x \in G, gx = xg\} \\ &= Z(G) \end{aligned}$$

Formule des classes

Énoncé, démonstration et définitions de la formule des classes.

Soit G un groupe et φ une action de G sur un ensemble X . On définit pour tout $x \in X$

$$\text{Stab}(x) = \{g \in G \mid g.x = x\}$$

C'est un sous groupe de G :

- $e.x = x$ d'où $e \in \text{Stab}(x)$
- $\forall g \in \text{Stab}(x), g^{-1}.x = g^{-1}.g.x = x$
- $\forall g, h \in \text{Stab}(x), (gh).x = g.h.x = x$

On définit également

$$\text{Orb}(x) = \{g.x, g \in G\}$$

Qui est la classe d'équivalence de x pour la relation d'équivalence

$$x \sim y \text{ si } \exists g \in G, y = g.x$$

Donc les orbites forment une partition de X .

Formule des classes

Pour tout $x \in X$ fini et G fini

$$|\text{Orb}(x)| \cdot |\text{Stab}(x)| = |G|$$

Démonstration

Soit $x \in X$, pour $y \in \text{Orb}(x)$, on dispose de $g_0 \in G$ tel que $g_0.x = y$.

Étudions $\{g \in G \mid g.x = y\}$:

$$\begin{aligned} g.x = y &\Leftrightarrow g.x = g_0.x \\ &\Leftrightarrow (g_0^{-1}g).x = x \\ &\Leftrightarrow g_0^{-1}g \in \text{Stab}(x) \\ &\Leftrightarrow g \in g_0 \text{ Stab } (x) \end{aligned}$$

D'où

$$\begin{aligned} G &= \bigsqcup_{y \in \text{Orb}(x)} \{g \in G \mid g.x = y\} \\ |G| &= \sum_{y \in \text{Orb}(x)} |g_0 \text{ Stab } (x)| \\ &= \sum_{y \in \text{Orb}(x)} |\text{Stab } (x)| \\ &= |\text{Orb}(x)| \cdot |\text{Stab } (x)| \end{aligned}$$

Exercice : Les p -groupes

Définitions d'un p -groupe, et démonstration de

1. Pour G p -groupe, $|Z(G)| = p^\alpha$ avec $\alpha \in \mathbb{N}^*$.
2. Tout groupe G d'ordre p^2 est abélien

Un p -groupe est un groupe dont tout les éléments sont d'ordre p^γ avec $p \in \mathbb{P}$. A fortiori, il s'agit d'un groupe de cardinal p^α .

1. On étudie l'action de groupe

$$\varphi : \begin{cases} G \rightarrow \mathfrak{S}(G) \\ g \mapsto \rho_g : \begin{cases} G \rightarrow G \\ x \mapsto gxg^{-1} \end{cases} \end{cases}$$

On montre que

$$x \in Z(G) \text{ ssi } \text{Orb}(x) = \{e_G\}$$

Et par la formule des classes on a pour tout $x \in G$:

$$p^\alpha = |G| = |\text{Orb}(x)| \cdot |\text{Stab}(x)|$$

Donc $|\text{Orb}(x)| \mid p^\alpha$ d'où si $|\text{Orb}(x)| > 0, p \mid |\text{Orb}(x)|$.

Or les $\text{Orb}(x)$ forment une partition de G donc

$$\begin{aligned} p^\alpha = |G| &= \sum_{x \in G} |\text{Orb}(x)| \\ &= |Z(G)| + \underbrace{\sum_{\substack{x \in G/\sim \\ |\text{Orb}(x)| > 1}} |\text{Orb}(x)|}_{\text{divisible par } p} \end{aligned}$$

Donc $p \mid |Z(G)|$ mais $e_G \in Z(G)$ donc $|Z(G)| > 0$ d'où $|Z(G)| \geq p$.

2. Par l'exercice ci dessus

$$Z(G) \in \{p, p^2\}$$

Supposons qu'il existe $x \in G \setminus Z(G)$, alors

$$Z(G) \subset \text{Stab}(x) \text{ et } x \in \text{Stab}(x)$$

Donc $|\text{Stab}(x)| \geq p + 1$ sous-groupe de G donc

$$\text{Stab}(x) = G$$

D'où $x \in Z(G)$, absurde.

Exercice : élément d'ordre p dans un groupe d'ordre divisé par p

Soit G un groupe d'ordre pq avec $p \in \mathbb{P}$ et $q \in \mathbb{N}^*$, démonstration de l'existence d'un élément d'ordre p .

Soit G d'ordre $n = pq$ avec $(p, q) \in \mathbb{P} \times \mathbb{N}^*$.

On pose

$$\Gamma = \{(x_1, \dots, x_p) \in G^p \mid x_1 \cdots x_p = e_G\}$$

$$\sigma = (1 \ 2 \ \dots \ p) \in \mathfrak{S}_p$$

On considère $H = \langle \sigma \rangle$ qui agit sur Γ via

$$\varphi : \begin{cases} H & \rightarrow \mathfrak{S}(\Gamma) \\ \sigma^k & \mapsto \rho_{\sigma^k} \end{cases}$$

Où

$$\rho_{\sigma^k} : \begin{cases} \Gamma & \rightarrow \Gamma \\ (x_1, \dots, x_p) & \mapsto (x_{\sigma^k(1)}, \dots, x_{\sigma^k(p)}) \end{cases}$$

(On montre par récurrence sur k que ρ_{σ^k} à bien valeur dans Γ).

On remarque que $|H| = p$ et

$$\forall X = (x_1, \dots, x_p) \in G^p,$$

$$X \in \Gamma \Leftrightarrow x_p^{-1} = x_1 \cdots x_{p-1}$$

$$\Gamma \simeq G^{p-1} \text{ donc } |\Gamma| = n^{p-1}$$

Pour tout $x \in \Gamma$ (par la formule des classes)

$$p = |H| = |\text{Orb}(x)| \cdot |\text{Stab}(x)|$$

$$\text{donc } |\text{Orb}(x)| \in \{1, p\}$$

$$\text{Orb}(x) = \{x\} \Leftrightarrow x_1 = x_2 = \dots = x_p$$

$$\Leftrightarrow x_1^p = e_G$$

Et

$$n^{p-1} = |\Gamma| = \sum_{x \in \Gamma/\sim} |\text{Orb}(x)|$$

$$= \sum_{\substack{x \in \Gamma/\sim \\ |\text{Orb}(x)|=1}} 1 + \sum_{\substack{x \in \Gamma/\sim \\ |\text{Orb}(x)|>1}} p$$

$$= |\{x \in G \mid x^p = e_G\}| + kp$$

Avec $k \in \mathbb{N}$. Or $p \mid n$ donc

$$p \mid |\{x \in G \mid x^p = e_G\}| \geq 1$$

Donc il existe au moins $p - 1$ éléments d'ordre p .

Cas $n = 2$:

On regroupe les éléments avec leurs inverse, ce qui montre par la parité du cardinale l'existence d'un élément d'ordre 2.

Théorème de Burnside

Énoncer et démonstration du théorème de Burnside.

Soit G un groupe fini qui agit sur un ensemble X fini par φ .

On définit pour $g \in G$

$$\text{Fix}(g) = \{x \in X, g.x = x\}$$

Notons N le nombre d'orbites :

$$N = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

Démonstration

On étudie

$$\begin{aligned} \Gamma &= \{(g, x) \in G \times X \mid g.x = x\} \\ &= \bigsqcup_{x \in X} \{(g, x), g \in \text{Stab}(x)\} \\ &= \bigsqcup_{g \in G} \{(g, x), x \in \text{Fix}(g)\} \end{aligned}$$

Or par la formule des classes

$$|\text{Stab}(x)| = \frac{|G|}{|\text{Orb}(x)|}$$

D'où (en notant x_i représentant du i -ème orbite)

$$\begin{aligned} |\Gamma| &= \sum_{x \in X} |\text{Stab}(x)| \\ &= \sum_{j=1}^N \sum_{x \in \overline{x_j}} |\text{Stab}(x)| \\ &= \sum_{j=1}^N \sum_{x \in \overline{x_j}} \frac{|G|}{|\text{Orb}(x_j)|} \\ &= N |G| \end{aligned}$$

Or

$$|\Gamma| = \sum_{g \in G} |\text{Fix}(g)|$$

D'où

$$N = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

Exercice : Groupe d'éléments d'ordre inférieur à deux

Propriétés du groupe G tel que
 $\forall x \in G, x^2 = 1$

On a immédiatement

$$\forall x \in G, x = x^{-1}$$

- G est abélien, soit $x, y \in G$:

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

- Si G fini, $G \simeq (\mathbb{Z}/2\mathbb{Z})^n$ et $|G| = 2^n$ pour un $n \in \mathbb{N}$.

Passons en notation additive
pour plus de clarté :

Faisons de G un \mathbb{F}_2 -ev :

$$\begin{aligned} \mathbb{F}_2 \times G &\rightarrow G \\ (\bar{k}, g) &\mapsto kg \end{aligned}$$

Qui ne dépend pas du
représentant car $2G = \{0\}$.

G un \mathbb{F}_2 -ev de dimension finie,
donc isomorphe à \mathbb{F}_2^n en tant
qu'espace vectoriel, et à fortiori
en tant que groupe.

Irréductibles d'un anneau

Définition, propriétés élémentaires sur les irréductibles dans un anneau principal.

Soit $(A, +, \cdot)$ un anneau principal.

- Dans un anneau principal on a un PGCD

Pour tout $a, b \in A$, il existe $d \in A$ tel que $aA + bA = dA$, unique (à associés près), qu'on appelle PGCD de a et b ($a \wedge b = d$).

On a aussi Bézout car $d \in dA = aA + bA$ d'où $\exists(u, v) \in A^2, d = au + bv$.

- Un élément de A est dit irréductible si ses seuls diviseurs sont ses associés et les inversibles.
- Pour tout $a \in A$, il existe une unique (à permutation et multiplication par des inversibles près) décomposition de a en irréductibles.

Démonstration de la décomposition

- Toute suite croissante d'idéaux est stationnaire.

$(I_i)_{i \in \mathbb{N}}$ suite d'idéaux de A croissante au sens de l'inclusion.

$$K = \bigcup_{i \in \mathbb{N}} I_i$$

Est encore un idéal car union croissante d'idéaux

Par principalité de A , $K = zA$ avec $z \in K$ donc on dispose de $k \in \mathbb{N}$ tel que $z \in I_k$ d'où

$$K = zA \subseteq I_k \subseteq K$$

- Tout élément de A admet au moins un diviseur irréductible dans A .

Soit $x \in A$, on construit la suite (x_n) par récurrence : $x_0 = x$ et pour $n \in \mathbb{N}$

- ▶ Si x_n irréductible, $x_{n+1} = x_n$
- ▶ Sinon on prend x_{n+1} diviseur de x_n non associés et non inversible.

Par définition de la divisibilité, $(x_n A)_n$ est une suite croissante d'idéaux, et est donc stationnaire.

Soit k le rang à partir du quel c'est le cas, x_k est donc un diviseur irréductible de x .

- Existence de la décomposition : récurrence avec la propriété ci dessus.
- Unicité de la décomposition : on prend deux décomposition on montre que chaque irréductible est présent à la même puissance dans les deux.

Polynômes en caractéristique strictement positive

Remarques et mises en gardes à propos de $\mathbb{K}[X]$ quand $\text{car}(\mathbb{K}) > 0$

Soit \mathbb{K} un corps tel que $\text{car}(\mathbb{K}) > 0$

- Le morphisme d'évaluation $\theta : \mathbb{K}[X] \rightarrow \mathcal{F}(\mathbb{K}, \mathbb{K})$ n'est pas forcément injectif.

Dans \mathbb{F}_p , $\theta(X^p - X) = \theta(0) = 0_{\mathcal{F}(\mathbb{F}_p, \mathbb{F}_p)}$ or $X^p - 1 \neq 0$.

- Il n'y a pas équivalence entre multiplicité d'une racine et les valeurs des dérivées successives.

Pour $\text{car}(\mathbb{K}) = p \in \mathbb{P}$

Pour $k \in \llbracket 1, p-1 \rrbracket$

$$\binom{k}{p} = \frac{\overbrace{p(p-1) \cdots (p-k+1)}^{p \text{ divise}}}{\underbrace{k!}_{p \text{ ne divise pas}}}$$

D'où $\binom{k}{p}$ nul dans \mathbb{K} .

Ainsi pour tout $a, b \in \mathbb{K}$

$$\begin{aligned} (a+b)^p &= a^p + b^p + \sum_{k=1}^{p-1} \binom{k}{p} a^k b^{p-k} \\ &= a^p + b^p \end{aligned}$$

Et on peut définir le morphisme de corps de Frobenius

$$\sigma : \begin{cases} \mathbb{K} \rightarrow \mathbb{K} \\ x \mapsto x^p \end{cases}$$

Donc dans $\mathbb{F}_p[X]$

$$Q = (X-1)^p = X^p - 1$$

1 est racine de multiplicité p de Q or $Q' = 0$ d'où pour tout $k \in \mathbb{N}$, $Q^{(k)}(1) = 0$.

