Leçon n°101 : Groupe opérant sur un ensemble. Exemples et applications.

28 juillet 2026

Soit G un groupe et X un ensemble

I Action d'un groupe sur un ensemble

I.A) Vocabulaire et premières propriétés [Rombaldi]

Définition 1 – Action d'un groupe sur un ensemble

On dit que G opère à gauche sur X si on a une application $G \times X \to X, (g,x) \mapsto g.x$ telle que $\forall h, g \in G, \forall x \in X, g.(h.x) = (gh).x$ et $1.x = x$

Remarque 2

Cela revient à se donner un morphisme de groupes $\Psi : G \to \mathfrak{S}(X)$ en posant $\Psi(g)(x) = g.x$.
Lorsque $\forall h, g \in G, \forall x \in X, g.(h.x) = (hg).x$ on parle d'action à droite.

Exemple 3

- G opère sur lui-même par translation à gauche $g.h = gh$
- G opère sur lui-même par conjugaison : $g.h = g^{-1}hg$. On note $\mathrm{Int}(G) = \{\mathrm{Int}(g), g \in G\}$ où $\mathrm{Int}(g) : h \mapsto g^{-1}hg$. On remarque alors que G agit sur tout sous-groupe distingué H de G par cette opération.
- $\mathfrak{S}(X)$ opère naturellement sur X : $\sigma.x = \sigma(x)$

Définition 4

Soit G opérant sur X.

- Pour $x \in X$, on appelle orbite de x et on note $O(x)$ l'ensemble $G.x = \{g.x, g \in G\}$. On note O l'ensemble des orbites de X. C'est une partition de X.
- L'action de G sur X est dite transitive si $\forall x \in X, O(x) = X$.
- On dit que l'action de G sur X est fidèle si le morphisme de groupe $\Psi : g \in G \mapsto (\Psi(g) : x \mapsto g.x) \in \mathfrak{S}(E)$ est injectif

Théorème 5 – Théorème de Cayley

G est isomorphe à un sous-groupe de $\mathfrak{S}(G)$.

Exemple 6

- L'action de G sur lui-même par translation est transitive et fidèle.
- Si $H < G$ agit sur G par translation à droite $h.g = gh^{-1}$, alors $O(g) = gH$ est la classe à gauche de g dans G/H. On note $[G : H]$ le cardinal des orbites lorsqu'il est fini.
- $\mathfrak{S}(X)$ agit transitivement sur X.
- Restreignons l'action de $\mathfrak{S}_n$ sur $[\![1, n]\!]$ à $< \sigma >$ où $\sigma \in \mathfrak{S}_n$. Chaque orbite correspond aux éléments d'un des cycles de la décomposition en cycles disjoints de σ.

Application 15

Ainsi si G est un p-groupe alors son centre n'est pas trivial.

I.B. Les orbites comme outil de dénombrement [Rombaldi]

On considère G opérant sur X.

Définition 7 – Stabilisateur, action libre, fixateur

On appelle stabilisateur de $x \in X$ le groupe $\mathrm{Stab}(x) = \{g \in G, g.x = x\}$.
On dit que G opère librement sur X si $\forall x \in X, \mathrm{Stab}(x) = \{e\}$ (en particulier, une action libre est fidèle).
Pour $g \in G$, on note $\mathrm{Fix}(g) = \{x \in X, g.x = x\}$.

Proposition 8

Soit $x \in X$. L'application $g \in G \mapsto g.x \in O(x)$ a pour noyau $\mathrm{Stab}(x)$. L'application quotient est alors une bijection de $G/\mathrm{Stab}(x)$ dans $O(x)$. Dans le cas où G est fini, on a alors

$$\forall x \in X, |O(x)| = \frac{|G|}{|\mathrm{Stab}(x)|}$$

Dans la suite de cette partie, on suppose que G et X sont finis.

Corollaire 9 – Equations aux classes

Si G est fini, choisissons pour chaque orbite O un représentant x_O. Alors :

$$|X| = \sum_{O \in \mathcal{O}} \frac{|G|}{|\mathrm{Stab}(x_O)|}$$

Exemple 10

Si G agit par conjugaison sur lui-même, notons $\mathcal{Z}_h(G) = \{g \in G, ghg^{-1} = h\}$. Alors $|G| = |\mathcal{Z}(G)| + \sum_{O \in \mathcal{O}, |O| \geq 2} \frac{|G|}{|\mathcal{Z}_{x_O}(G)|}$.

Corollaire 11 – Formule de Burnside

$|\mathcal{O}| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$.

II. Action sur les groupes finis

On suppose toujours G de cardinal fini dans cette partie. On note $n = |G|$.

II.A. Résultats généraux [Rombaldi]

Théorème 12 – Théorème de Lagrange

L'ordre de tout sous-groupe de G divise n. En particulier, l'ordre d'un élément de G divise n.

Théorème 13 – Théorème de Cauchy

Si p est un diviseur premier de n, alors il existe un élément d'ordre p dans G.

II.B. Cas particulier des p-groupes (p-Sylow) [Perrin]

Soit p un nombre premier diviseur de n. On notera $n = p^\alpha m$ avec $p \nmid m$.

Définition 14

Si n est une puissance de p ($m = 1$), on dit que G est un p-groupe.

Plus généralement, on appelle p-Sylow de G tout sous-groupe de G de cardinal p^α.

Théorème 16 – Théorème de Sylow 1

Il existe au moins un p-Sylow dans G

Corollaire 17

Il existe au moins un sous-groupe de G d'ordre p^i pour $i \in [\![1, \alpha]\!]$.

Théorème 18 – Théorème de Sylow 2

- Si $H < G$ est un p-groupe, alors il existe un p-Sylow tel que $H < S$,
- Les p-Sylow sont tous conjugués,
- Si on note n_p le nombre de p-Sylow de G, on a $n_p | m$ et $n_p \equiv 1 \mod p$.

Corollaire 19

Soit S un p-Sylow de G. Alors $S \lhd G \iff S$ est l'unique p-Sylow de G.

Application 20

Tout groupe d'ordre 63 n'est pas simple.

II.C. Action sur le groupe $\mathfrak{S}_n$ [Rombaldi]

Définition 21

Le support d'une permutation $\sigma \in \mathfrak{S}_n$ est le complémentaire dans $[\![1, n]\!]$ des points fixes de σ. Autrement dit,$\text{supp}(\sigma) = \{i \in [\![1, n]\!], \sigma(i) \neq i\}$

Théorème 22

Toute permutation de $\mathfrak{S}_n \backslash \{id\}$ se décompose en produit de cycles deux à deux disjoints. Cette décomposition est unique à l'ordre près.

Définition 23

On considère $\sigma \in \mathfrak{S}_n$. On appelle type de σ la liste $\lambda(\sigma) = [\lambda_1, \dots, \lambda_n]$ où λ_1 est le nombre de points fixes de σ et λ_k le nombre de k-cycles dans la décomposition de σ.

Théorème 24

Deux permutations sont conjuguées si et seulement si elles ont même type.

Théorème 25

Pour $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont intérieurs.

III. Applications des actions de groupes en algèbre linéaire

III.A. Action sur les matrices [H2G2 + Rombaldi+ Francinou Algèbre 2]

Soient $m, n \in \mathbb{N}^*$ et $\mathbb{K}$ un corps.

Théorème 26

On considère l'action de $\mathcal{GL}_n(\mathbb{K})$ sur $\mathcal{M}_{n,m}(\mathbb{K})$ par $(P, A) \mapsto PA$.
Deux matrices sont dans la même orbite si et seulement si, elles ont même noyau.

Théorème 27

On considère l'action de $\mathcal{GL}_m(\mathbb{K})$ sur $\mathcal{M}_{n,m}(\mathbb{K})$ par $(P, A) \mapsto AP^{-1}$.
Deux matrices sont dans la même orbite si et seulement si, elles ont même image.

Définition 28 – Action de Steinitz

Posons $G = \mathcal{GL}_m(\mathbb{K}) \times \mathcal{GL}_n(\mathbb{K})$.On appelle action de Steinitz l'action :

$$G = \mathcal{GL}_m(\mathbb{K}) \times \mathcal{GL}_n(\mathbb{K}) \to \mathcal{M}_{m,n}(\mathbb{K}), ((P, Q), A) \mapsto PAQ^{-1}$$

Les orbites pour cette action sont appelées classes d'équivalences.

Théorème 29

Deux matrices sont équivalentes si et seulement si elles ont même rang. Ainsi $\mathcal{O} = \{\mathcal{O}_r, r \in [\![0, \min(n, m)]\!]\}$ où $\mathcal{O}_r = \{A \in \mathcal{M}_{m,n}(\mathbb{K}), \text{rang}(A) = r\}$.

Définition 30

Les orbites de l'action de $\mathcal{GL}_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$ sont appelées classes de similitudes.

Proposition 31

Dans $\mathbb{K} = \mathbb{C}$, $M \in \mathcal{M}_n(\mathbb{C})$ est diagonalisable $\iff$ sa classe de similitude est fermée dans $\mathcal{M}_n(\mathbb{C})$.

III.B. Utilisation de la notion d'action en théorie des nombres [H2G2 p 182]

Définition 32

Deux formes quadratiques q et q' sont congruentes s'il existe $\varphi \in GL(E)$ tel que $q' = q \circ \varphi$. Si E est de dimension finie et si $\mathcal{B}$ est une base de E. Les formes quadratiques q et q' sont alors congruentes si

$$A_{q'} = {}^tPA_qP$$

.