Théorème de Wilson

Énoncer et démonstration du théorème de Wilson.

Pour tout $p \in \mathbb{N}^*$, p est premier ssi $(p-1)! \equiv -1[p]$.

Démonstration

- Soit $n \in \mathbb{N}^*$ non premier.
 - Si $3 \leq n = m^2$ avec $m \in \mathbb{N}^*$.
 $2m \cdot m \mid (n-1)!$ d'où $(n-1)! \equiv 0[n]$
 - Sinon on dispose de $1 \leq p, q < n$ tels que $n = pq$ d'où $n = pq \mid (n-1)!$ et $(n-1)! \equiv 0[n]$.
- Soit $p \in \mathbb{P}$, étudions $(p-1)!$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$

Soit $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $x^2 = 1$

$$(x+1)(x-1) = 0$$

Donc $x = \{1, -1\}$.

On peut donc regrouper les éléments du produit $(p-1)!$ avec leurs inverses (qui sont dans le produit), à l'exception de 1 et -1 d'où

$$\begin{aligned}(p-1)! &= (p-1)(p-2) \cdots 1 \\ &= -1 \cdot 1 = 1\end{aligned}$$

Dans $\mathbb{Z}/p\mathbb{Z}$.

Autre démonstration horrible pour le deuxième sens

Soit $p \in \mathbb{P}$, on étudie $R = X^p - X$ dans $\mathbb{F}_p[X]$.

Pour tout $x \in \mathbb{F}_p$, $R(x) = 0$ donc $(X-x) \mid R$ et premiers entre eux deux x à deux d'où

$$\prod_{x \in \mathbb{F}_p} (X-x) \mid R$$

Et par égalité des degrés on a égalité des polynômes.

Considérons maintenant le morphisme d'anneau suivant :

$$\pi : \begin{cases} \mathbb{Z}[X] & \rightarrow \mathbb{F}_p[X] \\ \sum_{k=0}^n a_k X^k & \mapsto \sum_{k=0}^n \overline{a_k} X^k \end{cases}$$

$$Q = \prod_{k=0}^{p-1} (X-k) = X^p + \sum_{k=0}^{p-1} a_k X^k$$

$$\pi(Q) = \prod_{k=0}^{p-1} (X - \overline{k}) = R$$

$$\begin{aligned}a_1 &= (-1)^{p-1} \sum_{\substack{I \subset \llbracket 0, p-1 \rrbracket \\ |I|=p-1}} \prod_{i \in I} i \\ &= (p-1)!\end{aligned}$$

$$\overline{a_1} = \overline{(p-1)!} = -1$$

Formule de Taylor-Langrange formelle

Formule de Taylor-Langrange formelle sur $\mathbb{K}[X]$, démonstration.

Soit \mathbb{K} un corps tel que $\text{car}(\mathbb{K}) = 0$, $P \in \mathbb{K}[X]$, $N \geq \deg P$ et $a \in \mathbb{K}$.

$$P = \sum_{k=0}^N P^{(k)}(a) \frac{(X-a)^k}{k!}$$

Démonstration

Notons $E = \mathbb{K}_N[X]$ qui est un \mathbb{K} -ev de dimension $N+1$.

La famille $((X-a)^k)_{k \in \llbracket 0, N \rrbracket}$ est libre car échelonné en degré, c'est donc une base de E , et comme $P \in E$, et comme $P \in E$

$$P = \sum_{k=0}^N \lambda_k (X-a)^k$$

Pour $j \in \llbracket 0, N \rrbracket$

$$\begin{aligned} P^{(j)}(a) &= \sum_{k=j}^N \frac{\lambda_k k!}{(k-j)!} (a-a)^{k-j} \\ &= \lambda_j j! \\ \lambda_j &= \frac{P^{(j)}(a)}{j!} \end{aligned}$$

Contenus d'un polynôme à coefficients entiers

Définitions, propriétés, et démonstrations à propos du contenu dans $\mathbb{Z}[X]$.

Soit $P = \sum_{k=0}^d a_k X^k \in \mathbb{Z}[X]$, on définit le contenu de P comme

$$c(P) = \bigwedge_{k=0}^d a_k$$

Et on dit qu'un polynôme P est primitif si $c(P) = 1$.

- Soient $P, Q \in \mathbb{Z}[X]$ tels que $c(P) = c(Q) = 1$, alors $c(PQ) = 1$.A
- Pour tout $P, Q \in \mathbb{Z}[X]$, $c(PQ) = c(P)c(Q)$.

Démonstration

- Soit $p \in \mathbb{P}$, posons le morphisme d'anneau

$$\pi : \begin{cases} \mathbb{Z}[X] & \rightarrow \mathbb{F}_p[X] \\ \sum_{k=0}^d a_k X^k & \mapsto \sum_{k=0}^d \overline{a_k} X^k \end{cases}$$

$c(P) = 1$ donc P admet au moins un coefficient non divisible par p et de même pour Q .

$$\begin{aligned} \pi(P) &\neq 0 \text{ et } \pi(Q) \neq 0 \\ \pi(PQ) &= \pi(P)\pi(Q) \neq 0 \end{aligned}$$

Donc p ne divise pas tous les coefficients de PQ pour tout $p \in \mathbb{P}$, d'où $c(PQ) = 1$.

- On remarque que pour $P \in \mathbb{Z}[X]$ et $k \in \mathbb{Z}$, $c(kP) = kc(P)$ et on étudie $\tilde{P} = \frac{P}{c(P)}$ et $\tilde{Q} = \frac{Q}{c(Q)}$.

Exercice : Produit de polynômes de rationnels unitaire entier

Soient $P, Q \in \mathbb{Q}[X]$ unitaires, montrer que si $PQ \in \mathbb{Z}[X]$ alors $P, Q \in \mathbb{Z}[X]$.

$P, Q \in \mathbb{Q}[X]$ unitaires, $PQ \in \mathbb{Z}[X]$.

Comme PQ unitaire $c(PQ) = 1$.

On trouve $a, b \in \mathbb{Z}$ tels que $aP, bQ \in \mathbb{Z}[X]$.

$$c(aP)c(bQ) = abc(PQ) = ab$$

Or P et Q étant unitaires

$$\begin{cases} c(aP) \mid a \\ c(bQ) \mid b \end{cases} \text{ donc } \begin{cases} a = k_a c(aP) \\ b = k_b c(bQ) \end{cases}$$

$$c(aP)c(bQ) = ab = k_a k_b c(aP)c(bQ)$$

$$\text{d'où } k_a = k_b = 1 \text{ et } \begin{cases} a = c(aP) \\ b = c(bQ) \end{cases}$$

Ainsi

$$\begin{cases} P = a \frac{P}{a} \in \mathbb{Z}[X] \\ Q = b \frac{Q}{b} \in \mathbb{Z}[X] \end{cases}$$

Exercice : Irréductibilité dans les rationnels

Soit $P \in \mathbb{Z}[X]$ dont les seuls diviseurs dans $\mathbb{Z}[X]$ sont de degré 0 ou $\deg P$, montrer que P est irréductible dans $\mathbb{Q}[X]$.

On suppose par contraposé que P n'est pas irréductible dans \mathbb{Q} .

$$P = QR$$

$$1 \leq \deg Q, \deg R \leq \deg P - 1$$

On introduit $a, b \in \mathbb{Z}$ tels que $aQ, bR \in \mathbb{Z}[X]$.

$$\begin{aligned} abc(P) &= c(aQbR) \\ &= c(aQ)c(bR) \end{aligned}$$

$$\begin{aligned} P &= \frac{aQbR}{ab} \\ &= \frac{(aQ)(bR)}{\frac{c(aQ)c(bR)}{c(P)}} \\ &= c(P) \cdot \underbrace{\frac{aQ}{c(aQ)}}_{Q_0} \cdot \underbrace{\frac{bR}{c(bR)}}_{R_0} \in \mathbb{Z}[X] \end{aligned}$$

Avec Q_0 et R_0 diviseurs de P dans $\mathbb{Z}[X]$ de degrés compris dans $\llbracket 1, \deg P - 1 \rrbracket$.

Entiers algébriques

Définition d'entier algébrique.

Soit $\alpha \in \mathbb{C}$, on dit que α est un entier algébrique s'il existe $Q \in \mathbb{Z}[X]$ unitaire tel que $Q(\alpha) = 0$.

1. α est donc aussi algébrique dans \mathbb{Q} , et son polynôme minimal est aussi dans $\mathbb{Z}[X]$.

Entiers algébrique de degré 2

2. $\alpha \in \mathbb{C}$ entier algébrique de degré 2 : on dispose de $\pi_\alpha \in \mathbb{Z}[X]$ unitaire de degré 2 qui annule α . $\mathbb{Z}[\alpha] = \text{im } \theta_\alpha$ est un sous-anneau de \mathbb{R} (et donc de \mathbb{C}).
3. $\mathbb{Z}[\alpha] = \{x + \alpha y, (x, y) \in \mathbb{Z}^2\}$ et tout élément s'écrit de manière unique sous cette forme.

4. On peut écrire

$$\pi_\alpha = (X - \alpha)(X - \beta)$$

On remarque que $\beta \in \mathbb{Z}[\alpha]$ car $\alpha + \beta = a \in \mathbb{Z}$ d'où $\beta = a - \alpha \in \mathbb{Z}[\alpha]$.

On définit

$$\tau : \begin{cases} \mathbb{Z}[\alpha] & \rightarrow \mathbb{Z}[\alpha] \\ x + \alpha y & \mapsto x + \beta y \end{cases}$$

On a alors

$$\forall z, z' \in \mathbb{Z}[\alpha], \tau(zz') = \tau(z)\tau(z')$$

5. Et on peut alors définir

$$N : \begin{cases} \mathbb{Z}[\alpha] & \rightarrow \mathbb{Z} \\ z = x + \alpha y & \mapsto z\tau(z) \end{cases}$$

Qui est aussi multiplicatif.

6. $z \in \mathbb{Z}[\alpha]$ est inversible ssi $N(z) = \pm 1$.

Démonstration

1. Notons P_α ce polynôme, comme $Q(\alpha) = 0$, $P_\alpha \mid Q$ dans $\mathbb{Q}[X]$, d'où

$$\mathbb{Z}[X] \ni Q = P_\alpha R \in \mathbb{Q}[X]$$

Et donc $P_\alpha, R \in \mathbb{Z}[X]$ car Q unitaire (cf. exercices sur le contenu).

3. α de degré 2 donc

$$\pi_\alpha(X) = X^2 + aX + b$$

- On a déjà $\{x + \alpha y, (x, y) \in \mathbb{Z}^2\} \subseteq \mathbb{Z}[\alpha]$.
- Soit $x = P(\alpha) \in \mathbb{Z}[\alpha]$, $P = Q\pi_\alpha + R$ avec $Q \in \mathbb{K}[X]$, $R \in \mathbb{K}_1[X]$.

Donc

$$\begin{aligned} R &= yX + x \in \mathbb{Z}[X] \\ P(\alpha) &= \underbrace{Q(\alpha)\pi_{\alpha(\alpha)}}_0 + y\alpha + x \end{aligned}$$

- Soit $x_1 + \alpha y_1 = x_2 + \alpha y_2$ avec $x_1, x_2, y_1, y_2 \in \mathbb{Z}$.

$$x_1 - x_2 = (y_2 - y_1)\alpha$$

Par l'absurde, si $y_1 \neq y_2$:

$$\alpha = \frac{x_1 - x_2}{y_2 - y_1} \in \mathbb{Q}[X]$$

Qui est absurde car π_α serait de degré 1.

4. Soit $z = x + \alpha y, z' = x' + \alpha y'$

On a $\alpha^2 = a\alpha - b$ et $\beta^2 = a\beta - b$ donc

$$\begin{aligned} \tau(zz') &= \tau(xx' + \alpha(xy' + x'y) + \alpha^2 yy') \\ &= \tau(xx' - byy' + \alpha(xy' + xy' + ayy')) \\ &= xx' - byy' + \beta(xy' + x'y + ayy') \\ &= (x + \beta y)(x' + \beta y) \\ &= \tau(z)\tau(z') \end{aligned}$$

5. Soit $z = x + \alpha y \in \mathbb{Z}[\alpha]$

$$\begin{aligned} N(z) &= z\tau(z) = (x + \alpha y)(x + \beta y) \\ &= x^2 + (\alpha + \beta)xy + \alpha\beta y^2 \\ &= x^2 = axy + by^2 \in \mathbb{Z} \end{aligned}$$

6. • Soit $z \in \mathbb{Z}[\alpha]$ inversible, on dispose de $z' \in \mathbb{Z}[\alpha]$ tel que $zz' = 1$.

$$N(zz') = N(1) = 1 = N(z)N(z')$$

Donc $|N(z)| = 1$

- Soit $z \in \mathbb{Z}[\alpha]$ tel que $N(z) = \varepsilon \in \{1, -1\}$

$$(x + \alpha y)(x + \beta y) = \varepsilon$$

$$z(\varepsilon x + \varepsilon \beta y) = 1 = \varepsilon^2$$

$$z^{-1} = \varepsilon(x + \beta y)$$

Exercice : Polynômes à coefficients entiers

1. Soit $P = \sum_{k=0}^d a_k X^k \in \mathbb{Z}[X]$, montrer que si P admet une racine rationnelle $\frac{p}{q}$ avec $p \wedge q = 1$, alors $q \mid a_d$ et $p \mid a_0$.

1.

$$\begin{aligned}
 0 &= P\left(\frac{p}{q}\right) = \sum_{k=0}^d a_k p^k q^{d-k} \\
 &\quad - \underbrace{\sum_{k=0}^{d-1} a_k p^k q^{d-k}}_{\text{divisible par } q} = a_d p^d \\
 &\quad - \underbrace{\sum_{k=1}^d a_k p^k q^{d-k}}_{\text{divisible par } p} = a_0 q^d
 \end{aligned}$$

D'où $\begin{cases} q \mid a_d p^d \\ p \mid a_0 q^d \end{cases}$ or $q \wedge p = 1$ donc par le théorème de Gauss,
 $\begin{cases} q \mid a_d \\ p \mid a_0 \end{cases}$.

On en déduit que si $P \in \mathbb{Z}[X]$ est unitaire et admet une racine rationnelle, alors elle est entière.

Critère d'Eisenstein

Énoncé et démonstration du critère d'Eisenstein.

Soit $P = \sum_{k=0}^d a_k X^k \in \mathbb{Z}[X]$ tel qu'il existe $p \in \mathbb{P}$ et

$$\begin{cases} \forall k \in \llbracket 0, d-1 \rrbracket, p \mid a_k \\ p \nmid a_d \\ p^2 \nmid a_0 \end{cases}$$

Alors P n'a pas de diviseurs dans $\mathbb{Z}[X]$ de degré compris dans $\llbracket 1, d-1 \rrbracket$, et est donc irréductible dans $\mathbb{Q}[X]$ (cf. exercices sur le contenu).

Démonstration

On considère le morphisme d'anneau suivant

$$\pi : \begin{cases} \mathbb{Z}[X] & \rightarrow \mathbb{F}_p[X] \\ \sum_{k=0}^d a_k X^k & \mapsto \sum_{k=0}^d \overline{a_k} X^k \end{cases}$$

Supposons par l'absurde que $P = QR$ avec $Q, R \in \mathbb{Z}[X]$

$$\overline{0} \neq \overline{a_d} X^d = \pi(P) = \pi(Q)\pi(R)$$

Par unicité de la décomposition en irréductibles dans $\mathbb{F}_p[X]$

$$\pi(Q) = \alpha X^k \quad \pi(R) = \beta X^l$$

$$k + l = d \quad \deg Q \geq k \quad \deg R \geq l$$

Or $\deg Q + \deg R = d$ d'où

$$Q = \sum_{i=0}^k b_i X^i \text{ avec } \begin{cases} \overline{b_k} = \alpha \neq 0 \\ \overline{b_0} = 0 \end{cases}$$

$$R = \sum_{i=0}^l c_i X^i \text{ avec } \begin{cases} \overline{c_l} = \beta \neq 0 \\ \overline{c_0} = 0 \end{cases}$$

D'où $a_0 = b_0 c_0$ est divisible par p^2 , absurde.

Exercice : rationalité d'une racine de haute multiplicité

Soit $P \in \mathbb{Q}[X]$ de degré n et α racine de P de multiplicité $m_\alpha > \frac{n}{2}$, montrer que $\alpha \in \mathbb{Q}$.

Soit $P \in \mathbb{Q}[X]$ de degré n et α racine de P de multiplicité $m_\alpha > \frac{n}{2}$.

$$P = \prod_{k=0}^N Q_k^{p_k}$$

Décomposition en irréductibles de P dans $\mathbb{Q}[X]$. Pour tout $i \neq j$, $P_i \wedge P_j = 1$ dans $\mathbb{Q}[X]$ et donc dans $\mathbb{C}[X]$.

Ainsi α n'est racine que d'un des P_i , notons $P_1(\alpha) = 0$.

C'est une racine simple car P_1 irréductible, d'où

$$p_1 \geq m_\alpha > \frac{n}{2}$$

$$2p_1 > n \geq p_1 \deg(P_1)$$

$$2 > \deg(P_1) = 1$$

Donc $P_1 = \lambda(X - \alpha) \in \mathbb{Q}[X]$ d'où $\alpha \in \mathbb{Q}$.

Algèbres

Définition d'une \mathbb{K} -Algèbre avec \mathbb{K} un corps.

Une \mathbb{K} -Algèbre est un ensemble A muni de deux lois de composition internes $(+)$, (\times) et d'une loi de composition externe (\cdot) tel que

- $(A, +, \times)$ est un anneau
- $(A, +, \cdot)$ est un \mathbb{K} -ev
- $\forall (\alpha, x, y) \in \mathbb{K} \times A^2$

$$\alpha(x \times y) = (\alpha x) \times y = x \times (\alpha y)$$

Exemples

- \mathbb{K} est une \mathbb{K} -Algèbre
- $(\mathbb{K}[X], +, \times, \cdot)$ est une \mathbb{K} -Algèbre
- Pour E un \mathbb{K} -ev, $(\mathcal{L}(E), +, \circ, \cdot)$ est une \mathbb{K} -Algèbre.

Exercice : existence d'un élément d'ordre du ppcm de deux autres

1. Soit G un groupe abélien fini, montrer que pour tout $x, y \in G$, il existe un élément $z \in G$ tel que $\text{ord}(z) = \text{ord}(x) \vee \text{ord}(y)$.
2. En déduire que

$$\max_{g \in G} \text{ord}(g) = \bigvee_{g \in G} \text{ord}(g)$$

1. Soit G un groupe abélien, $x, y \in G$ qui admettent un ordre.

$$\begin{aligned} \text{ord}(x) &= \prod_{i=1}^N p_i^{\alpha_i} \\ \text{ord}(y) &= \prod_{i=1}^N p_i^{\beta_i} \end{aligned}$$

Pour tout $k \in \llbracket 1, N \rrbracket$

$$\begin{aligned} \text{ord}\left(x^{\prod_{i \neq k} p_i^{\alpha_i}}\right) &= p_k^{\alpha_k} \\ \text{ord}\left(y^{\prod_{i \neq k} p_i^{\beta_i}}\right) &= p_k^{\beta_k} \end{aligned}$$

On pose alors

$$z_k = \begin{cases} x^{\prod_{i \neq k} p_i^{\alpha_i}} & \text{si } \alpha_k \geq \beta_k \\ y^{\prod_{i \neq k} p_i^{\beta_i}} & \text{sinon} \end{cases}$$

D'où $\text{ord}(z_k) = p_k^{\max(\alpha_k, \beta_k)}$

Ainsi en posant $z = \prod_{k=1}^N z_k$:

$$\begin{aligned} \text{ord}(z) &= \prod_{k=1}^N p_k^{\max(\alpha_k, \beta_k)} \\ &= \text{ord}(x) \vee \text{ord}(y) \end{aligned}$$

(Car G est abélien).

2. Par récurrence (car G fini) on dispose de $h \in G$ tel que

$$\text{ord}(h) = \bigvee_{g \in G} \text{ord}(g) = m$$

Posons $g_0 \in G$ d'ordre $\max_{g \in G} \text{ord}(g)$.

On a donc

$$\begin{aligned} m &\leq \text{ord}(g_0) \mid m \\ m &= \text{ord}(g_0) \end{aligned}$$

Exercice : Cyclicité des sous-groupes finis des inversibles d'un corps

Soit \mathbb{K} un corps, et $G \leq \mathbb{K}^\times$ fini.
Montrer que G est cyclique.

Première méthode

On utilise la propriété suivante (à redémontrer) : si G abélien fini

$$\max_{g \in G} \text{ord}(g) = \bigvee_{g \in G} \text{ord}(g)$$

Or pour tout $g \in G$, $g^m = 1$ d'où

$$G \subset \{\text{racines de } X^m - 1 \text{ dans } \mathbb{K}[X]\}$$

D'où $|G| \leq m$ car \mathbb{K} est un corps
et ainsi l'élément d'ordre
maximale est d'ordre supérieure
ou égal au cardinal de G , d'où G
cyclique.

Deuxième méthode

Pour $d \mid n = |G|$ on pose

$$\Gamma_d = \{g \in G \mid \text{ord}(g) = d\}$$

$$G = \bigsqcup_{d \mid n} \Gamma_d$$

$$n = \sum_{d \mid n} |\Gamma_d|$$

On pose aussi

$$\begin{aligned} A_d &= \{g \in G \mid g^d = 1\} \\ &= \{\text{racines de } X^d - 1\} \cap G \end{aligned}$$

$$|A_d| \leq d$$

Pour $d \mid n$ on a

- $\Gamma_d = \emptyset$ et $|\Gamma_d| = 0$
- Ou il existe $x \in \Gamma_d$, d'où $\langle x \rangle \subset A_d$ et $d \leq |A_d| \leq d$.

Ainsi

$$\begin{aligned} \Gamma_d &= \{g \in A_d = \langle x \rangle \mid \text{ord}(g) = d\} \\ |\Gamma_d| &= \varphi(d) \end{aligned}$$

Finalement

$$\sum_{d \mid n} \varphi(d) = n = \sum_{d \mid n} \underbrace{|\Gamma_d|}_{\in \{0, \varphi(d)\}}$$

D'où nécessairement $|\Gamma_d| = \varphi(d)$
pour tout $d \mid n$, en particulier
pour $|\Gamma_n| = \varphi(n) > 0$: il existe $\varphi(n)$
éléments d'ordre n .

Exercice : Les carrés de \mathbb{F}_p

Notons $\mathbb{F}_p^2 = \{x^2, x \in \mathbb{F}_p\}$ et $\mathbb{F}_p^{*2} = \{x^2, x \in \mathbb{F}_p^*\}$.

1. Montrer que $|\mathbb{F}_p^2| = \frac{p+1}{2}$ et $|\mathbb{F}_p^{*2}| = \frac{p-1}{2}$.
2. Montrer que pour $x \in \mathbb{F}_p^*$, $x \in \mathbb{F}_p^{*2}$ ssi $x^{\frac{p-1}{2}} = \bar{1}$.
3. En déduire que pour $p \geq 3$, -1 est un carré ssi $p \equiv 1[4]$.
4. On suppose $p \equiv 3[4]$, pour $x \in \mathbb{F}_p^*$ montrer que x est un carré ssi $-x$ n'en est pas un.
5. Soit $p \in \mathbb{P} \mid p \equiv -1[4]$, pour tout $r \in \mathbb{F}_p^*$ montrer que $\Gamma_r = \{(x, y) \in (\mathbb{F}_p^*)^2 \mid x^2 - y^2 = r\}$ est de cardinal $p - 3$.

1. On étudie le morphisme de groupe

$$\theta : \begin{cases} \mathbb{F}_p^* & \rightarrow \mathbb{F}_p^{*2} \\ x & \mapsto x^2 \end{cases}$$

$$\begin{aligned} \ker \theta &= \{x \in \mathbb{F}_p^*, x^2 = 1\} \\ &= \{x \in \mathbb{F}_p^*, (x-1)(x+1) = 0\} \\ &= \{-1, 1\} \end{aligned}$$

$$\underbrace{|\ker \theta|}_2 \cdot \underbrace{(\text{im } \theta)}_{|\mathbb{F}_p^{*2}|} = p - 1$$

D'où $|\mathbb{F}_p^{*2}| = \frac{p-1}{2}$.

Et $\mathbb{F}_p = \mathbb{F}_p^* \cup \{0\}$ d'où

$$|\mathbb{F}_p^2| = |\mathbb{F}_p^{*2}| + 1 = \frac{p+1}{2}$$

2. Soit $x \in \mathbb{F}_p^{*2}$, on écrit $x = y^2$ avec $y \in \mathbb{F}_p^*$.

$$x^{\frac{p-1}{2}} = y^{p-1} = \bar{1}$$

D'où

$$\underbrace{\mathbb{F}_p^{*2}}_{\frac{p-1}{2}} \subset \underbrace{\left\{ \text{racines de } X^{\frac{p-1}{2}} - 1 \right\}}_{\leq \frac{p-1}{2}}$$

D'où l'égalité des ensembles.