On dira alors que deux matrices symétriques A et B sont congruentes s'il existe une matrice $P \in GL_n(\mathbb{K})$ telle que $B = {}^tPAP$

Théorème 33 – Classification des formes quadratiques sur différents corps

Corps K	**Invariant total**	**Forme normale**
$\mathbb{C}$	Rang : $r \in \{0, \dots, n\}$	$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$
$\mathbb{R}$	Signature : (s, t) ; $s + t \leq n$	$\begin{pmatrix} I_s & 0 & 0 \\ 0 & -I_t & 0 \\ 0 & 0 & 0 \end{pmatrix}$
$\mathbb{F}_q$	Discriminant : $\delta \in \mathbb{K}^*/(\mathbb{K}^*)^2$	$\begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & \delta \end{pmatrix}$

Théorème 34 – Loi de réciprocité quadratique

Soient $p \neq q$ des nombres premiers impairs. Alors :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Théorème 35 – Loi de réciprocité quadratique complémentaires

Soit p un nombre premier impair

— $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

— $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

III.C. Utilisation de la notion d'action en géométrie [Carnet de voyages en Algébrie / H2G2]

Théorème 36 – Isométries du cube + coloriage

Les isométries du cube sont :

$$Iso^+(\mathcal{C}) \simeq \mathfrak{S}_4 \text{ et } Iso(\mathcal{C}) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$$

Il y a 57 manières de colorier les faces d'un cube avec au plus 3 couleurs.

Lemme 37

Soit $M \in SO_3(\mathbb{R})$. Alors M est conjuguée dans $O_3(\mathbb{R})$ à une matrice de la forme

$$\begin{pmatrix} 1 & 0 \\ 0 & R_\theta \end{pmatrix}$$

Lemme 38

Pour tout toute droite vectorielle $\mathcal{D}$ de $\mathbb{R}^3$ et toute matrice $M \in O_3(\mathbb{R})$, on a :

$$M\rho_{\mathcal{D}}M^{-1} = \rho_{M(\mathcal{D})}$$

Lemme 39

Les retournements engendrent $SO_3(\mathbb{R})$.

Lemme 40

Les retournements sont tous conjugués dans $SO_3(\mathbb{R})$

Théorème 41

Le groupe $SO_3(\mathbb{R})$ est simple.

Références :

— Rombaldi page 21 et page 184,

— Perrin ,

— Caldéro Histoires Hédonistes de groupes et de géométries TOME PREMIER,

— Nouvelle H2G2

— Carnet de voyage en algébrie.

— Francinou Algèbre 2 et 3

PLAN :

Table des matières

I Action d'un groupe sur un ensemble **1**

I.A Vocabulaire et premières propriétés [Rombaldi] . . . 1

I.B. Les orbites comme outil de dénombrement . . . 1

II. Action sur les groupes finis **1**

II.A. Résultats généraux . . . 1

II.B. Cas particulier des p-groupes (p-Sylow) . . . 1

II.C. Action sur le groupe $\mathfrak{S}_n$ . . . 2

III. Applications des actions de groupes en algèbre linéaire **2**

III.A. Action sur les matrices . . . 2

III.B. Utilisation de la notion d'action en théorie des nombres . . . 2

III.C. Utilisation de la notion d'action en géométrie . . . 3

Leçon n° 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.

Lever Hugo, Piroutet Alban

Agrégation de Mathématiques — 2025

I De l'exponentielle complexe au groupe $\mathbb{U}$ [Arnaudiès Cours de mathématiques Tome 1 p. 247]

I.A) Autour de l'exponentielle

Définition 1
Exponentielle complexe, cos et sin complexe

Proposition 2

1. exp, sin et cos sont des séries entières de rayon de convergence infini et sont donc définies et holomorphe sur $\mathbb{C}$. De plus exp est sa propre dérivée.
2. $\forall z \in \mathbb{C}, \exp(iz) = \cos(z) + i\sin(z)$
3. Pour $\theta \in \mathbb{R}, \cos(\theta)$ et $\sin(\theta)$ sont réels et $|e^{i\theta}| = 1$.
4. exp est un morphisme continue surjectif de $(\mathbb{C}, +) \to (\mathbb{C}^*, \times)$ de noyau $2i\pi\mathbb{Z}$

Proposition 3

1. Formule de Moivre : $\forall n \in \mathbb{N}, \forall \theta \in \mathbb{R}, (\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$
2. Formule D'Euler : $\forall \theta \in \mathbb{R}, \cos(\theta) = \frac{e^{i\theta}+e^{-i\theta}}{2}$ et $\sin(\theta) = \frac{e^{i\theta}-e^{-i\theta}}{2i}$

Application 4
Linéarisation de $\cos^n$ et $\sin^n$.

Application 5
Calcul des noyaux de Dirichlet et Féjer :

$$D_N = \sum_{n=-N}^{N} e^{in.} = \frac{\sin(\frac{2N+1}{2}.)}{\sin(./2)} \text{ et } K_N = \frac{1}{N}\sum_{n=0}^{N-1} D_n = \sum_{n=-N}^{N}(1 - \frac{|n|}{N})e_n = \frac{\sin^2(N./2)}{\sin^2(./2)}$$

I.B. Le groupe des nombres complexes de module 1 et racine $n$ième de l'unité [Cours de Mathematiques. Tome 1 - Jean-Marie Arnaudiés, Henri Fraysse PDF p°226]

On notera $\mathbb{U} = \{z \in \mathbb{C}, |z| = 1\}$ le groupe des racines de l'unité, $\mathbb{U}_{\mathbb{Q}} = \{e^{2ip\pi}, p \in \mathbb{Q}\}$ et pour $n \in \mathbb{N}^*, \mathbb{U}_n = \{e^{\frac{2ik\pi}{n}} | k \in \mathbb{N}^*\}$ le groupe des racines n-ième de l'unité.

Exemple 6
Sur l'annexe représenté $\mathbb{U}_1$,$\mathbb{U}_2$,$\mathbb{U}_3$,$\mathbb{U}_4$.

Proposition 7

1. Pour $n \in \mathbb{N}^*, \mathbb{U}_n \subset \mathbb{U}_{\mathbb{Q}} \subset \mathbb{U}$ sont des sous-groupes de $(\mathbb{C}^*, \times)$ et $\mathbb{U}_n$ fini d'ordre n et c'est le seul.
2. $\mathcal{E} : \mathbb{R} \to \mathbb{U}$ est un morphisme surjectif et induit un isomorphisme $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$.
3. $\mathbb{R}_+^* \times \mathbb{U} \to \mathbb{C}^*, (r, u) \mapsto r\mathcal{E}(u)$ est un isomorphisme de groupes

Application 8
Pour $n \geq 2$, $\sum_{w \in \mathbb{U}_n} w = 0$

Application 9
Résolution de $z^n = z_0$ pour un $z_0 \in \mathbb{C}$.

Définition 10
Racine primitive de l'unité et ensemble des racines $n$ième primitive de l'unité $\mathbb{U}_n^*$.

Définition 11
Indicatrice D'Euler

Proposition 12

1. $\mathbb{U}_d \subset \mathbb{U}_n \iff d|n$
2. $\mathbb{U}_n = \cup_{d|n}\mathbb{U}_d^*$

Application 13
$n = \sum_{d|n} \varphi(d)$

Application 14
Soient $(z_1, \ldots, z_n) \in \mathbb{C}^n$ les affixes des sommets d'un polygone P pris dans cet ordre. On définit par récurrence une suite de polygones (P_k) par $P_0 = P$ et, pour tout $k \geq 0$, les sommets de P_{k+1} sont les milieux des arêtes de P_k, c'est-à-dire

$$z_i^{(k+1)} = \frac{z_i^{(k)} + z_{i+1}^{(k)}}{2}, \qquad 1 \leq i \leq n,$$

avec la convention $z_{n+1}^{(k)} = z_1^{(k)}$. Alors la suite (P_k) converge vers l'isobarycentre du polygone P, donné par

$$G = \frac{1}{n}\sum_{i=1}^{n} z_i.$$

II. Angles orientés et argument [Tauvel Analyse complexe pour la licence p. 58 et p. 62]

II.A. Angles orientés et rotation du plan

Définition 15

On définit :
- la rotation autour de 0 d'angle θ : $r_\theta : \mathbb{C} \to \mathbb{C}, z \mapsto ze^{i\theta}$
- la rotation autour de $a \in \mathbb{C}$ d'angle θ, $r_{\theta,a} : \mathbb{C} \to \mathbb{C}, z \mapsto a + r_\theta(z-a)$

Proposition 16

Les rotations sont des isométries, en particulier $\mathbb{U}$ est stable par toute rotation autour de 0.

Application 17

Les rotations du plan préservant un polygone régulier à n côtés de centre O est un groupe constitué des n rotations de centre O et d'angle $\frac{2k\pi}{n}$ pour $k \in [\![0, n-1]\!]$. Autrement dit c'est,$\{z \mapsto z\omega | \omega \in \mathbb{U}_n\}$.

Remarque 18

Si l'on rajoute les n symétries d'axe 2 sommets ou 2 milieux de côtés opposés si n est pair, 1 sommet et le milieu du côté opposé si n est impair, on obtient le groupe des isométries du plan préservant le polygone régulier à n côtés : c'est le groupe diédral D_{2n}.

II.B. Argument continu et logarithme continu sur les ouverts de $\mathbb{C}^*$

Définition 19

Soit Ω un ouvert de $\mathbb{C}^*$.