3.
$$\begin{aligned} \bar{-1} \in \mathbb{F}_p^{*2} &\Leftrightarrow (-1)^{\frac{p-1}{2}} = \bar{1} \\ &\Leftrightarrow \frac{p-1}{2} \in 2\mathbb{Z} \\ &\Leftrightarrow p \equiv 1[4] \end{aligned}$$

4. On suppose $p \equiv 3[4]$

$$(-1) \notin \mathbb{F}_p^{*2} \quad \text{car } (-1)^{\frac{p-1}{2}} = -1$$

$$\begin{aligned} x \in \mathbb{F}_p^{*2} &\Leftrightarrow x^{\frac{p-1}{2}} = 1 \\ &\Leftrightarrow (-x)^{\frac{p-1}{2}} = -1 \\ &\Leftrightarrow -x \notin \mathbb{F}_p^{*2} \end{aligned}$$

5. • Si r est un carré, $r = a^2$ avec

$$a \in \mathbb{F}_p^*$$

$$\begin{aligned} (x, y) \in \Gamma_r &\Leftrightarrow x^2 - y^2 = a^2 \\ &\Leftrightarrow (xa^{-1})^2 - (ya^{-1})^2 = 1 \\ &\Leftrightarrow (xa^{-1}, ya^{-1}) \in \Gamma_1 \end{aligned}$$

D'où $|\Gamma_r| = |\Gamma_1|$

- Si r n'est pas un carré, $-r$ en est un.

$$(x, y) \in \Gamma_r \Leftrightarrow y^2 - x^2 = -r$$

Et on se ramène au cas précédent.

$$|\Gamma_r| = |\Gamma_1|$$

Dénombrons Γ_1 .

$$\begin{aligned} (x, y) \in \Gamma_1 &\Leftrightarrow x^2 - y^2 = 1 \\ &\Leftrightarrow (x-y)(x+y) = 1 \end{aligned}$$

Posons $a = x + y, b = x - y$ (p impair d'où $2 \in \mathbb{F}_p^*$)

$$\begin{aligned} x &= a + \frac{b}{2} \\ y &= a - \frac{b}{2} \end{aligned}$$

$$(x, y) \in \Gamma_1 \Leftrightarrow b = a^{-1}$$

On a $(p-1)$ choix pour a , et b déterminé par a , d'où au plus $(p-1)$ couples.

Il faut exclure les cas où notre choix de a permet $x, y \notin \mathbb{F}_p^*$:

$$\begin{aligned} x = \bar{0} &\Leftrightarrow a = -a^{-1} \\ &\Leftrightarrow a^2 = -1 \\ y = \bar{0} &\Leftrightarrow a = a^{-1} \\ &\Leftrightarrow a^2 = 1 \end{aligned}$$

Ainsi $|\Gamma_r| = |\Gamma_1| = p - 3$.

Sous algèbres

Définition, propriétés des sous-algèbres.

Soit $(A, +, \times, \cdot)$ une \mathbb{K} -algèbre, $B \subset A$ est une sous-algèbre de A si c'est un sous-anneau et un sev de A .

De plus si B est de dimension finie

$$B^\times = B \cap A^\times$$

Démonstration

On a évidemment $B^\times \subset B \cap A^\times$.

On suppose $b \in B \cap A^\times$, on dispose de $a \in A, ab = ba = 1$.

On pose

$$\varphi_b = \left\{ \begin{array}{l} B \rightarrow B \\ x \mapsto bx \end{array} \right. \in \mathcal{L}(B)$$

Soit $x \in \ker \varphi_b$, on a $bx = 0$ donc $(ab)x = x = 0$.

Donc φ_b bijectif (argument dimensionnel), et $\varphi_b^{-1}(1) = a$ existe et $a \in B$.

Algèbres commutatives intégrales de dimension finie

Que peut-on dire d'une algèbre $(A, +, \times, \cdot)$ commutative et intégrale de dimension finie ?

Si $(A, +, \times, \cdot)$ est commutative, intégrale et de dimension finie, alors c'est un corps.

Démonstration

Soit $a \in A \setminus \{0\}$, étudions

$$\varphi_a : \begin{cases} A \rightarrow A \\ x \mapsto ax \end{cases} \in \mathcal{L}(A)$$

$$\begin{aligned} \ker \varphi_a &= \{x \in A \mid ax = 0\} \\ &= \{x \in A \mid x = 0\} \quad (\text{par intégrité}) \\ &= \{0\} \end{aligned}$$

Et par argument dimensionnel, φ_a bijectif, d'où $\varphi_a^{-1}(a) = a^{-1}$ existe.

Morphisme d'algèbre

Définition, propriétés des morphismes d'algèbres.

Pour A, B deux \mathbb{K} -algèbre, une application $\varphi : A \rightarrow B$ est un morphisme d'algèbre si c'est un morphisme d'anneau linéaire.

Et dans ce cas $\text{im } \varphi$ est une sous-algèbre de B et $\ker \varphi$ est un idéal et un sev de A .

Dévissage de groupes

Propriétés, outils du dévissage de groupes.

1. Soient G et H deux groupes cycliques de cardinaux n et p , $G \times H$ est cyclique ssi $n \wedge p = 1$.
- 2.

Démonstration

1. • Par contraposé, supposons que $n \wedge p = d > 1$, ainsi $m = n \vee p < np$.

Pour tout $(x, y) \in G \times H$,

$$(x, y)^m = (x^m, y^m) = (e_G, e_H)$$

donc $\text{ord}((x, y)) \mid m < |G \times H|$ qui ne peut être cyclique.

- Soit $x \in G$ d'ordre n et $y \in H$ d'ordre p . Pour $k \in \mathbb{N}^*$

$$(x, y)^k \Leftrightarrow (x^k, y^k) = (e_G, e_H)$$

$$\Leftrightarrow \begin{cases} n \mid k \\ p \mid k \end{cases} \Leftrightarrow np \mid k$$

$$\Leftrightarrow G \times H \text{ cyclique}$$

- Autre méthode :

$$G \simeq \mathbb{Z}/n\mathbb{Z}$$

$$H \simeq \mathbb{Z}/p\mathbb{Z}$$

$$G \times H \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

$$\simeq \mathbb{Z}/(np)\mathbb{Z} \quad \text{cyclique}$$

2. Soient H, K sous-groupes de G et φ (qui n'est pas forcément un morphisme) tel que

$$\varphi : \begin{cases} H \times K \rightarrow G \\ (h, k) \mapsto hk \end{cases}$$

On note $HK = \varphi(H \times K)$.

Soient $(h, k), (h_0, k_0) \in H \times K$

$$\varphi(h, k) = \varphi(h_0, k_0)$$

$$\Leftrightarrow hk = h_0k_0$$

$$\Leftrightarrow h_0^{-1}h = k_0k^{-1} = t \in H \cap K$$

$$\Leftrightarrow \exists t \in H \cap K, \begin{cases} h = k_0t \\ k = t^{-1}h_0 \end{cases}$$

φ est injectif ssi $H \cap K = \{e_G\}$, c'est automatique si $|H| \wedge |K| = 1$ (en étudiant les ordres et les divisibilités de ceux-ci).

Dans ce cas $|HK| = |\text{im } \varphi| = |H| \cdot |K|$

Dans le cas général

$$|\varphi^{-1}\{\varphi(h_0, k_0)\}| = |H \cap K|$$

Groupe Diédral

Construction et propriétés du groupe diédral.

Construction

Soient $n \geq 2$ et A_0, \dots, A_{n-1} des points de \mathbb{R}^2 d'afixes

$$\forall i \in \llbracket 0, n-1 \rrbracket, A_i : e^{\frac{2ik\pi}{n}}$$

On considère Γ l'ensemble des isométries qui préservent le polygone A_0, \dots, A_{n-1} .

Comme une transformation affine préserve les barycentres, tout élément de Γ préserve l'isobarycentre (l'origine).

On a alors

$$\Gamma \in O(\mathbb{R}^2)$$

Et donc tout $\gamma \in \Gamma$, est soit une rotation ou une réflexion.

- Si γ est une rotation : $\gamma(A_0) \in \{A_0, \dots, A_{n-1}\}$ d'où $\gamma = \text{rot}\left(\frac{2k\pi}{n}\right)$ pour un $k \in \llbracket 0, n-1 \rrbracket$.

On note r la rotation d'angle $\frac{2\pi}{n}$

$$\gamma = r^k$$

- Si γ est une réflexion

Soit s la réflexion à l'axe des abscisses, $s \in \Gamma$.

$s \circ \gamma \in \Gamma$ est une rotation car

$$\det(s \circ \gamma) = (-1)^2 = 1$$

Ainsi $\exists k \in \llbracket 0, n-1 \rrbracket$ tel que

$$s \circ \gamma = r^k \Leftrightarrow \gamma = s \circ r^k$$

Donc

$$\Gamma = \bigcup_{k=0}^{n-1} \{r^k, sr^k\}$$

Groupe

Γ est un sous-groupe de $O(\mathbb{R}^2)$.

- $|\Gamma| = 2n$
- $\Gamma = \langle s, r \rangle$

Algèbre engendrée

Pour $(A, +, \times, \cdot)$ une \mathbb{K} -algèbre et $\alpha \in A$, définition et propriétés de $\mathbb{K}[\alpha]$.

Soit $(A, +, \times, \cdot)$ une \mathbb{K} -algèbre et $\alpha \in A$. Si on pose le morphisme d'algèbre

$$\theta_\alpha : \begin{cases} \mathbb{K}[X] & \rightarrow A \\ P = \sum_{k=0}^d a_k X^k & \mapsto \sum_{k=0}^d a_k \alpha^k \end{cases}$$

On note $\mathbb{K}[\alpha] = \text{im } \theta_\alpha$ qui est la plus petite sous-algèbre de A contenant α .

De plus $\ker \theta_\alpha$ est un idéal de $\mathbb{K}[X]$.

- Si θ_α est injectif et $\mathbb{K}[\alpha] \simeq \mathbb{K}[X]$ qui est donc de dimension infinie.
- Sinon on dispose d'un unique polynôme π_α unitaire tel que $\ker \theta_\alpha = \pi_\alpha \mathbb{K}[X]$ (par principalité).

π_α est appelé polynôme minimal de α , $\mathbb{K}[\alpha]$ est de dimension $d = \deg \pi_\alpha$ et $(1, \alpha, \dots, \alpha^{d-1})$ en est une base.

Démonstration

- Soit $B \in \mathbb{K}[X] \setminus \{0\}$ et $d = \deg B$, par l'existence et l'unicité de la division euclidienne on a

$$\mathbb{K}[X] = B\mathbb{K}[X] \oplus \mathbb{K}_{d-1}[X]$$

- Soit $u \in \mathcal{L}(E, F)$ et G un supplémentaire de $\ker u$, montrons que $u|_G$ est un isomorphisme de $G \rightarrow \text{im } u$.

$\ker u|_G = \ker u \cap G = \{0\}$ par complémentarité.

Soit $y \in \text{im } u$, $y = u(x)$, $x = a + b$ avec $(a, b) \in \ker u \times G$.

$$\begin{aligned} u(x) &= \underbrace{u(a)}_0 + u(b) \\ y &= u|_G(b) \end{aligned}$$

Soit $y \in \text{im } u|_G$, $y = u|_G(x) = u(x)$.

D'où $\text{im } u = \text{im } u|_G$.

- Si θ_α est injectif, c'est un isomorphisme de $\mathbb{K}[X]$ sur $\text{im } \theta_\alpha = \mathbb{K}[\alpha]$.
- Sinon on a π_α de degré d et

$$\mathbb{K}[X] = \pi_\alpha \mathbb{K}[X] \oplus \mathbb{K}_{d-1}[X]$$

\mathbb{K}_{d-1} est un supplémentaire de $\ker \theta_\alpha$, ainsi $\theta_\alpha|_{\mathbb{K}_{d-1}[X]}$ est un isomorphisme de $\mathbb{K}_{d-1}[X] \rightarrow \mathbb{K}[\alpha]$, d'où

$$\dim \mathbb{K}[\alpha] = d$$

Et l'image de la base canonique de $\mathbb{K}_{d-1}[X]$ par $\theta|_{\mathbb{K}_{d-1}[X]}$ est

$$(1, \alpha, \dots, \alpha^{d-1})$$

Qui est donc une base de $\mathbb{K}[\alpha]$.

Condition d'intégrité d'une sous-algèbre engendrée

Pour A une \mathbb{K} -algèbre et $\alpha \in A$ tel que θ_α n'est pas injectif, sous quelle condition $\mathbb{K}[\alpha]$ est elle intègre ?

Soit A une \mathbb{K} -algèbre et $\alpha \in A$ tel que θ_α n'est pas injectif.

$\mathbb{K}[\alpha]$ est intègre ssi π_α est irréductible.

Démonstration

- Si π_α irréductible, soit $x = P(\alpha), y = Q(\alpha) \in \mathbb{K}[\alpha]$ tels que $xy = 0$.

$$PQ(\alpha) = 0$$

$$\pi_\alpha \mid PQ$$

Donc par le lemme d'Euclide,

$$\text{ou } \begin{array}{l} \pi_\alpha \mid P \Leftrightarrow x = 0 \\ \pi_\alpha \mid Q \Leftrightarrow y = 0 \end{array}$$

- Par contraposé, si π_α non irréductible, $\pi_\alpha = PQ$ avec $P, Q \in \mathbb{K}[X]$ non inversible ou associé à π_α .

$$\underbrace{P(\alpha)}_{\neq 0} \underbrace{Q(\alpha)}_{\neq 0} = \pi_\alpha(\alpha) = 0$$

D'où $\mathbb{K}[\alpha]$ non intègre.

inversibilité des éléments d'une sous-algèbre engendrée

Soit $\mathbb{K}[\alpha]$ une sous-algèbre de A de dimension finie pour $\alpha \in A$, sous quelle condition $x \in \mathbb{K}[\alpha]$ est-il inversible ?

Soit $\mathbb{K}[\alpha]$ une sous-algèbre de A de dimension finie pour $\alpha \in A$.
Soit $x = P(\alpha) \in \mathbb{K}[\alpha]$.

$$x \in \mathbb{K}[\alpha]^\times \text{ ssi } P \wedge \pi_\alpha = 1$$

On en déduit que $\mathbb{K}[\alpha]$ est un corps ssi π_α est irréductible.

Démonstration

Par propriété de sous-algèbre

$$\mathbb{K}[\alpha]^\times = A^\times \cap \mathbb{K}[\alpha]$$

Ainsi

$$\begin{aligned} x \in \mathbb{K}[\alpha]^\times &\Leftrightarrow \exists y \in \mathbb{K}[\alpha], xy = 1 \\ &\Leftrightarrow \exists Q \in \mathbb{K}[X], PQ(\alpha) = 1 \\ &\Leftrightarrow \exists Q \in \mathbb{K}[X], \pi_\alpha \mid (PQ - 1) \\ &\Leftrightarrow \exists Q, V \in \mathbb{K}[X], PQ - 1 = \pi_\alpha V \\ &\Leftrightarrow \exists Q, V \in \mathbb{K}[X], PQ - \pi_\alpha V = 1 \\ &\Leftrightarrow P \wedge \pi_\alpha = 1 \end{aligned}$$

Ainsi si π_α irréductible, pour tout $x = P(\alpha) \in \mathbb{K}[\alpha] \setminus \{0\}$, $P \wedge \pi_\alpha = 1$ d'où x inversible et $\mathbb{K}[\alpha]$ est un corps.

Et si $\mathbb{K}[\alpha]$ est un corps, alors il est intègre et π_α irréductible.

Algèbres et extensions de corps

Propriétés des algèbres en lien avec les extensions de corps.

Soient $\mathbb{K} \subseteq \mathbb{L}$ deux corps. On remarque que \mathbb{L} est une \mathbb{K} -algèbre.

1. Soit $\alpha \in \mathbb{L}$ qui admet un polynôme annulateur dans $\mathbb{K}[X]$ et π_α son polynôme minimal.

π_α est irréductible dans $\mathbb{K}[X]$ et $\mathbb{K}[\alpha]$ est un corps.

Démonstration

1. $P, Q \in \mathbb{K}[X]$ tels que $\pi_\alpha = PQ$.

Dans \mathbb{L}

$$P(\alpha)Q(\alpha) = \pi_\alpha(\alpha) = 0$$

Donc $P(\alpha) = 0 \Leftrightarrow \pi_\alpha \mid P$ ou $Q(\alpha) = 0 \Leftrightarrow \pi_\alpha \mid Q$ donc π_α irréductible.

Ainsi $\mathbb{K}[\alpha]$ est un corps.

Nombres algébriques

Définitions et propriétés des nombres algébriques sur un corps \mathbb{K} .

Soit $\alpha \in A$ une \mathbb{K} -algèbre, on dit que α est algébrique sur \mathbb{K} s'il admet un polynôme annulateur dans $\mathbb{K}[X]$.

Par défaut α algébrique veut dire algébrique sur \mathbb{Q} , quitte à les échanger prenons $P(\alpha) = 0, P \in \ker \theta_\alpha = \pi_\alpha \mathbb{K}[X]$.

Propriété

1. Soit $\alpha \in \mathbb{L}$ une extension de corps de \mathbb{K} , α algébrique sur \mathbb{K} .

Pour tout $P \in \mathbb{K}[X]$ unitaire, $P = \pi_\alpha$ ssi $P(\alpha) = 0$ et P irréductible sur $\mathbb{K}[X]$.

Démonstration

1. Sens direct connu. Soit $P \in \mathbb{K}[X]$ unitaire, irréductible et annulateur de α .

On a $\pi_\alpha \mid P$, or P irréductible donc P et π_α sont associés, or tout deux unitaires donc $P = \pi_\alpha$.

Théorème de la base téléscopique

Énoncer et démonstration du
théorème de la base
téléscopique.

Soit $\mathbb{K} \subseteq \mathbb{L}$ deux corps tel que \mathbb{L}
est de dimension finie sur \mathbb{K} .

Soient

- E un \mathbb{L} -ev, (et donc un \mathbb{K} -ev).
- $e = (e_1, \dots, e_n)$ base de E sur \mathbb{L} .
- $z = (z_1, \dots, z_p)$ base de \mathbb{L} sur \mathbb{K} .

Alors $F = (z_i e_j)_{\substack{i \in \llbracket 1, p \rrbracket \\ j \in \llbracket 1, n \rrbracket}}$ est une
base de E sur \mathbb{K}

Ainsi $\dim_{\mathbb{K}} E = \dim_{\mathbb{L}} E \cdot \dim_{\mathbb{K}} \mathbb{L}$.

Démonstration

- Soit $\omega \in E$, on dispose de
 $\lambda_1, \dots, \lambda_n \in \mathbb{L}$ tels que

$$\omega = \sum_{j=1}^n \lambda_j e_j$$

On dispose de $(a_{ij})_{ij} \in \mathbb{K}^{\llbracket 1, p \rrbracket \llbracket 1, n \rrbracket}$

$$\forall j \in \llbracket 1, n \rrbracket, \lambda_j = \sum_{i=1}^p \alpha_{ij} z_i$$

Ainsi

$$\omega = \sum_{j=1}^n \sum_{i=1}^p \alpha_{ij} z_i e_j$$

- Soit $(a_{ij})_{ij} \in \mathbb{K}^{\llbracket 1, p \rrbracket \llbracket 1, n \rrbracket}$ tel que

$$\sum_{j=1}^n \underbrace{\sum_{i=1}^p a_{ij} z_i}_{\lambda_j \in \mathbb{L}} e_j = 0$$

$$\sum_{j=1}^n \lambda_j e_j = 0$$

Donc pour tout $j \in \llbracket 1, n \rrbracket, \lambda_j = 0$.

$$\lambda_j = \sum_{i=1}^p a_{ij} z_i = 0$$

Donc par liberté de $z, a_{ij} = 0$
pour tout i, j .

Clôture algébrique des rationnels

Propriétés de la clôture algébrique de \mathbb{Q} .

Notons \mathbb{K} l'ensemble des $\alpha \in \mathbb{C}$ algébriques sur \mathbb{Q} .

\mathbb{K} est un corps algébriquement clos.

Démonstration : corps

- Soit $\alpha, \beta \in \mathbb{K}$, montrons que $\alpha\beta, \alpha + \beta \in \mathbb{K}$.

On utilise le fait que z algébrique dans \mathbb{L} ssi $\mathbb{L}[z]$ de dimension finie sur \mathbb{L} (car z admet un polynôme annulateur dans $\mathbb{L}[X]$).

- ▶ Donc $\mathbb{Q}[\alpha]$ est de dimension finie sur \mathbb{Q} ,
- ▶ β algébrique sur $\mathbb{Q} \subset \mathbb{Q}[\alpha]$ donc algébrique sur $\mathbb{Q}[\alpha]$.
- ▶ Donc $\mathbb{Q}[\alpha][\beta]$ est de dimension finie sur $\mathbb{Q}[\alpha]$, et donc par le théorème de la base télescopique, sur \mathbb{Q} .
- ▶ Or $\mathbb{Q}[\alpha + \beta], \mathbb{Q}[\alpha\beta] \subseteq \mathbb{Q}[\alpha][\beta]$, donc $\mathbb{Q}[\alpha + \beta]$ et $\mathbb{Q}[\alpha\beta]$ sont de dimension finie sur \mathbb{Q} .
- Soit $\alpha \in \mathbb{K} \setminus \{0\}$, soit π_α son polynôme minimal et $d = \deg \pi_\alpha$.

$$\underbrace{X^d \pi_\alpha \left(\frac{1}{X} \right)}_{\in \mathbb{Q}[X]} \text{ annule } \frac{1}{\alpha}$$

Donc $\frac{1}{\alpha} \in \mathbb{K}$

- $1 \in \mathbb{K}$ car $\mathbb{Q} \subseteq \mathbb{K}$.

Démonstration : clôture

Soit $P = \sum_{k=0}^d a_k X^k \in \mathbb{K}[X]$. Soit $\alpha \in \mathbb{C}$ racine de P , montrons que $\alpha \in \mathbb{K}$.

Pour tout $k \in \llbracket 0, d \rrbracket$, $a_k \in \mathbb{K}$ donc $\mathbb{Q}[a_k]$ de dimension finie sur \mathbb{Q} .

Par récurrence on a

$$\mathbb{L} = \mathbb{Q}[a_0][a_1] \cdots [a_d]$$

De dimension finie sur \mathbb{Q} .

Comme $P \in \mathbb{L}[X]$ annule α , $\mathbb{L}[\alpha]$ est de dimension finie sur \mathbb{L} et donc sur \mathbb{Q} , id est $\alpha \in \mathbb{K}$.

Exercice : Gauss-Lucas

Soit $P \in \mathbb{C}[X]$, montrer que les racines de P' sont dans l'enveloppe convexe des racines de P .

Soit $P \in \mathbb{C}[X]$, montrer que les racines de P' sont dans l'enveloppe convexe des racines de P .

On écrit

$$P = c \prod_{k=1}^N (X - a_k)^{m_k}$$

Soit b une racine de P' .

Si $b \in \{a_1, \dots, a_N\}$, b est nécessairement dans leur enveloppe convexe.

Sinon

$$\frac{P'}{P} = \sum_{k=1}^n \frac{m_k}{X - a_k}$$

$$0 = \frac{P'}{P}(b) = \sum_{k=1}^N \frac{m_k}{b - a_k} = \sum_{k=1}^N \frac{m_k}{\overline{b - a_k}}$$

$$= \sum_{k=1}^N \frac{m_k}{|b - a_k|^2} (b - a_k)$$

$$b = \frac{\sum_{k=1}^N \frac{a_k m_k}{|b - a_k|^2}}{\sum_{k=1}^N \frac{m_k}{|b - a_k|^2}}$$

$$= \sum_{k=1}^N \lambda_k a_k$$

Où $\lambda_k = \frac{\frac{a_k m_k}{|b - a_k|^2}}{\sum_{i=1}^N \frac{m_i}{|b - a_i|^2}}$ (on a alors $\sum_{k=1}^N \lambda_k = 1$).

b est donc un barycentre à coefficients positifs des a_1, \dots, a_n et est donc dans leur enveloppe convexe.

Exercice : Dénombrement de morphismes

1. Dénombrer les morphismes de G_1 vers G_2 , avec $|G_1| \wedge |G_2| = 1$.
2. Dénombrer les morphismes de G_1 vers G_2 où G_1 et G_2 sont cyclique.
3. Même chose avec les injections et les surjections.

Remarque générale

Soit $\varphi : G_1 \rightarrow G_2$ morphisme de groupe, $x \in G_1$

$$\begin{aligned}\varphi(x)^{\text{ord}(x)} &= e_{G_2} \\ \text{donc } \text{ord}(\varphi(x)) & \mid |G_2| \\ \text{et } \text{ord}(\varphi(x)) & \mid |G_1|\end{aligned}$$

Ainsi $\text{ord}(\varphi(x)) \mid |G_1| \wedge |G_2|$.

Exercices

1. Soit $\varphi : G_1 \rightarrow G_2$ morphisme, $x \in G_1$. Par la remarque ci dessus $\text{ord}(\varphi(x)) \mid p \wedge q = 1$ donc $\varphi(x) = 0$, il n'y a donc que morphisme le morphisme triviale.

2. Notons $G_1 = \langle a \rangle$, posons

$$\theta : \begin{cases} \text{hom}(G_1, G_2) & \rightarrow G_2 \\ \varphi & \mapsto \varphi(a) \end{cases}$$

Qui est injectif car tout morphisme est uniquement déterminé par son image du générateur a .