1. Un argument continu sur Ω est une application continue $\Theta : \Omega \to \mathbb{R}$ telle que $\forall z \in \Omega$, $\frac{z}{|z|} = \mathcal{E} \circ \Theta(z)$
2. un logarithme continu sur Ω est une application continue $l : \Omega \to \mathbb{C}$ telle que $\forall z \in \Omega, z = \exp(l(z))$

Proposition 20

Soit $\Omega = \mathbb{C} \setminus \mathbb{R}_-$.
- Il existe un argument continu Θ sur Ω. Si on suppose en plus que Θ est à valeurs dans $]-\pi, \pi[$, on a alors unicité et on appelle Θ la détermination principale de l'argument,
- Il existe un logarithme continu sur Ω

Proposition 21

Soit Ω un ouvert connexe de $\mathbb{C}$ et $l : \Omega \to \mathbb{C}$.

$$\exists C \in \mathbb{C} \text{ tel que } \ C + l \text{ est un logarithme continu sur } \Omega \iff l \text{ est une primitive de } \ z \to \frac{1}{z} \text{ sur } \Omega$$

En particulier, tout logarithme continu sur Ω est holomorphe.

III. Polynômes cyclotomiques [Perrin]

III.A. Définitions et propriétés

Soit $n \in \mathbb{N}^*$

Définition 22

On définit le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\xi \in \mathbb{U}_n^\times} (X - \xi)$

Proposition 23

1. Φ_n est unitaire de degré $\varphi(n)$
2. $X^n - 1 = \prod_{d|n} \Phi_d(X)$. En particulier si n est premier, $\Phi_n = \frac{X^n-1}{X-1} = \sum_{k=0}^{n-1} X^k$.

Proposition 24

$\Phi_n \in \mathbb{Z}[X]$

Théorème 25

Φ_n est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$

Corollaire 26

$[\mathbb{Q}(e^{2i\pi/n}) : \mathbb{Q}] = \varphi(n)$

III.B. Applications [Gourdon + Francinou Algèbre 1]

Théorème 27 – Kronecker

Soit $P \in \mathbb{Z}[X]$ unitaire avec $P(0) \neq 0$, si toutes les racines de P sont de module inférieur ou égal à 1, ce sont des racines de l'unité.

Corollaire 28

Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$. Si toutes les racines de P sont de module inférieur ou égal à 1, alors $P = X$ ou $P = \Phi_k$ pour un certain $k \in \mathbb{N}^*$.

IV. Autres applications

IV.A. Transformée de Fourier discrète et interpolation polynômiale [G. PEYRÉ fourier discrète+ Algèbre et calcul formel Foissy, L'oral à l'agrégation de math Isenmann-Pecate]

Proposition 29

L'application

$$\mathrm{DFT}_\omega : K[X]/(X^n - 1) \longrightarrow K^n$$

est un isomorphisme. Dans la base

$$\{1, X, \ldots, X^{n-1}\}$$

à la source et la base canonique au but, sa matrice est la matrice de Vandermonde :

$$V_\omega = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)^2} \end{pmatrix}.$$

La matrice de l'isomorphisme inverse est $\frac{1}{n} V_{\omega^{-1}}$.

Application 30

La multiplication de deux polynômes de degré N se fait en $\mathcal{O}(Nln(N))$.

Références :

— Gourdon Analyse,

— Francinou Algèbre 1,

— Perrin,

— G.Peyré Algèbre discrète Fourier,

— Rombaldi Algèbre,

— Tauvel Analyse complexe L3

— Algèbre et calcul formel Foissy Ninet

— L'oral à l'agrégation de mathématiques Isenmann Pecatte

— Arnaudiès Cours de mathématiques 1
— Saux Picard

Table des matières

I De l'exponentielle complexe au groupe $\mathbb{U}$ [Arnaudiès Cours de mathématiques Tome 1 p. 247] **1**

I.A Autour de l'exponentielle 1

I.B. Le groupe des nombres complexes de module 1 et racine $n$ième de l'unité 1

II. Angles orientés et argument **2**

II.A. Angles orientés et rotation du plan 2

II.B. Argument continu et logarithme continu sur les ouverts de $\mathbb{C}^*$ 2

III. Polynômes cyclotomiques **2**

III.A. Définitions et propriétés 2

III.B. Applications 2

IV. Autres applications **2**

IV.A. Transformée de Fourier discrète et interpolation polynômiale 2

Leçon n° 103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.

Piroutet Alban

28 juillet 2026

Soit G un groupe et H un sous-groupe de G.

I Définitions et premières propriétés

I.A) Classe à gauche [Perrin, Rombaldi]

Définition 1

On appelle classe à gauche de $a \in G$ relativement à H le sous-ensemble $aH = \{ah, h \in H\}$. On définit de même la classe à droite de a relativement à H. Les classes à gauche forment une partition de G. Leur ensemble est noté G/H. Ce n'est pas un groupe en général. On appelle indice de H le cardinal de G/H.

Théorème 2 – Théorème de Lagrange

Soit H un sous-groupe du groupe fini G, l'ordre de H et l'indice de H divise l'ordre de G. Plus précisément, on a

$$|G| = |H| \times |G/H|$$

I.B) Sous-groupe distingué [Rombaldi]

Définition 3

Un sous-groupe H de G est dit distingué si et seulement si $\forall g \in G, gH = Hg$.

Proposition 4

$H \triangleleft G \iff \forall g \in G, gHg^{-1} = H$.

Définition 5

On considère l'action de G sur lui-même par conjugaison : $\forall g, x \in G, g.x = gxg^{-1}$

Remarque 6

Un sous-groupe distingué est alors stable par l'action de conjugaison.

Théorème 7

Si G, G' sont deux groupes et φ un morphisme de groupes de G dans G'. Alors $\ker(\varphi) \triangleleft G$.

Remarque 8

Dans un groupe abélien, tous les sous-groupes sont distingués. La réciproque est fausse avec le groupe des quaternions.

Définition 9

On appelle classe de conjugaison les orbites de l'action par conjugaison. En particulier deux éléments sont conjugués s'ils appartiennent à la même classe de conjugaison.

Proposition 10

$H \triangleleft G \iff H$ est réunion de classes de ses classes de conjugaison.

Proposition 11

Soit H un sous-groupe d'indice de 2 de G alors $H \triangleleft G$.

Définition 12

On appelle centre de G l'ensemble $\mathcal{Z}(G) = \{g \in G | \forall \tilde{g} \in G, g\tilde{g} = \tilde{g}g\}$.

Proposition 13

$\mathcal{Z}(G) \triangleleft G$

Théorème 14

Un sous-groupe H de G est distingué si, et seulement si, il existe une unique structure de groupe sur l'ensemble quotient G/H des classes à gauche modulo H telle que la surjection canonique $\pi_H : G \to G/H$ soit un morphisme de groupes.

Définition 15

$\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes modulo n est un groupe quotient.

Proposition 16 – Principe de transport

Soit $g \in G$ alors pour tout $h \in G$, $o(hgh^{-1}) = o(g)$

Remarque 17

L'idée derrière la conjugaison est de transformer un élément un autre qui est plus simple et conserve les mêmes propriétés.

I.C. Liens avec d'autres sous-groupes [Rombaldi]

Définition 18

Un sous-groupe H de G est dit caractéristique s'il est stable par tout automorphisme de G. On note $H \blacktriangleleft G$.

Proposition 19

On a $H \blacktriangleleft G \implies H \triangleleft G$.

Définition 20

Soient $g, h \in G$, on appelle commutateur de g et h, l'élément $[g, h] = ghg^{-1}h^{-1}$. On appelle groupe dérivé de G le sous-groupe engendré par les commutateurs de G. On le note $D(G)$.

Proposition 21

Soit G un groupe, alors $\mathcal{Z}(G) \blacktriangleleft G$ et $D(G) \blacktriangleleft G$.

Proposition 22

$G/D(G)$ est abélien, c'est le plus petit sous-groupe distingué de G pour lequel le groupe quotient est abélien.

Proposition 23

Si $K < H < G$ avec $K \triangleleft G$ alors $K \triangleleft H$.

Proposition 24

Soit φ un morphisme de groupes. L'image d'un sous-groupe distingué H est toujours distingué dans $\varphi(G)$. L'image réciproque d'un sous-groupe distingué H' est un sous-groupe distingué de G.

I.D. Passage au quotient [Ulmer, Perrin]

Théorème 25 – Premier théorème d'isomorphisme

Si G, G' sont deux groupes et $\varphi : G \to G'$ un morphisme de groupes, il existe alors un unique isomorphisme de groupe $\overline{\varphi} : G/\ker(\varphi) \to \mathrm{Im}(\varphi)$ tel que $\varphi = i \circ \overline{\varphi} \circ \pi$ où $i : \mathrm{Im}(\varphi) \to G'$ l'injection canonique.

Théorème 26

Soit G un groupe cyclique d'ordre n alors $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Exemple 27

$\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$.

Proposition 28

$|\mathcal{A}_n| = \frac{n!}{2}$

II.Utilisation des sous-groupes distingués

II.A. Groupes simples [Rombaldi]

Définition 29

Un groupe simple est un groupe dont les groupes distingués sont triviaux.

Proposition 30

Soit G un groupe cyclique d'ordre n, G est simple $\iff$ n est premier.

Théorème 31

Pour $n \geq 5, \mathcal{A}_n$ est simple.

II.B. Théorèmes de Sylow [Perrin]

Soit p un nombre premier diviseur de n. On notera $n = p^\alpha m$ avec $p \nmid m$.

Définition 32

Si n est une puissance de p ($m = 1$), on dit que G est un p-groupe.

Plus généralement, on appelle p-Sylow de G tout sous-groupe de G de cardinal p^α.

Application 33

Ainsi si G est un p-groupe alors son centre n'est pas trivial.

Théorème 34 – Théorème de Sylow 1

Il existe au moins un p-Sylow dans G

Corollaire 35

Il existe au moins un sous-groupe de G d'ordre p^i pour $i \in [\![1, \alpha]\!]$.

Théorème 36 – Théorème de Sylow 2

- Si $H < G$ est un p-groupe, alors il existe un p-Sylow tel que $H < S$,
- Les p-Sylow sont tous conjugués,
- Si on note n_p le nombre de p-Sylow de G, on a $n_p | m$ et $n_p \equiv 1 \mod p$.

Corollaire 37

Soit S un p-Sylow de G. Alors $S \triangleleft G \iff S$ est l'unique p-Sylow de G.

II.C. Le groupe linéaire [Rombaldi]

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n.

Définition 38

On note $\mathcal{GL}(E)$ l'ensemble des automorphismes de E et $\mathcal{SL}(E)$ l'ensemble des automorphismes de E de déterminant égal à 1.

Proposition 39

$\mathcal{SL}(E) \triangleleft \mathcal{GL}(E)$

Proposition 40

On a $\mathcal{Z}(\mathcal{GL}(E)) = \{\lambda Id, \lambda \in \mathbb{K}\}$ et $\mathcal{Z}(\mathcal{SL}(E)) = \{\lambda Id, \lambda^n = 1\}$.

Proposition 41

Les transvections engendrent $\mathcal{SL}(E)$ et sont conjugués deux à deux dans $\mathcal{SL}(E)$ pour $n \geq 3$.

Définition 42

Pour D une droite vectorielle de $\mathbb{R}^3$, on appelle retournement par rapport à la droite D l'élément de $SO_3(\mathbb{R})$ valant l'identité sur D et $-Id$ sur $D^\perp$.

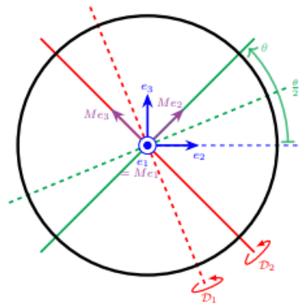
Lemme 43

Soit $M \in O_3(\mathbb{R})$, on a pour toute droite vectorielle $\mathcal{D}$, on a : $M\rho_D\ {}^tM = \rho_{M(\mathcal{D})}$

Proposition 44

Les retournements engendrent $SO_3(\mathbb{R})$

La sphère unité $\mathbb{S}^2$ de $\mathbb{R}^3$ vue "du dessus" ; l'axe de rotation $\mathbb{R}e_1$ pointe vers le lecteur.



(Dans le plan orthogonal à l'axe de rotation [i.e. le plan de la feuille], les droites pleines verte et rouge sont perpendiculaires, de même que les droites en pointillés verte et rouge.)

Figure 1 – Visualiser une rotation $M \in \mathrm{SO}(3)$ comme produit $\rho_{\mathcal{D}_2} \times \rho_{\mathcal{D}_1}$ de deux retournements.

Proposition 45

Les retournements sont deux à deux conjugués entre eux dans $SO_3(\mathbb{R})$.

Théorème 46

$SO_3(\mathbb{R})$ est simple.

III. Etude de quelques classes de conjugaison [Ulmer, Rombaldi, Mansuy]

Remarque 47
Principe de conjugaison de Perrin : un élément conjugué est du même type qu'un élément de départ.

Théorème 48
Décomposition des éléments de $\mathfrak{S}_n$

Définition 49
Type d'une permutation

Exemple 50
On considère $\sigma = (1\ 2\ 4)(3\ 5) \in \mathfrak{S}_6$ est de type $[1, 2, 3]$

Proposition 51
Deux permutations sont conjuguées si et seulement si elles ont mêmem type.

Théorème 52 – Réduction de Frobenius

Proposition 53
Deux endomorphismes sont conjugués si et seulement si ils ont même facteurs invariants

Théorème 54
Deux matrices sont conjuguées si et seulement si elles ont même rang.

Références :

— Perrin Algèbre,

— Rombaldi Algèbre,

— S. LANG : Algèbre. Dunod,

— Nouvelles histoires hédonistes,

— Carnet de voyage en Algébrie,

— Francinou Cassini 3 Algèbre

— Ulmer Théorie des groupes

— Mansuy

PLAN

Table des matières

I Définitions et premières propriétés **1**
I.A Classe à gauche [Perrin, Rombaldi] . . . 1
I.B Sous-groupe distingué [Rombaldi] . . . 1
I.C.Liens avec d'autres groupes . . . 1
I.D. Passage au quotient . . . 2

II.Utilisation des sous-groupes distingués **2**
II.A. Groupes simples . . . 2
II.B. Théorèmes de Sylow . . . 2
II.C. Le groupe linéaire . . . 2

III. Etude de quelques classes de conjugaison **3**

Leçon n° 104 : GROUPES FINIS. EXEMPLES ET APPLICATIONS.

Piroutet Alban

28 juillet 2026

I Généralités et outils des groupes finis

I.A) Vocabulaire des groupes finis [Perrin]

Définition 1 – Groupes, sous-groupes, morphismes de groupes

1. groupe engendré par une partie, par un élément + écriture explicite
2. définition de l'ordre d'un élément

Exemple 2

$\mathbb{Z}/n\mathbb{Z}, \mathfrak{S}_n$ sont des groupes finis. L'ordre de $\overline{1}$ est n et l'ordre de $(a_1 \ \dots \ a_l)$ est l.

Soit G un groupe fini d'ordre n.

Définition 3 – Classe à gauche

Pour $H < G$, on définit $G/H = \{gH, g \in G\}$ l'ensemble des classes à gauche modulo H. On note $[G : H] = |G/H|$.

Théorème 4 – Théorème de Lagrange

L'ordre de tout sous-groupe de G divise n. En particulier, l'ordre de tout élément de G divise n.

Définition 5

$H < G$ est dit distingué si pour tout $g \in G, gH = Hg$. Dans ce cas, on note alors $H \triangleleft G$ et on remarque que G/H est muni naturellement d'une structure de groupe.
G est dit simple, si ses sous-groupes distingués sont triviaux.

Exemple 6

Si $[G : H] = 2$ alors H est distingué dans G.

Définition 7 – Groupe cyclique

G est dit cyclique si $G =< g >$ pour un $g \in G$.

Remarque 8

Un groupe cyclique est abélien.

Exemple 9

Le groupe $\mathbb{U}_n$ des racines n ièmes de l'unité est cyclique d'ordre n et c'est le seul de $\mathbb{C}$.

I.B. Actions de groupes [Perrin]

Définition 10 – Action de groupe sur un ensemble, vocabulaire

On dit que G opère à gauche sur X si on a une application $G \times X \to X, (g, x) \mapsto g.x$ telle que $\forall g, h \in G, \forall x \in X, g.(h.x) = (gh).x$ et $\forall x \in X, 1.x = x$.
Pour $x \in X$, on appelle orbite de x et on note $O(x)$ l'ensemble $G.x = g.x | x \in X$. On note O l'ensemble des orbites de X. C'est une partition de X.
On appelle stabilisateur de $x \in X$ le groupe $\mathrm{Stab}(x) = \{g \in G | g.x = x\}$. Pour $g \in G$, on note $\mathrm{Fix}(g) = \{x \in X | g.x = x\}$.

Remarque 11

G opère sur lui-même par conjugaison : $g.h = ghg^{-1}$. On note $\mathrm{Int}(G) = \{\mathrm{Int}(g), g \in G\}$ l'ensemble des automorphismes intérieurs de G, où $\mathrm{Int}(g) : h \mapsto ghg^{-1}$. On remarque alors que G agit sur tout sous-groupe distingué H de G par cette opération.

Dans la suite de cette partie, on suppose que X est fini.

Corollaire 12 – Equations aux classes

Si $|G| < +\infty$, choisissons pour chaque orbite O un représentant x_O. Alors on a $|X| = \sum_{O \in \mathcal{O}} \frac{|G|}{|\mathrm{Stab}(x_O)|}$

Application 13

Tout groupe d'ordre p^2 est abélien.

Application 14

Notons $X^G = \{x \in X | \forall g \in G, g.x = x\} = \{x \in X | \mathrm{Fix}(x) = G\}$. Alors si G est un groupe d'ordre p^k où p est premier et $k > 1$, on a $|X^G| \equiv |X| \mod p$. Cela permet de prouver le théorème suivant :

Théorème 15 – Théorème de Cauchy

Soit G un groupe fini et p un diviseur premier de l'ordre de G. Alors G admet au moins un élément d'ordre p.

Exemple 16

G agit par conjugaison sur lui-même, notons $Z_h(G) = \{ g \in G \mid ghg^{-1} = h \}$.
Alors $|G| = |Z(G)| + \sum_{\substack{O \in \mathcal{O} \\ |O| \geq 2}} \frac{|G|}{|Z_{x_O}(G)|}$.

Application 17

Le centre d'un groupe d'ordre p^k où p est premier et $k \geq 1$ est non trivial.

I.C. Sous-groupe de Sylow

[Perrin]
Soit p un nombre premier diviseur de n. On notera $n = p^\alpha m$ avec $p \nmid m$.

Définition 18

Si n est une puissance de p ($m = 1$), on dit que G est un p-groupe.

Plus généralement, on appelle p-Sylow de G tout sous-groupe de G de cardinal p^α.

Application 19

Ainsi si G est un p-groupe alors son centre n'est pas trivial.

Corollaire 21

Il existe au moins un sous-groupe de G d'ordre p^i pour $i \in [\![1, \alpha]\!]$.

Théorème 22 – Théorème de Sylow 2

- Si $H < G$ est un p-groupe, alors il existe un p-Sylow tel que $H < S$,
- Les p-Sylow sont tous conjugués,
- Si on note n_p le nombre de p-Sylow de G, on a $n_p | m$ et $n_p \equiv 1 \mod p$.

Corollaire 23

Soit S un p-Sylow de G. Alors $S \lhd G \iff S$ est l'unique p-Sylow de G.