Pour tout $\varphi \in \text{hom}(G_1, G_2)$ on a

$$\varphi(a)^{|G_1|} = \varphi(a^{|G_1|}) = \varphi(e_{G_1}) = e_{G_2}$$

D'où

$$\text{im } \theta \subset \{y \in G_2 \mid y^{|G_1|} = e_{G_2}\}$$

Soit $y \in \text{im } \theta$ posons

$$\varphi : \begin{cases} G_1 & \rightarrow G_2 \\ x = a^k & \mapsto y^k \end{cases}$$

Qui ne dépend pas du k choisi, soit $x = a^k = a^l$:

$$\begin{aligned}a^{k-l} &= e_{G_1} \\ \text{donc } |G_1| & \mid k-l \\ \text{et } y^{k-l} &= e_{G_2} \\ \text{d'où } y^k &= y^l\end{aligned}$$

Donc $\theta(\varphi) = y$.

$$\begin{aligned}|\text{hom}(G_1, G_2)| &= |\text{im } \theta| \\ &= \left| \{y \in G_2 \mid y^{|G_1|} = e_{G_2}\} \right| \\ &= |\{y \in G_2 \mid \text{ord}(y) \mid |G_1|\}| \\ &= \bigoplus_{d \mid |G_1|} \{y \in G_2 \mid \text{ord}(y) = d\} \\ &= \sum_{d \mid |G_1| \wedge |G_2|} \varphi(d) \\ &= |G_1| \wedge |G_2|\end{aligned}$$

3. • Pour les injections on veut $\varphi \in \text{hom}(G_1, G_2)$ tels que $\ker \varphi = \{e_{G_1}\}$.

Pour $k \in \llbracket 1, |G_1| - 1 \rrbracket$,

$$\begin{aligned}\varphi(a)^k &= \varphi(a^k) \neq 0 \\ \text{ord } \varphi(a) &= |G_1|\end{aligned}$$

Si $|G_1| \nmid |G_2|$, G_2 ne contient pas éléments d'ordre $|G_1|$ donc aucune injection.

Si $|G_1| \mid |G_2|$, il y a $\varphi(|G_1|)$ éléments d'ordre $|G_1|$, donc autant d'injections.

- Pour les surjections on veut $\text{ord } \varphi(a) = |G_2|$, donc

$$\begin{cases} 0 & \text{si } |G_2| \nmid |G_1| \\ \varphi(|G_2|) & \text{sinon} \end{cases}$$

Exercice : Union de sous espaces vectoriels

E un \mathbb{K} espace vectoriel.

1. Soit F, G deux sev de E ,
montrer que $F \cup G$ sev ssi $F \subseteq G$ ou $G \subseteq F$.
2. Supposons \mathbb{K} infini, soit
 F_1, \dots, F_n n sevs, montrer que si
 $\bigcup_{k=1}^n F_k$ est un sev, alors il
existe $i \in \llbracket 1, n \rrbracket$ tel que

$$\bigcup_{k=1}^n F_k = F_i$$

1. Soit F, G sevs de E un \mathbb{K} -ev tel
que $F \cup G$ est un sev.

Si $F \not\subseteq G$, on pose $z \in F \setminus G$,
soit $x \in G$.

$$x + z \in F \cup G$$

$x + z \notin G$ car sinon

$$F \setminus G \ni z = \underbrace{(x + z)}_{\in G} - \underbrace{x}_{\in G} \in G$$

Donc $x + z \in F$ d'où

$$x = (x + z) - z \in F$$

Et $G \subseteq F$.

2. Soient F_1, \dots, F_n sevs de E tels
que $\bigcup_{k=1}^n F_k$ est un sev.

Notons $U_m = \bigcup_{k=1}^m F_k$ pour $m \in \mathbb{N}$.

On a déjà fait le cas $n = 2$ et le
cas $n = 1$ est trivial.

Supposons la propriété vraie
pour un $n \in \mathbb{N}$.

Si $U_n \subseteq F_{n+1}$ alors on a fini.

Si $F_{n+1} \subseteq U_n$ alors par
hypothèse de récurrence, on
dispose de $i \in \llbracket 1, n \rrbracket$

$$U_{n+1} = U_n = F_i$$

Sinon, on dispose de

$$x \in F_{n+1} \setminus U_n \subseteq U_{n+1}$$

$$y \in U_n \setminus F_{n+1} \subseteq U_{n+1}$$

Soient $\lambda_0, \dots, \lambda_{n+1} \in \mathbb{K}$ deux à
deux distincts.

$$z_k = x + \lambda_k y$$

Par le lemme des tiroirs, on
dispose de $k \neq l$ et j tel que

$$z_k, z_l \in F_j$$

Si $j = n + 1$

$$z_k - z_l = \underbrace{(\lambda_k - \lambda_l)}_{\neq 0} y \in F_{n+1}$$

Et $y \in F_{n+1}$ impossible.

Si $j \in \llbracket 1, n \rrbracket$

$$\lambda_l z_k - \lambda_k z_l = \underbrace{(\lambda_l - \lambda_k)}_{\neq 0} x \in F_j$$

Et $x \in F_j$ impossible.

Somme directe de sous espaces vectoriels

Définition et propriétés de
somme directe de sev.

Soient F_1, \dots, F_n sev de E un \mathbb{K} -ev.
On dit qu'ils sont en somme
directe si pour tout $x \in \sum_{k=1}^n F_k$

$$\exists! (x_1, \dots, x_n) \in \prod_{k=1}^n F_k, \quad x = \sum_{k=1}^n x_k$$

Il y a équivalence entre F_1, \dots, F_n
en somme directe et

1. $\forall (x_1, \dots, x_n) \in \prod_{k=1}^n F_k, \quad \sum_{k=1}^n x_k = 0 \Rightarrow \forall k \in \llbracket 1, n \rrbracket, \quad x_k = 0.$
2. $\forall i \in \llbracket 1, n \rrbracket, \quad F_i \cap \left(\sum_{i \neq k} F_k \right) = \{0\}$
3. $F_n \cap \bigoplus_{k=1}^{n-1} F_k = \{0\}$

En dimension finie

4. $\dim \sum_{k=1}^n F_k \leq \sum_{k=1}^n \dim F_k$
avec égalité ssi les F_1, \dots, F_n
sont en somme directe.

Démonstration

1. \Rightarrow il s'agit d'un cas particulier
pour $x = 0$.

$$\Leftarrow \text{Supposons } \sum_{k=1}^n x_k = \sum_{k=1}^n x'_k$$

Alors $\sum_{k=1}^n (x_k - x'_k) = 0$ donc
 $x_k = x'_k$ pour tout $k \in \llbracket 1, n \rrbracket$.

3. \Rightarrow Soit $x \in F_n \cap \bigoplus_{k=1}^n F_k$

$$\begin{aligned} x &= \sum_{k=1}^{n-1} 0 + x \\ &= \sum_{k=1}^{n-1} x_k + 0 \quad \text{car } x \in \bigoplus_{k=1}^{n-1} F_k \end{aligned}$$

Donc par unicité de la
décomposition $x = \sum_{k=1}^n 0 = 0$.

\Leftarrow Soit $x_1, \dots, x_n \in E$ tels que

$$\begin{aligned} \sum_{k=1}^n x_k &= 0 \\ -x_n &= \sum_{k=1}^{n-1} x_k \in F_n \cap \bigoplus_{k=1}^{n-1} F_k \end{aligned}$$

Donc $x_n = 0$ et $\sum_{k=1}^{n-1} x_k = 0$
donc $x_1 = x_2 = \dots = x_n = 0$.

Espaces supplémentaires

Définition, propriétés des
espaces supplémentaires.

Soient F_1, \dots, F_n sevs de E un \mathbb{K} -
ev. On dit qu'ils sont
supplémentaires si

$$E = \bigoplus_{k=1}^n F_k$$

Et on a

$$E = \bigoplus_{k=1}^n F_k$$

$$\Leftrightarrow \begin{cases} E = \sum_{k=1}^n F_k \\ \dim(E) = \sum_{k=1}^n \dim(F_k) \end{cases}$$

$$\Leftrightarrow \begin{cases} \sum_{k=1}^n F_k = \bigoplus_{k=1}^n F_k \\ \dim(E) = \sum_{k=1}^n \dim(F_k) \end{cases}$$

Notations de matrices

Notations de matrices :
changements de bases, matrices
d'un endomorphisme, ...

Soit $u \in \mathcal{L}(E, F)$, $e = (e_1, \dots, e_n)$, $e' = (e'_1, \dots, e'_n)$ bases de E et $f = (f_1, \dots, f_p)$ base de F .

Applications linéaires

$$\mathcal{M}_{e,f}(u) = \mathcal{M}_{e \leftarrow f}(u) = \mathcal{M}_e^f(u) \in M_{pn}(\mathbb{K})$$

Et la matrice est alors

$$\mathcal{M}_{f \leftarrow e}(u) = \begin{matrix} & u(e_1) & u(e_2) & \cdots & u(e_n) \\ \begin{matrix} f_1 \\ f_2 \\ \vdots \\ f_p \end{matrix} & \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{p1} & a_{p2} & \cdots & a_{pn} \end{pmatrix} \end{matrix}$$

Où pour $j \in \llbracket 1, n \rrbracket$

$$u(e_j) = \sum_{k=1}^p a_{kj} f_k$$

Endomorphismes

$$\mathcal{M}_e(u) = \mathcal{M}_{e \leftarrow e}(u) = \mathcal{M}_e^e(u)$$

$$u(e_j) = \sum_{k=1}^p a_{kj} f_k$$

Changement de base

$$P_{e \rightarrow e'} = \mathcal{M}_e(e') = \mathcal{M}_{e \leftarrow e'}(\text{id})$$

Exercice : Noyaux et images itérées

Soit $u \in \mathcal{L}(E)$ avec E un \mathbb{K} -ev.

Que peut on dire des suites

$(\ker u^k)_k$ et $(\operatorname{im} u^k)_k$?

Soit $u \in \mathcal{L}(E)$ avec E un \mathbb{K} -ev.

Dimension quelconque

- Si $\ker u^k = \ker u^{k+1}$ pour un $k \in \mathbb{N}$ alors pour tout $n \geq k$, $\ker u^k = \ker u^n$.
- De même pour les images.

Dimension finie

En notant $n = \dim E$ on a

$$d_k = \dim \ker u^k \in \llbracket 0, n \rrbracket \nearrow$$

$$r_k = \operatorname{rg} u^k \in \llbracket 0, n \rrbracket \searrow$$

Ces deux suites sont donc stationnaires, on peut poser

$$m_K = \min\{k \in \mathbb{N} \mid \ker u^k = \ker u^{k+1}\}$$

$$m_I = \min\{k \in \mathbb{N} \mid \operatorname{im} u^k = \operatorname{im} u^{k+1}\}$$

On a de plus $m_K = m_I = m$.

Et en notant

$$K = \bigcup_{k \in \mathbb{N}} \ker u^k = \ker u^m$$

$$I = \bigcap_{k \in \mathbb{N}} \operatorname{im} u^k = \operatorname{im} u^m$$

Qui sont les valeurs auxquelles les suites stationnent, on a

- $K \oplus I = E$
- K, I stables par u
- $u|_K^K$ est nilpotent
- $u|_I^I$ est inversible.
- Si $E = K' \oplus I'$ avec K', I' stables par u , $u|_{K'}^{K'}$ nilpotent et $u|_{I'}^{I'}$ inversible, alors $K' = K$ et $I' = I$.

Démonstration

- Soit $l \geq k$, on a évidemment $\ker u^l \subseteq \ker u^{l+1}$.

Soit $x \in \ker u^{l+1}$:

$$u^{k+1}(u^{l-k}(x)) = 0$$

$$u^{l-k}(x) \in \ker u^{k+1} = \ker u^k$$

$$u^k(u^{l-k}(x)) = 0$$

$$x \in \ker u^l$$

- Soit $l \geq k$, on a évidemment $\operatorname{im} u^{l+1} \subseteq \operatorname{im} u^l$.

Soit $u^l(x) = y \in \operatorname{im} u^l$:

$$u^{l-k}(u^k(x)) = y$$

$$u^k(x) \in \operatorname{im} u^k = \operatorname{im} u^{k+1}$$

$$u^k(x) = u^{k+1}(x')$$

$$u^{l-k}(u^{k+1}(x')) = y$$

$$y \in \operatorname{im} u^{l+1}$$

Dimension finie

- Par le théorème de rang on a $d_k = n - r_k$, donc si r_k est constante à partir du rang m_I , alors d_k est aussi constante à partir de ce rang, donc $m_K = m_I$.

- Soit $y \in K \cap I$, on dispose de $x \in E$ tel que

$$u^m(x) = y$$

$$u^m(y) = 0$$

$$u^{2m}(x) = 0$$

$$x \in \ker u^{2m} = \ker u^m$$

$$u^m(x) = y = 0$$

donc $K \cap I = \{0\}$.