Application 24

Tout groupe d'ordre 63 n'est pas simple.

I.B) Quelques calculs de cardinaux

Proposition 25

$GL_n(\mathbb{F}_p), SL_n(\mathbb{F}_p)$

II. Exemples fondamentaux

Soit $n \in \mathbb{N}^*$ et p un entier premier.

II.A. Le groupe $\mathbb{Z}/n\mathbb{Z}$ [Rombaldi]

Définition 26

En remarquant que $n\mathbb{Z}$ est distingué dans $\mathbb{Z}$, on définit le groupe quotient $\mathbb{Z}/n\mathbb{Z}$.

Proposition 27

$\mathbb{Z}/n\mathbb{Z}$ est cyclique et engendré par les $\overline{d}$ tels que $d \wedge n = 1$. On note $\varphi(n)$ le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$ (indicatrice d'Euler).

Proposition 28

$\mathbb{Z}/n\mathbb{Z}$ est un corps $\iff$ n est premier $\iff$ $\mathbb{Z}/n\mathbb{Z}$ est intègre.

Proposition 29

Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Proposition 30

On a $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. En particulier, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est abélien de cardinal $\varphi(n)$.
De plus $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

Théorème 31 – Théorème des restes chinois

Remarque 32

C'est faux si les entiers ne sont pas premiers entre eux. $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

Théorème 20 – Théorème de Sylow 1

Il existe au moins un p-Sylow dans G

II.B. Le groupe $\mathfrak{S}_n$ [Rombaldi]

Définition 33

On note $\mathfrak{S}_n$ le groupe des permutations de $[\![1, n]\!]$.

Théorème 34 – Théorème de Cayley

Si G est d'ordre n alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Proposition 35

Les familles suivantes engendrent $\mathfrak{S}_n$:

1. les transpositions $((i\ j))_{1 \le i < j \le n}$
2. les transpositions $((1\ i))_{2 \le i \le n}$
3. les transpositions $((i\ i+1))_{1 \le i < n}$
4. la transposition $(1\ 2)$ et le cycle $(1\ 2\ \dots\ n)$

Proposition 36

Toute permutation σ de $\mathfrak{S}_n$ se décompose en un produit de cycles à supports disjoints. Ce produit est unique à l'ordre des cycles près. En particulier, la suite $(l_1, l_2, ..., l_m)$ des longueurs des cycles est unique si on impose $l_1 \ge l_2 \ge \cdots \ge l_m$. On appelle cette suite le type de σ.

Proposition 37

Deux permutations sont conjuguées si et seulement si, elles ont même type.

Proposition 38

Il existe deux morphismes de $\mathfrak{S}_n$ dans $\mathbb{C}^\times$: l'identité et le morphisme signature $\mathcal{E}$ qui envoie toute transposition sur -1.

Proposition 39

Calcul de la signature d'une permutation.

Définition 40

On définit le groupe alterné $\mathfrak{U}_n$ le noyau de $\mathcal{E}$.

Proposition 41

Pour $n \ge 5, \mathfrak{U}_n$ est simple.

III. Applications

III.A. Classification des groupes finis [Rombaldi]

Théorème 42

Supposons G abélien fini d'ordre n. Alors il existe un unique entier ℓ et une unique suite

$$d_1 \ge d_2 \ge \cdots \ge d_\ell$$

d'entiers supérieurs ou égaux à 2 tels que $d_{i+1} \mid d_i$ pour tout $i \le \ell - 1$, et $G \simeq \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$.

Application 43

Tout sous-groupe fini d'un corps commutatif est cyclique.

III.B. En géométrie[H2G2 TOME PREMIER, Carnet de voyage en Algébrie]

Théorème 44

Les isométries du cube sont :

$$Iso^+(\mathcal{C}) \simeq \mathfrak{S}_4 \text{ et } Iso(\mathcal{C}) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$$

Application 45

Il existe 57 manières de colorier un cube avec au plus 3 couleurs.

Références :

— Perrin,

— Rombaldi Algèbre 2EME EDITION,

— Felix Ulmer,

— Carnet de voyage en Algébrie,

— Histoires hédonistes des groupes et de géométries TOME PREMIER

Table des matières

I Généralités et outils des groupes finis **1**
I.A Vocabulaire des groupes finis [Perrin] . . . 1
I.B. Actions de groupes . . . 1
I.C. Sous-groupe de Sylow . . . 1
I.B Quelques calculs de cardinaux . . . 2

II. Exemples fondamentaux **2**
II.A. Le groupe $\mathbb{Z}/n\mathbb{Z}$ . . . 2
II.B. Le groupe $\mathfrak{S}_n$ . . . 2

III. Applications **2**
III.A. Classification des groupes finis . . . 2
III.B. En géométrie . . . 3

105. GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI. APPLICATIONS

Lever Hugo, Piroutet Alban

Agrégation de Mathématiques — 2025

Soit E un ensemble fini de cardinal $n \in \mathbf{N}^*$

Définition 1

On note $\mathfrak{S}(E)$ le groupe des permutations de E. Il est fini de cardinal $n!$. On note $\mathfrak{S}_n = \mathfrak{S}(\llbracket 1, n \rrbracket)$. Pour $\sigma \in \mathfrak{S}_n$, on note

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Proposition 2

$\mathfrak{S}(E) \simeq \mathfrak{S}_n$

Remarque 3

Dans la suite on étudira seulement $\mathfrak{S}_n$

Théorème 4 – Théorème de Cayley

Si G est un groupe fini de cardinal n, G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

I Le groupe $\mathfrak{S}_n$: éléments et générateurs

I.A) Orbites et cycles [Rombaldi]

On considère l'action naturelle de $\mathfrak{S}_n$ sur $\{1, \dots, n\}$: $(\sigma, k) \longmapsto \sigma(k)$.
Soient $\sigma \in \mathfrak{S}_n$ et $k \in \{1, \dots, n\}$ fixés. On note

$$O_\sigma(k) = \{\, \sigma^q(k) \mid q \in \mathbb{Z} \,\}$$

l'orbite de k par l'action restreinte à $\langle \sigma \rangle$.

Définition 5

On appelle support d'une permutation : $Supp(\sigma) = \{x \in \llbracket 1, n \rrbracket, \sigma(x) \neq x\}$

Définition 6

On dit que $\sigma \in \mathfrak{S}_n$ est un ℓ-*cycle* s'il n'y a qu'une unique orbite non ponctuelle et que celle-ci est de cardinal ℓ.
On note alors

$$\sigma = (\, x \;\; \sigma(x) \;\; \dots \;\; \sigma^{\ell-1}(x) \,)$$

où x est un élément de l'orbite non ponctuelle.

Lorsque $\ell = 2$, on parle d'une *transposition*.

Exemple 7

Considérons

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 6 & 1 & 3 \end{pmatrix} \qquad \text{et} \qquad c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}.$$

On a

$$O_\sigma(1) = \{1, 5\}, \quad O_\sigma(2) = \{2\}, \quad O_\sigma(3) = \{3, 4, 6\}.$$

Ainsi σ n'est pas un cycle mais un produit de deux cycles :

$$\sigma = (1\ 5)(3\ 4\ 6).$$

De plus,

$$c = (1\ 5\ 3)$$

est un 3-cycle.

Proposition 8

- Un ℓ-cycle est d'ordre ℓ.
- Deux cycles à supports disjoints commutent.
- Pour $\sigma \in \mathfrak{S}_n$, on a

$$\sigma \circ (i_1\ i_2\ \dots\ i_\ell) \circ \sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \dots\ \sigma(i_\ell)).$$

Théorème 9 – Théorème de Cauchy

Si p est un diviseur premier de n, alors il existe un élément d'ordre p dans G.

I.B. Générateurs et classes de conjugaison [Rombaldi]

Proposition 10

Toute permutation de $\mathfrak{S}_n$ se décompose en un produit de (au plus $n-1$) transpositions.

Application 11

Les familles suivantes engendrent $\mathfrak{S}_n$:

i) Les transpositions $(1i)_{2 \leq i \leq n}$
ii) Les transpositions $(i \;\; i+1)$
iii) (12) et le cycle $(1\,2 \dots n)$

Proposition 12

Deux permutations de $\mathfrak{S}_n$ sont conjugués si et seulement si elles ont le même type.

Exemple 13

Décompose une permutation en produit de cycles à support disjoints.

Application 14

Le nombre de classes de conjugaison est égal au nombre de partition de l'entier n.

Proposition 15

L'ordre d'une permutation est égal au PPCM de son type.

Théorème 16

Pour $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont intérieurs.

II. Autour du groupe alterné

II.A. Signature et groupe alterné [Rombaldi]

Proposition 17

Il existe deux morphismes de $\mathfrak{S}_n$ dans $\mathbf{C}^*$: l'identité et le morphisme ε qui envoie toute transposition sur -1.

Définition 18

On appelle ε l'application signature. On définit le groupe alterné $\mathfrak{U}_n = \ker \varepsilon$.

Proposition 19

- ε est à valeurs dans $\{\pm 1\}$
- la signature d'une l-cycle vaut $(-1)^{l+1}$

Proposition 20

$\mathfrak{U}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$ de cardinal $\frac{n!}{2}$

Théorème 21

Pour $n \geq 5$, $\mathfrak{U}_\mathfrak{n}$ est simple.

II.B. Applications à l'étude des sous-groupes de $\mathfrak{S}_n$ [Rombaldi]

Corollaire 22

Pour $n \geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{Id\}; \mathfrak{U}_n$ et $\mathfrak{S}_n$.