- Soit $x \in K = \ker u^m$

$$u^m(u(x)) = u^{m+1}(x) = 0$$

donc $u(x) \in K$.

- Soit $y \in I = \operatorname{im} u^m$, on dispose de $x \in E$ tel que

$$u^m(x) = y$$

$$u^{m+1}(x) = u(y) \in \operatorname{im} u^m$$

$$u(y) = u^m(x')$$

et $u(y) \in I$.

- Notons $\tilde{u} = u|_K^K$ l'endomorphisme induit par u sur K .

$$\tilde{u}^m(K) = u^m(K) = \{0\}$$

Donc \tilde{u} est nilpotent d'indice m .

- Notons $\tilde{u} = u|_I^I$ l'endomorphisme induit par u sur I .

$$\tilde{u}(I) = u(\operatorname{im} u^m) = \operatorname{im} u^{m+1}$$

$$= \operatorname{im} u^m = I$$

Donc \tilde{u} est inversible.

- Soit $K' \oplus I' = E$ qui respectent les hypothèses.

On dispose de $d \in \mathbb{N}^*$ tel que

$$u^d(K') = \{0\}$$

$$K' \subseteq \ker u^d \subset K = \bigcup_{k \in \mathbb{N}} \ker u^k$$

Et on a

$$u(I') = I'$$

$$u^m(I') = I'$$

$$I' \subseteq \operatorname{im} u^m = I$$

Donc

$$\dim K' \leq \dim K$$

$$\dim I' \leq \dim I$$

Et on obtient l'égalité par complémentarité, d'où $K' = K$ et $I' = I$.

Développement du déterminant par ligne ou par colonne

Formules et définitions du développement du déterminant par ligne ou par colonne.

Soit $A \in M_n(\mathbb{K})$

- pour tout $j \in \llbracket 1, n \rrbracket$:

$$\det(A) = \sum_{i=1}^n (-1)^{i+j} a_{ij} \det(\tilde{A}_{ij})$$

- pour tout $i \in \llbracket 1, n \rrbracket$:

$$\det(A) = \sum_{j=1}^n (-1)^{i+j} a_{ij} \det(\tilde{A}_{ij})$$

Où $\tilde{A}_{ij} \in M_{n-1}(\mathbb{K})$ est la matrice A privée de sa $i^{\text{ème}}$ ligne et $j^{\text{ème}}$ colonne.

On appelle $\hat{A}_{ij} = (-1)^{i+j} \det(\tilde{A}_{ij})$ cofacteur.

On appelle $\text{com}(A)$ la matrice des cofacteurs.

Et on a

$$A \cdot \text{com}(A)^T = \det(A) I_n$$

Exercice : rang d'une comatrice

Soit $A \in M_n(\mathbb{K})$ ($n \geq 3$), calculer $\text{rg com}(A)$ en fonction de $\text{rg } A$.

Soit $A \in M_n(\mathbb{K})$ avec $n \geq 3$.

- Si $\text{rg } A = n$, $A \in \text{GL}_n(\mathbb{K})$ donc $\text{com } A \in \text{GL}_n(\mathbb{K})$ et $\text{rg com}(A) = n$.
- Si $\text{rg } A \leq n - 2$, pour tout $i, j \in \llbracket 1, n \rrbracket$ la matrice \tilde{A}_{ij} extraite de A privée de sa $i^{\text{ème}}$ ligne et $j^{\text{ème}}$ colonne est de rang inférieur à $n - 2$ et n'est donc pas inversible, $\text{com } A = 0$ et $\text{rg com}(A) = 0$.
- Si $\text{rg } A = n - 1$, on dispose d'une matrice extraite de taille $n - 1$ inversible, donc au moins un des cofacteur est non nul d'où $\text{rg com}(A) \geq 1$.

De plus

$$A^T \text{com}(A) = \det(A)I_n = 0$$

Donc $\text{im com}(A) \subseteq \ker A^T$ et $\dim \ker A^T = 1$ d'où $\text{rg com}(A) \leq 1$.

Algorithme du pivot de Gauss

Description de l'algorithme du pivot de Gauss, et propriétés qui en découlent.

Opérations, représentation matricielle

Notons $(E_{ij})_{ij}$ la base canonique de $M_n(\mathbb{K})$. On a

$$E_{ik}E_{lj} = \delta_{kl}E_{ij}$$

Pour $A \in M_{np}(\mathbb{K})$

$$E_{kl}^{(n)} A = \left(\begin{array}{c|c} & \begin{matrix} 1 \\ \vdots \\ k \\ \vdots \\ n \end{matrix} \end{array} \right)$$

$$AE_{kl}^{(p)} = \left(\begin{array}{ccc|ccc} & & C_k & & & \\ 1 & \dots & l & \dots & n \end{array} \right)$$

Ainsi on peut définir

- $T_{kl}(\lambda) = I_n + \lambda E_{kl}^{(n)}$ la transvection sur les lignes ($L_k \leftarrow L_k + \lambda L_l$)
- $T'_{kl}(\lambda) = I_p + \lambda E_{kl}^{(p)}$ la transvection sur les colonnes ($C_l \leftarrow C_l + \lambda C_k$)
- $P_{kl} = I_n - E_{kk}^{(n)} - E_{ll}^{(n)} + E_{kl}^{(n)} + E_{lk}^{(n)}$ la transposition de lignes ($L_l \leftrightarrow L_k$)
- $P_{kl} = I_p - E_{kk}^{(p)} - E_{ll}^{(p)} + E_{kl}^{(p)} + E_{lk}^{(p)}$ la transposition de colonnes ($C_l \leftrightarrow C_k$)

Algorithme

Prenons $A = (C_1 \dots C_n) \in M_n(\mathbb{K})$

- Si $A = 0$ fini.
- Soit $j = \min\{k \in \llbracket 1, n \rrbracket \mid C_k \neq 0\}$

$$A^{(1)} : C_j \leftrightarrow C_1$$

- Soit $i = \min\{k \in \llbracket 1, n \rrbracket \mid a_{i1} \neq 0\}$
 - Si $i = 1$ on effectue $L_2 \leftarrow L_2 + L_1$ et on prend $i = 2$.

$$A^{(2)} : L_1 \leftarrow L_1 + \left(1 - \frac{a_{11}}{a_{i1}}\right) L_i$$

$$A^{(2)} = \left(\begin{array}{c|ccc} 1 & * & \dots & * \\ * & & & \\ \vdots & & & \\ * & & & * \end{array} \right)$$

- Pour tout $i \in \llbracket 2, n \rrbracket$ on effectue

$$A^{(i+1)} : L_i \leftarrow L_i - a_{i1} L_1$$

Ainsi

$$A^{(n+1)} = \left(\begin{array}{c|ccc} 1 & * & \dots & * \\ 0 & & & \\ \vdots & & & \\ 0 & & & \tilde{A} \end{array} \right)$$

On répète l'algorithme sur \tilde{A} , on obtient alors

$$\tilde{\tilde{A}} = \left(\begin{array}{cc|c|c} 1 & (*) & * & \\ & \ddots & \vdots & (*) \\ & & 1 & * \\ \hline & & \mu & * \dots * \\ \hline & & & 0 \\ & & & \ddots \\ & & & 0 \end{array} \right)$$

Avec $\mu \neq 1$ ssi le blocs de zéros à la fin est de taille nulles (on ne dispose pas des lignes nécessaires pour se ramener à $\mu = 1$).

On peut alors finalement effectuer pour tout $i \in \llbracket 1, \text{rg } A \rrbracket$, puis pour $j \in \llbracket i + 1, n \rrbracket$

$$\tilde{\tilde{\tilde{A}}} : C_j \leftarrow C_j - \frac{\tilde{\tilde{A}}_{ij}}{\tilde{\tilde{A}}_{ii}} C_i$$

$$\tilde{\tilde{\tilde{A}}} = \left(\begin{array}{ccccccc} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \mu & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{array} \right)$$

On remarque que si A est inversible, les transpositions sont inutiles car il n'existe pas de colonnes nulles.

Propriétés

- Les transvections engendrent $\text{SL}_n(\mathbb{K})$.
- Les transvections et une dilatation (pour atteindre n'importe quel déterminant) suffisent à engendrer $\text{GL}_n(\mathbb{K})$.

Intersection d'hyperplans

Propriétés sur les intersections
d'hyperplans.

Soient $(\varphi_1, \dots, \varphi_p) \in \mathcal{L}(E, \mathbb{K})^p$

$$\dim \bigcap_{k=1}^p \ker \varphi_k = n - \operatorname{rg}(\varphi_1, \dots, \varphi_p) \\ \geq n - p$$

Démonstration

On montre l'inégalité par
récurrence sur p .

Montrons l'égalité.

Quitte à extraire et renuméroter,
 $(\varphi_1, \dots, \varphi_r)$ est libre.

Or pour tout $k \in \llbracket r+1, p \rrbracket$,

$$\varphi_k \in \operatorname{Vect}(\varphi_1, \dots, \varphi_r)$$

$$\text{Donc } \bigcap_{i=1}^r \ker \varphi_i \subseteq \ker \varphi_k$$

$$\text{D'où } \bigcap_{k=1}^p \ker \varphi_k = \bigcap_{k=1}^r \ker \varphi_k$$

Donc (cf. lemme sur la liberté
d'une famille de formes linéaires)

$$\theta : \begin{cases} E \rightarrow \mathbb{K}^r \\ x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_r(x) \end{pmatrix} \end{cases} \text{ surjective} \\ \ker \theta = \bigcap_{k=1}^r \ker \varphi_k$$

Donc par le théorème du rang

$$\dim \left(\bigcap_{k=1}^p \ker \varphi_k \right) = n - \operatorname{rg}(\varphi_1, \dots, \varphi_p)$$

Liberté d'une famille de l'espace dual

Démonstration d'une CNS pour
la liberté d'une famille de $\mathcal{L}(E, \mathbb{K})$
où E est un \mathbb{K} -ev.

Soient $\varphi_1, \dots, \varphi_p \in \mathcal{L}(E, \mathbb{K})$.

La famille $(\varphi_1, \dots, \varphi_p)$ est libre ssi

$$\theta : \begin{cases} E \rightarrow \mathbb{K}^p \\ x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_p(x) \end{pmatrix} \end{cases} \text{ surjective}$$

Démonstration

- Supposons θ surjective, on considère $\lambda_1, \dots, \lambda_p \in \mathbb{K}$ tels que

$$\sum_{k=1}^p \lambda_k \varphi_k = 0$$

Soit $i \in \llbracket 1, p \rrbracket$, on dispose de $x \in E$ tel que

$$\theta(x) = \begin{pmatrix} 1 \\ \vdots \\ i \\ \vdots \\ p \end{pmatrix} = \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_i(x) \\ \vdots \\ \varphi_p(x) \end{pmatrix}$$

Ainsi

$$\left(\sum_{k=1}^p \lambda_k \varphi_k \right)(x) = 0 = \lambda_i$$

- Par contraposé supposons θ non surjective : $\text{rg } \theta \leq p - 1$.

On dispose de H hyperplan tel que $\text{im } \theta \subseteq H$. Donc on dispose de $(\alpha_1, \dots, \alpha_p) \in \mathbb{K}^p \setminus \{0\}$ tels que

$$H = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in \mathbb{K}^p \mid \sum_{k=1}^p \alpha_k x_k = 0 \right\}$$

Donc pour tout $x \in E$,

$$\theta(x) = \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_p(x) \end{pmatrix} \in \text{im } \theta \subseteq H$$

$$\sum_{k=1}^p \alpha_k \varphi_k(x) = 0$$

Donc $\sum_{k=1}^p \alpha_k \varphi_k = 0$ et la famille est liée

Condition de liberté d'une forme linéaire à une famille

Soit $\varphi_1, \dots, \varphi_p, \psi \in \mathcal{L}(E, \mathbb{K})$.

Démonstration d'une CNS pour que $\psi \in \text{Vect}(\varphi_1, \dots, \varphi_p)$.

Soit $\varphi_1, \dots, \varphi_p, \psi \in \mathcal{L}(E, \mathbb{K})$.

Pour tout $\psi \in \mathcal{L}(E, \mathbb{K})$

$$\varphi \in \text{Vect}(\varphi_1, \dots, \varphi_p)$$

$$\text{ssi } \bigcap_{k=1}^p \ker \varphi_k \subseteq \ker \psi$$

Démonstration

- Si $\varphi \in \text{Vect}(\varphi_1, \dots, \varphi_p)$, on dispose de $\lambda_1, \dots, \lambda_p \in \mathbb{K}$ tels que

$$\psi = \sum_{k=1}^p \lambda_k \varphi_k$$

D'où

$$\begin{aligned} \psi \left(\bigcap_{k=1}^p \ker \varphi_k \right) &= \sum_{k=1}^p \lambda_k \varphi_k \left(\bigcap_{i=1}^p \ker \varphi_i \right) \\ &= \{0\} \end{aligned}$$

Et donc $\bigcap_{k=1}^p \ker \varphi_k \subseteq \ker \psi$.