Proposition 23

- Pour $n \geq 3$, $Z(\mathfrak{S}_n) = \{Id\}$
- Pour $n \geq 4$, $Z(\mathfrak{U}_n) = \{Id\}$

Proposition 24

- $D(\mathfrak{S}_n) = \mathfrak{U}_n$
- Pour $n \geq 5$, $D(\mathfrak{U}_n) = \mathfrak{U}_n$

III. Applications du groupe symétrique

III.A. Dérangements [Rombaldi]

Définition 25

Pour $n \in \mathbb{N}^*$, on appelle dérangement de n une permutation de $[\![1, n]\!]$ sans point fixe. On note alors d_n le nombre de dérangement de d_n.

Proposition 26

On a $d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$ (faire avec la formule du crible)

Application 27

Le nombre de permutations de $\mathfrak{S}_n$ ayant exactement r points fixes est

$$\binom{n}{r} d_{n-r} = \frac{n!}{r!} \sum_{k=0}^{n-r} \frac{(-1)^k}{k!}.$$

III.B. Déterminant [Gourdon]

Soient $\mathbb{K}$ un corps et E un $\mathbb{K}$-espace vectoriel de dimension.

Théorème 28

L'ensemble $\Lambda^n(E)$ des formes n-linéaires alternées sur E est un espace vectoriel de dimension 1.
Il existe une unique forme n-linéaire alternée égale à 1 sur une base donnée B.

Définition 29

Soit $\mathcal{B}$ une base de E. On appelle déterminant dans la base $\mathcal{B}$, et on note $\det_\mathcal{B}$, l'unique forme n-linéaire alternée égale à 1 sur $\mathcal{B}$. On appelle déterminant de $A \in \mathcal{M}_n(\mathbb{K})$le déterminant des vecteurs colonnes de A dans la base canonique de $\mathbb{K}^n$. On le note $\det(A)$.

Proposition 30

Soient $x_1, \ldots, x_n$ des vecteurs de E. En notant $(x_{i,1}, \ldots, x_{i,n})$ les coordonnées de x_i dans la base $\mathcal{B}$ de E, on a :

$$\det_\mathcal{B}(x_1, \ldots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \mathcal{E}(\sigma) x_{1,\sigma(1)} \times \cdots \times x_{n,\sigma(n)}$$

III.C. Matrices de permutations [Rombaldi]

Soit $\mathbb{K}$ un corps commutatif.

Définition 31

Pour $\sigma \in \mathfrak{S}_n$, on appelle matrice de permutation associée à σ la matrice P_σ définie par : $P_\sigma = (\delta_{i,\sigma(j)})_{1 \leq i,j \leq n}$

Exemple 32

$P_{Id} = I_n$

Théorème 33

L'application $P : \mathfrak{S}_n \longrightarrow \mathcal{GL}_n(K), \quad \sigma \longmapsto P_\sigma$ est un morphisme de groupe injectif et on a $\det(P_\sigma) = \mathcal{E}(\sigma)$.

III.D. Polynômes symétriques [Rombaldi]

Soit $\mathbb{K}$ un corps de caractéristique différente de 2.

Définition 34

On dit que $P \in \mathbb{K}[X_1, \ldots, X_n]$ est **symétrique** si :

$$\forall \sigma \in \mathfrak{S}_n, \quad P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n).$$

Exemple 35

Les polynômes

$$\Sigma_{k,n} = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} X_{i_1} X_{i_2} \cdots X_{i_k} \quad (0 \leq k \leq n)$$

sont des polynômes symétriques, appelés **polynômes symétriques élémentaires**.

Théorème 36

Soit $P \in \mathbb{K}[X_1, \ldots, X_n]$ un polynôme symétrique. Alors il existe un polynôme

$$Q \in \mathbb{K}[X_1, \ldots, X_n]$$

tel que

$$P(X_1, \ldots, X_n) = Q(\Sigma_{1,n}, \Sigma_{2,n}, \ldots, \Sigma_{n,n}).$$

Exemple 37

On considère $P = X^3 + Y^3 + Z^3 \in \mathbb{R}[X, Y, Z]$, on remarque alors que $P = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3$.

III.E. Groupe symétrique et géométrie [Rombaldi, H2G2 tome premier, Carnet de voyage en Algébrie]

Définition 38

Un espace affine $\mathcal{E}$ de direction E est un ensemble non-vide $\mathcal{E}$ sur lequel on peut définir une action simplement transitive.

$$\mathcal{E} \times E \to \mathcal{E}, (x, u) \mapsto x + u$$

Définition 39

On appelle isométrie affine toute application $f : \mathcal{E} \to \mathcal{E}$ qui converse les distances. On note $I_S(\mathcal{E})$ l'ensemble des isométries affines de $\mathcal{E}$.

Proposition 40

L'isobarycentre est conservé par une isométrie (en particulier un potentiel centre de symétrie).

Théorème 41

$$\mathrm{Isom}(C) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}, \qquad \mathrm{Isom}^+(C) \simeq \mathfrak{S}_4.$$

Application 42

Il est possible de colorier un cube de 57 manières différentes avec au plus 3 couleurs.

Références :

— Gourdon Algèbre,

— Rombaldi Algèbre,

— Carnet de voyage en Algébrie,

— H2G2 TOME PREMIER

PLAN :

Table des matières

I Le groupe $\mathfrak{S}_n$: éléments et générateurs **1**
I.A Orbites et cycles [Rombaldi] . . . 1
I.B. Générateurs et classes de conjugaison . . . 1

II. Autour du groupe alterné **2**
II.A. Signature et groupe alterné . . . 2
II.B. Applications à l'étude des sous-groupes de $\mathfrak{S}_n$ . . . 2

III. Applications du groupe symétrique **2**
III.A. Dérangements . . . 2
III.B. Déterminant . . . 2
III.C. Matrices de permutations . . . 2
III.D. Polynômes symétriques . . . 2
III.E. Groupe symétrique et géométrie . . . 3

Leçon n° 106 : Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications.

Piroutet Alban

28 juillet 2026

I Définitions et premières propriétés [Rombaldi]

Soient $\mathbb{K}$ un corps et E un $\mathbb{K}$ espace vectoriel de dimension finie n.

Définition 1
On appelle $\mathcal{L}(E)$ l'ensemble des endomorphismes de E et $\mathcal{GL}(E)$ l'ensemble des automorphismes de E

Proposition 2
Soit $\mathcal{B}$ une base de E, on a alors un isomorphisme de $\mathbb{K}$-algèbres entre $\mathcal{L}(E)$ et $\mathcal{M}_n(\mathbb{K})$ via $u \mapsto Mat_{\mathcal{B}}(u)$.

Remarque 3
Ainsi on se ramène à l'étude de $\mathcal{GL}_n(\mathbb{K})$. On rajoute ainsi un outil au calcul matriciel.

Définition 4
On note Id [resp I_n] l'endomorphisme [resp la matrice] identité.
On appelle homothétie [resp matrice scalaire] tout endomorphisme [resp toute matrice] de la forme λId [resp λI_n] avec $\lambda \in \mathbb{K}$.
On note $\mathrm{diag}(\lambda_1, \dots, \lambda_n)$ la matrice diagonale de termes diagonaux $\lambda_1, \dots, \lambda_n$.
Pour tout $n \in \mathbb{N}^*$, on désigne par $(e_k)_{k\in[\![1,n]\!]}$ la base canonique de $\mathbb{K}^n$ et par $(E_{i,j})_{1\leq i,j\leq n}$ celle de $\mathcal{M}_n(\mathbb{K})$.

Proposition 5
Soit $u \in \mathcal{L}(E)$, on a :

$$u \in \mathcal{GL}(E) \iff u \text{ injective} \iff u \text{ surjective} \iff \det(u) \neq 0 \iff \mathrm{rg}(u) = n$$

Définition 6
On note $\mathcal{SL}(E) = \{u \in \mathcal{GL}(E), \det u = 1\}$. C'est le groupe spécial linéaire. De la même manière on définit $\mathcal{SL}_n(\mathbb{K}) = \{A \in \mathcal{GL}_n(\mathbb{K}), \det A = 1\}$.

Théorème 7
$\mathcal{SL}(E)$ est un sous-groupe distingué de $\mathcal{GL}(E)$ isomorphe à $\mathcal{SL}_n(\mathbb{K})$, le groupe quotient $\mathcal{GL}(E)/\mathcal{SL}(E) \simeq \mathbb{K}^*$.

II. Quelques éléments de $\mathcal{GL}(E)$

I.A) Les hométhéties [Rombaldi, Perrin]

Proposition 8
Soit u une homothétie de rapport λ alors $\det u = \lambda^n$.

Proposition 9
u homothétie $\iff$ elle stabilise toute droite

Définition 10
On appelle centre d'un groupe l'ensemble des éléments qui commutent avec tous les éléments de G. On le note $\mathcal{Z}(G)$.

Proposition 11
On a $\mathcal{Z}(\mathcal{GL}(E)) = \{\lambda Id, \lambda \in \mathbb{K}\}$ et $\mathcal{Z}(\mathcal{SL}(E)) = \mathcal{Z}(\mathcal{GL}(E) \cap \mathcal{SL}(E) = \{\lambda Id, \lambda \in \mathbb{K}, \lambda^n = 1\}$

On cherche déjà des générateurs de $\mathcal{GL}(E)$, on veut les plus simples, donc ayant, comme les transpositions dans le cas de $\mathfrak{S}_n$, le plus de points fixes possibles, c'est à dire ici, un hyperplan.

II.B. Les dilatations [Rombaldi, Perrin]

Proposition 12
Soit H un hyperplan de E et soit $u \in \mathcal{GL}(E)$ tel que $u_{|H} = Id_H$. Les conditions suivantes sont équivalentes :

1. $\det u = \lambda \neq 1$ (i.e $u \notin \mathcal{SL}(E)$)
2. u admet une valeur propre $\lambda \neq 1$ (donc une droite propre D pour λ) et u diagonalisable
3. $Im(u - Id) \not\subset H$
4. dans une base convenable, u a pour matrice $\mathrm{diag}(1, \dots, 1, \lambda)$, avec $\lambda \in \mathbb{K}^*, \lambda \neq 1$

On dit alors que u est une dilatation d'hyperplan H, de droite D et de rapport λ. On a alors $D = Im(u-id), H = \ker(u - id)$. Lorsque $\lambda = -1$ et $\mathrm{car}(\mathbb{K}) \neq 2$, u est appelée une réflexion.

II.C. Les transvections [Rombaldi, Perrin]

Proposition 13
définition

Proposition 14
Comportement par conjugaison

Proposition 15
Les transvections sont conjuguées dans $\mathcal{GL}(E)$ et dans $\mathcal{SL}(E)$ pour $n \geq 3$.

III. Etude du groupe linéaire

III.A. Générateurs [Rombaldi, Perrin, Fleury]

Théorème 16
$\mathcal{SL}_n(\mathbb{K})$ est engendré par les transvections et $\mathcal{GL}_n(\mathbb{K})$ par les transvections et dilatations.

Application 17
Algorithme du pivot de Gauss (cf annexe)

Théorème 18
1. $\mathcal{GL}_n(\mathbb{C})$ et $\mathcal{SL}_n(\mathbb{C})$ sont connexes par arcs,
2. $\mathcal{GL}_n(\mathbb{R})$ n'est pas connexe mais $\mathcal{GL}_n^+(\mathbb{R})$ et $\mathcal{SL}_n(R)$ sont connexes par arcs.

III.B. Commutateurs [Perrin, Rombaldi]

Théorème 19

1. On a $D(\mathcal{GL}_n(\mathbb{K})) = \mathcal{SL}_n(\mathbb{K})$ sauf dans le cas :($n = 2$ et $\mathbb{K} = \mathbb{F}_2$)
2. $D(\mathcal{SL}_n(\mathbb{K})) = \mathcal{SL}_n(\mathbb{K})$ sauf dans le cas :($n = 2$ et $\mathbb{K} = \mathbb{F}_2$) et ($n = 2$ et $\mathbb{K} = \mathbb{F}_3$)

III.C. Quelques calculs de cardinalité [Perrin, Rombaldi]

Théorème 20

Cardinalité de $\mathcal{GL}_n(\mathbb{F}_q), \mathcal{SL}_n(\mathbb{F}_q)$.

III.D. Matrices de permutations [Rombaldi+ Objectif Agreg]

Définition 21

Matrices de permutations

Proposition 22

L'application $P : \sigma \in \mathfrak{S}_n \mapsto P_\sigma \in GL_n(\mathbb{K})$ est un morphisme de groupes injectif. De plus, pour toute permutation $\sigma \in \mathfrak{S}_n$, on a $\det(P_\sigma) = \varepsilon(\sigma)$.

Corollaire 23

Tout groupe fini d'ordre $n \geq 1$ est isomorphe à un sous-groupe de $GL_n(\mathbb{F}_p)$ avec $p \geq 2$ un nombre premier.

IV. Groupes orthogonal et unitaire

On considère E un espace préhilbertien réel.

IV.A. Généralités [Perrin, Rombaldi]

Définition 24

Une isométrie (ou application orthogonale) de E est une application $u : E \to E$ qui conserve le produit scalaire.

Théorème 25

Une application $u : E \to E$ est une isométrie si, et seulement si, elle est linéaire et conserve la norme.

Corollaire 26

$O(E)$ est un sous-groupe de $GL(E)$.

Théorème 27

Caractérisation matricielle.

Proposition 28

Soit $u \in O(E)$ alors $\det(u) = \pm 1$

Définition 29

On définit $O^+(E)$ le sous-groupe des isométries directes de E, i.e. $O^+(E) = \{u \in O(E), \det u = 1\}$

Théorème 30 – Réduction des endomorphismes orthogonaux

Soit $u \in O_n(\mathbb{R})$. Il existe une base orthonormée $\mathcal{B}$ de E telle que

$$M_{\mathcal{B}}(u) = \begin{pmatrix} I_s & & & & \\ & -I_t & & & \\ & & R_1 & & \\ & & & \ddots & \\ & & & & R_r \end{pmatrix}$$

où $s + t + 2r = n$ et, pour $1 \leq k \leq r$,

$$R_k = \begin{pmatrix} \cos(\theta_k) & -\sin(\theta_k) \\ \sin(\theta_k) & \cos(\theta_k) \end{pmatrix}, \qquad \theta_k \not\equiv 0 \pmod{\pi}.$$

Théorème 31

$\mathcal{SO}_3(\mathbb{R})$ est simple

V. Autres résultats

V.A. Action de groupes matriciels [Rombaldi]

Proposition 32

Action $(P, A) \mapsto PA$ et orbites

Proposition 33

Action $(P, A) \mapsto AP^{-1}$ et orbites

Proposition 34

Action de Steinitz (par équivalence) et orbites

V.B. Topologie [Rombaldi, Francinou Algèbre 2]

On se place sur $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Proposition 35

$\mathcal{GL}(E)$ est un ouvert dense dans $\mathcal{L}(E)$.

Proposition 36

$SL(E)$ est fermé.

Proposition 37

$\mathcal{O}_n(\mathbb{R})$ est compact.

Proposition 38

$GL_n(\mathbb{C})$ est connexe.

Annexe

Algorithme du pivot de Gauss à prendre dans le Fleury

Références :

— Perrin Algèbre,

— Nouvelles Histoires hédonistes de groupes et de géométrie,

— Rombaldi Algèbre,

— Oraux X-ens 2 Francinou,

— Objectif Agreg

— Fleury, Foissy Algèbre et calcul formel

Table des matières

I Définitions et premières propriétés [Rombaldi] **1**

II. Quelques éléments de $\mathcal{GL}(E)$ **1**

I.A Les hométhéties [Rombaldi, Perrin] . . . 1

II.B. Les dilatations . . . 1

II.C. Les transvections . . . 1

III. Etude du groupe linéaire **1**

III.A. Générateurs . . . 1

III.B. Commutateurs . . . 2

III.C. Quelques calculs de cardinalité . . . 2

III.D. Matrices de permutations . . . 2

IV. Groupes orthogonal et unitaire **2**

IV.A. Généralités . . . 2

V. Autres résultats **2**

V.A. Action de groupes matriciels . . . 2

V.B. Topologie . . . 2

Leçon n° 108 : EXEMPLES DE PARTIES GÉNÉRATRICES D'UN GROUPE. APPLICATIONS.

Piroutet Alban

Agrégation de Mathématiques — 2025

Soit G un groupe

I Parties génératrices de groupes [Perrin page 9 et page 95],[Rombaldi page 12]

I.A) Définitions

Définition 1
Définition de partie générée par une partie A et partie génératrice.

Définition 2
Groupes de type finie (admet une famille génératrice finie)

Exemple 3
$\mathbb{Z}$ est de type finie, pas $\mathbb{Q}$, tout groupe finie est de type fini.

Définition 4
Groupe dérivé

Proposition 5
Abélianisé

I.B) Groupes monogènes et cycliques, cas de $\mathbb{Z}/n\mathbb{Z}$ [Rombaldi p°13 à 18] [Perrin p°25]

Définition 6
Groupe monogène, cyclique

Proposition 7
Si G est fini d'ordre premier, il est cyclique

Proposition 8
$\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n et ses générateurs sont les $\overline{k}$ où $k \wedge n = 1$.

Corollaire 9
$\mathbb{Z}/n\mathbb{Z}$ possède donc $\varphi(d) = \text{card}(\{k \in [\![1, n]\!], k \wedge n = 1\})$ générateurs d'ordre $\frac{d}{n}$.

Application 10
$n = \sum_{d|n} \varphi(d)$

Proposition 11
Si G est monogène infini, alors $G \simeq \mathbb{Z}$; si G est cyclique, alors $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Proposition 12
Les sous-groupes d'un groupe cyclique sont cycliques

Proposition 13 – Perrin
$(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique $\iff n = 2, 4, p^\alpha, 2p^\alpha$.

I.C. Groupes abéliens de types finis [Rombaldi, Ulmer]

Théorème 14 – Théorème de structure des groupes abéliens de type finis, [Félix Ulmer Théorie des groupes p°107]

Corollaire 15
Théorème de structure des groupes abéliens finis

Application 16
Tout sous-groupe fini d'un corps multiplicatif est cyclique.

Application 17
Détermination à isomorphismes près de tous les groupes abéliens d'ordre donné avec théorème chinois.

II. Cas du groupe symétrique et applications

II.A. Système de générateurs [Rombaldi, Ulmer H2G2]

Théorème 18 – Théorème de décomposition en cycles disjoints des permutations
+ application au calcul de l'ordre d'un élément.

Corollaire 19
Les transpositions engendrent $\mathfrak{S}_n$

Proposition 20
Toute permutation de $\mathfrak{S}_n$ se décompose en produit de au plus $(n-1)$ transpositions.

Exemple de décomposition

Proposition 21
Autres systèmes de générateurs de $\mathfrak{S}_n$ sont $\{(1, k)\}, \{(k, k+1)\}$ et $\{(1, 2), (1\ 2\ \dots\ n)\}$. Il est utile d'avoir un système de générateur de petite taille.

II.B. Cas du groupe alterné [Rombaldi p° 48]

Proposition 22
Existence et unicité du morphisme signature.

Proposition 23
Propriétés du morphisme signature

Application 24
Calcul de la signature d'une permutation

Définition 25
Groupe alterné

Lemme 26
$\mathfrak{A}_n$ est engendré par les 3-cycles et y sont conjugués

Théorème 27
$\mathfrak{A}_n$ est simple pour $n \geq 5$.