- Supposons $\bigcap_{k=1}^p \ker \varphi_k \subseteq \ker \psi$.

Quitte à extraire et renuméroter, $(\varphi_1, \dots, \varphi_r)$ est libre.

Or pour tout $k \in \llbracket r+1, p \rrbracket$,

$$\varphi_k \in \text{Vect}(\varphi_1, \dots, \varphi_r)$$

$$\text{Donc } \bigcap_{i=1}^r \ker \varphi_i \subseteq \ker \varphi_k$$

$$\text{D'où } \bigcap_{k=1}^p \ker \varphi_k = \bigcap_{k=1}^r \ker \varphi_k$$

Donc

$$\theta : \begin{cases} E \rightarrow \mathbb{K}^r \\ x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_r(x) \end{pmatrix} \end{cases} \text{ surjective}$$

Posons alors

$$\theta' : \begin{cases} E \rightarrow \mathbb{K}^{r+1} \\ x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_r(x) \\ \psi(x) \end{pmatrix} \end{cases}$$

Or

$$\bigcap_{k=1}^r \ker \varphi_k = \bigcap_{k=1}^p \ker \varphi_k \subseteq \ker \psi$$

$$\text{Donc } \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \notin \text{im } \theta'$$

La famille $(\varphi_1, \dots, \varphi_r, \psi)$ est liée d'où $\psi \in \text{Vect}(\varphi_1, \dots, \varphi_p)$.

Base duale, antéduale

Définitions, propriétés, démonstrations autour des bases duales.

Base duale

Soit E un \mathbb{K} -ev de dimension finie, $e = (e_1, \dots, e_n)$ une base de E .

Il existe une unique famille $(\varphi_1, \dots, \varphi_n) \in \mathcal{L}(E, \mathbb{K})^n$ tel que

$$\forall i, j \in \llbracket 1, n \rrbracket, \varphi_i(e_j) = \delta_{ij}$$

Cette famille est appelée base duale de e et est une base de $\mathcal{L}(E, \mathbb{K})$.

Dans ce cas

$$\forall x \in E, x = \sum_{k=1}^n \varphi_k(x) e_k$$

$$\forall \psi \in \mathcal{L}(E, \mathbb{K}), \psi = \sum_{k=1}^n \psi(e_k) \varphi_k$$

Base antéduale

Pour toute base $(\varphi_1, \dots, \varphi_n)$ de $\mathcal{L}(E, \mathbb{K})$, il existe une unique base (e_1, \dots, e_n) de E tel que $(\varphi_1, \dots, \varphi_n)$ en est la base duale.

Démonstration

- Existence / Unicité : car les formes linéaires sont uniquement déterminés par leurs images d'une base.
- Génératrice : Soit $\psi \in \mathcal{L}(E, \mathbb{K})$ pour tout $i \in \llbracket 1, n \rrbracket$

$$\left(\sum_{k=1}^n \psi(e_k) \varphi_k \right) (e_i) = \sum_{k=1}^n \psi(e_k) \varphi_k(e_i) = \psi(e_i)$$

$$\text{Donc } \psi = \sum_{k=1}^n \psi(e_k) \varphi_k$$

Donc $(\varphi_1, \dots, \varphi_n)$ est une base.

- Soit $x = \sum_{k=1}^n x_k e_k \in E, i \in \llbracket 1, n \rrbracket$

$$\begin{aligned} \varphi_i(x) &= \varphi_i \left(\sum_{k=1}^n x_k e_k \right) \\ &= \sum_{k=1}^n x_k \delta_{ik} = x_i \end{aligned}$$

- Soit $(\varphi_1, \dots, \varphi_n)$ base de $\mathcal{L}(E, \mathbb{K})$

$$\theta : \begin{cases} E \rightarrow \mathbb{K}^n \\ x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_n(x) \end{pmatrix} \end{cases} \text{ surjective}$$

Par liberté de la famille, donc bijective par argument dimensionnel.

Notons (b_1, \dots, b_n) la base canonique de \mathbb{K}^n .

La famille $(e_k = \theta^{-1}(b_k))_{k \in \llbracket 1, n \rrbracket}$ est l'unique base de E tel que

$$\forall i, j \in \llbracket 1, n \rrbracket, \varphi_i(e_j) = \delta_{ij}$$

Lemme de factorisation

Énoncé et démonstration du lemme de factorisation en algèbre linéaire.

Soient E, F, G trois \mathbb{K} -ev

1. Soient $u \in \mathcal{L}(E, F), v \in \mathcal{L}(E, G)$, dans ce cas

$$\ker u \subseteq \ker v \\ \Leftrightarrow \exists w \in \mathcal{L}(F, G), v = w \circ u$$

(Si u est inversible $w = v \circ u^{-1}$).

2. Soient $u \in \mathcal{L}(E, F), v \in \mathcal{L}(G, F)$, dans ce cas

$$\operatorname{im} v \subseteq \operatorname{im} u \\ \Leftrightarrow \exists w \in \mathcal{L}(G, E), v = u \circ w$$

Démonstration

1. • Supposons qu'il existe $w \in \mathcal{L}(F, G)$ tel que $v = w \circ u$.

$$v(\ker u) = w(u(\ker u)) \\ = w(\{0\}) = 0$$

D'où $\ker u \subseteq \ker v$.

- Supposons que $\ker u \subseteq \ker v$.

Soient H, K tels que

$$\ker u \oplus H = E \\ \operatorname{im} u \oplus K = F$$

Posons

$$\tilde{u} : \begin{cases} H \rightarrow \operatorname{im} u \\ x \mapsto u(x) \end{cases} \\ \ker \tilde{u} = \ker u \cap H = \{0\} \\ \dim H = \operatorname{rg} u$$

Donc \tilde{u} inversible.

On peut donc écrire

$$w : \begin{cases} F = \operatorname{im} u \oplus K \rightarrow G \\ x = y + z \mapsto v \circ \tilde{u}^{-1}(y) \end{cases}$$

Soit $x = y + z \in E = \ker u \oplus H$.

$$w \circ u(x) = v(\tilde{u}^{-1}(u(z))) \\ = v(z) \\ v(x) = \underbrace{v(y)}_0 + v(z)$$

2. • Supposons qu'il existe $w \in \mathcal{L}(G, E)$ tel que $v = u \circ w$

$$v(E) = u \circ w(E) \subseteq u(E)$$

D'où $\operatorname{im} v \subseteq \operatorname{im} u$.

- Supposons que $\operatorname{im} v \subseteq \operatorname{im} u$.

Soit H tel que $\ker u \oplus H = E$.

$$\tilde{u} : \begin{cases} H \rightarrow \operatorname{im} u \\ x \mapsto u(x) \end{cases} \\ w : \begin{cases} G \rightarrow E \\ x \mapsto \tilde{u}^{-1} \circ v(x) \end{cases}$$

On a bien pour $x \in E$

$$u \circ w(x) = \tilde{u}(\tilde{u}^{-1}(v(x))) = v(x)$$

Vandermonde, interpolation de Lagrange

Définitions, propriétés et démonstrations de l'interpolation de Lagrange et des matrices des Vandermonde.

Soit \mathbb{K} un corps, $n \in \mathbb{N}$, $a_0, \dots, a_n \in \mathbb{K}$ deux à deux distincts.

$$\theta : \begin{cases} \mathbb{K}_n[X] \rightarrow \mathbb{K}^{n+1} \\ P \mapsto \begin{pmatrix} P(a_0) \\ \vdots \\ P(a_n) \end{pmatrix} \in \mathcal{L}(\mathbb{K}_n[X], \mathbb{K}^{n+1}) \end{cases}$$

Pour tout $P \in \ker \theta$,

$$P(a_0) = P(a_1) = \dots = P(a_n) = 0$$

Donc P est de degré n avec $n + 1$ racines distinctes, d'où $P = 0$.

Donc θ est un isomorphisme.

Notons

$$e = (e_0, \dots, e_n)$$

$$c = (1, X, \dots, X^n)$$

Les bases canoniques de \mathbb{K}^{n+1} et $\mathbb{K}_n[X]$.

$$\forall k \in \llbracket 0, n \rrbracket, \theta^{-1}(e_k) = \prod_{\substack{i=0 \\ i \neq k}}^n \frac{X - a_i}{a_k - a_i} = L_k(X)$$

La matrice de θ dans les bases canoniques est appelée matrice de Vandermonde de a_0, \dots, a_n .

$$\mathcal{M}_{e \leftarrow c}(\theta) = \begin{pmatrix} 1 & a_0 & a_0^2 & \dots & a_0^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^n \end{pmatrix}$$

Son déterminant vaut

$$\begin{aligned} V(a_0, \dots, a_n) &= \det(\mathcal{M}_{e \leftarrow c}(\theta)) \\ &= \prod_{0 \leq i < j \leq n} (a_j - a_i) \end{aligned}$$

Démonstration

Par récurrence sur n , initialisée aisément pour $n = 1$.

On suppose la formule pour un $n \in \mathbb{N}$.

$$P(X) = V(a_0, \dots, a_n, X)$$

$$\begin{aligned} &= \begin{vmatrix} 1 & a_0 & a_0^2 & \dots & a_0^{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n+1} \\ 1 & X & X^2 & \dots & X^{n+1} \end{vmatrix} \\ &= \sum_{j=0}^{n+1} (-1)^{n+j} X^j V_j \end{aligned}$$

Où V_j est le déterminant mineur en $(n + 2, j + 1)$. De plus

$$\deg P \leq n + 1$$

$$\text{cd } P = V(a_0, \dots, a_n) \neq 0$$

De plus pour tout $k \in \llbracket 0, n \rrbracket$, $P(a_k) = 0$ donc

$$\begin{aligned} P &= V(a_0, \dots, a_n) \prod_{k=0}^n (X - a_k) \\ &= \prod_{0 \leq i < j \leq n} (a_j - a_i) \prod_{k=0}^n (X - a_k) \end{aligned}$$

Ainsi on peut calculer

$$\begin{aligned} P(a_{n+1}) &= V(a_0, \dots, a_{n+1}) \\ &= \prod_{0 \leq i < j \leq n} (a_j - a_i) \prod_{k=0}^n (a_{n+1} - a_k) \\ &= \prod_{0 \leq i < j \leq n+1} (a_j - a_i) \end{aligned}$$

Exercice : endomorphisme qui stabilise toutes les droites

Soit $u \in \mathcal{L}(E)$ qui stabilise toute les droites, qu'en dire de u ?

Par définition pour tout $x \in E$, $u(x) = \lambda_x x$ avec $\lambda_x \in \mathbb{K}$.

Soit $x, y \in E \setminus \{0\}$.

- Si (x, y) est liée, $y = \alpha x$

$$\lambda_y \alpha x = u(y) = \alpha u(x) = \lambda_x \alpha x$$

$$\lambda_y = \lambda_x$$

- Sinon (x, y) est libre

$$\lambda_{x+y}(x+y) = u(x+y) = u(x) + u(y)$$

$$\lambda_{x+y}x + \lambda_{x+y}y = \lambda_x x + \lambda_y y$$

$$\lambda_x = \lambda_{x+y} = \lambda_y$$

Donc pour tout $x \in E$, $\lambda_x = \lambda$ et
 $u = \lambda \text{id}$.

Endomorphismes nilpotents

Définition d'un endomorphisme nilpotent et inégalité sur son indice.

Soit $u \in \mathcal{L}(E)$, u est dit nilpotent s'il existe $q \in \mathbb{N}^*$ tel que $u^q = 0$.

On appelle indice de nilpotence la valeur

$$d = \min\{q \in \mathbb{N}^* \mid u^q = 0\}$$

On a toujours $d \leq \dim E$.

Démonstration

Comme $u^{d-1} \neq 0$ on dispose de $x \in E$ tel que $u^{d-1}(x) \neq 0$.

Considérons la famille $(x, u(x), \dots, u^{d-1}(x))$, soient $\lambda_0, \dots, \lambda_{d-1}$ tels que

$$\sum_{k=0}^{d-1} \lambda_k u^k(x) = 0$$

$$\begin{aligned} u^{d-1} \left(\sum_{k=0}^{d-1} \lambda_k u^k(x) \right) &= \lambda_0 u^{d-1}(x) = 0 \\ &\Rightarrow \lambda_0 = 0 \end{aligned}$$

$$\begin{aligned} u^{d-2} \left(\sum_{k=1}^{d-1} \lambda_k u^k(x) \right) &= \lambda_1 u^{d-1}(x) = 0 \\ &\Rightarrow \lambda_1 = 0 \end{aligned}$$

\vdots

$$\lambda_0 = \lambda_1 = \dots = \lambda_{d-1} = 0$$

D'où $d \leq n$.