Corollaire 28
Les sous-groupes distingués de $\mathfrak{S}_n$ pour $n \geq 5$.

III. Le cas du groupe linéaire et ses sous-groupes [Rombaldi p°139]

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n, où $\mathbb{K}$ est un corps commutatif
Définition du groupe linéaire, de $\mathrm{SL}(E)$. Exemple des homothéties.
On se ramène à l'étude de $\mathcal{GL}_n(\mathbb{K})$ via un isomorphisme, et $\mathcal{GL}_n(K) \simeq \mathcal{GL}(E)$
Proposition : $u \in \mathcal{GL}(E) \iff \ker u = \{0\} \iff \mathrm{Im}(u) = E \iff \det(u) \neq 0$.

III.A. Systèmes de générateurs [Perrin p°95, Rombaldi p°139]

Définition 29
Homothéties

Définition 30
Déterminant

Proposition 31
u homothétie $\iff$ u laisse stable toute droite vectorielle.

Proposition 32
$\mathcal{Z}(\mathcal{GL}(E)) = \{\text{homothétie}\}$ et $\mathcal{Z}(\mathcal{SL}(E))$ est l'ensemble des homothéties de déterminant 1.

Proposition 33

1. $D(\mathcal{GL}_n(\mathbb{K})) = \mathcal{SL}_n(\mathbb{K})$ sauf dans le cas $n = 2$ et $\mathbb{K} = \mathbb{F}_2$.
2. $D(\mathcal{SL}_n(\mathbb{K})) = \mathcal{SL}_n(\mathbb{K})$ sauf dans les deux cas $n = 2, \mathbb{K} = \mathbb{F}_2$ et $n = 2, \mathbb{K} = \mathbb{F}_3$. Pour cela on montre qu'une transvection est un commutateur car ces dernières engendrent le groupe.

Définition 34
Matrices de transvections et dilatations

Proposition 35
Formule de conjugaison

Théorème 36
$\mathrm{SL}_n(\mathbb{K})$ est engendré par les transvections

Corollaire 37
$\mathrm{GL}_n(\mathbb{K})$ est engendré par les transvections et dilatations.

Proposition 38
Deux dilations sont conjuguées dans $\mathcal{GL}(E) \iff$ elles ont même rapport.

Proposition 39
Deux transvections quelconques sont conjuguées dans $\mathcal{GL}(E)$ et pour $n \geq 3$, elles le sont aussi dans $\mathcal{SL}(E)$.

Théorème 40
Implémentation et application de l'algorithme du pivot de Gauss. (cf annexe)

Théorème 41
$\mathrm{SO}_3(\mathbb{R})$ est simple.

III.B. Application en topologie [Francinou Algèbre 2 p. 177, Rombaldi Algèbre]

Théorème 42
$\mathcal{GL}_n(\mathbb{R})$ a deux composantes connexes et $\mathcal{GL}_n(\mathbb{C})$ est connexe est connexe par arcs.

Théorème 43
Pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $\mathcal{SL}_n(\mathbb{K})$ est connexe par arcs.

Annexe

Algorithme du pivot de Gauss

Références :

— Perrin,

— Rombaldi Algèbre,

— Nouvelles H2G2,

— Ulmer groupe

— Francinou Algèbre 2, 3

Table des matières

I Parties génératrices de groupes [Perrin page 9 et page 95],[Rombaldi page 12] **1**

I.A Définitions . . . 1

I.B Groupes monogènes et cycliques, cas de $\mathbb{Z}/n\mathbb{Z}$ [Rombaldi p°13 à 18] [Perrin p°25] . . . 1

I.C. Groupes abéliens de types finis . . . 1

II. Cas du groupe symétrique et applications **1**

II.A. Système de générateurs [Félix Ulmer p°47, Rombaldi p°37] . . . 1

II.B. Cas du groupe alterné . . . 1

III. Le cas du groupe linéaire et ses sous-groupes **2**

III.A. Systèmes de générateurs . . . 2

III.B. Application en topologie . . . 2

Leçon n° 120 :Anneaux Z/nZ. Applications.

Piroutet Alban

Agrégation de Mathématiques — 2025

Soit $n \in \mathbb{N}^*$. On désigne par $\mathcal{P}$ l'ensemble des nombres premiers.

I Structure de $\mathbb{Z}/n\mathbb{Z}$ [Rombaldi p°279]

I.A) Le groupe $\mathbb{Z}/n\mathbb{Z}$

Définition 1

Définition de la relation d'équivalence " être congruo mod n". Et $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence de cette relation.

Proposition 2

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique à n éléments engendré par $\overline{1}$.

Application 3

Tout groupe cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exemple 4

$\mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

Proposition 5

L'ordre de $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est $\frac{n}{n \wedge k}$

Corollaire 6

$(\mathbb{Z}/n\mathbb{Z}, +)$ est engendré par les $\overline{k}$ tels que $k \wedge n = 1$.

Définition 7

Pour $n \geq 2$, on définit $\varphi(n)$ le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$. φ s'appelle l'indicatrice d'Euler.

Exemple 8

Pour $p \in \mathcal{P}$, $\varphi(p^\alpha) = p^\alpha(1 - \frac{1}{p})$ pour $\alpha \in \mathbb{N}^*$.

Proposition 9

Pour $d|n$, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, engendré par $\frac{\overline{n}}{d}$ et formé des éléments dont l'ordre divise d.

Proposition 10

Si $d|n$, $\mathbb{Z}/n\mathbb{Z}$ contient $\varphi(d)$ éléments d'ordre d.

Application 11

$$n = \sum_{d|n} \varphi(d)$$

Théorème 12 – Théorème de structure des groupes abéliens finis

Soit G un groupe abélien fini. Alors il existe $r \geq 1$ et $2 \leq d_1 | \dots | d_r$ uniques tels que $G \simeq \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$

I.B. L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Proposition 13

Les idéaux de $\mathbb{Z}$ sont les $(k\mathbb{Z})_{k\in\mathbb{N}}$

Définition 14

L'ensemble des classes modulo n est muni d'une structure d'anneau : on définit l'anneau commutatif $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Application 15

Soit A un anneau commutatif unitaire. Il existe un unique entier positif, appelé caractéristique de A, noté $car(A)$, tel que le sous-anneau premier de A est isomorphe à $\mathbb{Z}/\text{car}(A)\mathbb{Z}$.

Proposition 16

Les inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{k}$ tels que $k \wedge n = 1$. Ils forment un groupe à $\varphi(n)$ éléments.

Application 17

On a l'isomorphisme $(\text{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ) \simeq ((\mathbb{Z}/n\mathbb{Z})^\times, \times)$

Proposition 18

$\mathbb{Z}/n\mathbb{Z}$ est intègre $\iff$ c'est un corps $\iff$ $n \in \mathcal{P}$.

Théorème 19

Si $n, m \geq 1$, on a $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \iff n \wedge m = 1$.

Corollaire 20

Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, on a $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$. On a donc : $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{r}(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$. D'où

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$$

Théorème 21

Si $p \in \mathcal{P}$, $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$ est cyclique.

II. Application dans différents domaines des mathématiques

II.A. Test de primalité [Rombaldi, Demazure]

Théorème 22 – Théorème D'Euler

Soit $a \in \mathbb{Z}$ premier avec n alors $a^{\varphi(n)} \equiv 1 \mod n$.

Théorème 23 – Petit théorème de Fermat

Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$ tels que $p \nmid a$. Alors $a^{p-1} \equiv 1 \bmod p$.

Remarque 24

Réciproque fausse : Nombre de Carmichael (561)

Application 25

Codage RSA

— Bob choisit deux entiers premiers distincts $p, q \in \mathbb{P}$, et pose $n = pq$.
— Il calcule ensuite $\varphi(n) = (p-1)(q-1)$.
— Bob choisit deux entiers $d, e \in \mathbb{Z}$ tels que

$$de \equiv 1 \pmod{\varphi(n)}.$$

Autrement dit, d et $\varphi(n)$ sont premiers entre eux, et e est l'inverse de d modulo $\varphi(n)$.
— Bob publie la clé publique (n, d) et conserve la clé secrète (n, e).
— Pour envoyer un message m mod n, Alice calcule le message chiffré :

$$M \equiv m^d \pmod{n}.$$

— Pour déchiffrer, Bob calcule :

$$m \equiv M^e \pmod{n}.$$

Par le théorème d'Euler, on a bien $M^e \equiv (m^d)^e \equiv m^{de} \equiv m \pmod{n}$.

Le succès de cet algorithme repose sur la **difficulté de factoriser** un grand entier $n = pq$ en ses deux facteurs premiers.

Théorème 26 – Théorème de Wilson

Si $n \geq 2$, on a $n \in \mathcal{P} \iff (n-1)! \equiv -1 \bmod n$.

Théorème 27 – Test de primalité de Miller-Rabin

Théorème 28 – Test de Solovay-Strassen

II.B. Equations arithmétiques

Théorème 29

Résolution d'équation diophantiennes ie de $ax \equiv b[mod\ n]$

Le théorème des restes chinois nous permet de résoudre des systèmes de congruence

Exemple 30

Résolution du système de congruence

$$\begin{cases} k \equiv 2 \pmod 4, \\ k \equiv 3 \pmod 5 \end{cases}$$

II.C. Application à la théorie des corps [Rombaldi section corps finis]

Proposition 31

Caractéristique et $\mathbb{F}_p$ sous-corps premiers des corps $\mathbb{K}$ de caractéristique p.

Corollaire 32

Les corps finis sont de cardinal une puissance d'un nombre premier.

Proposition 33

Existence et unicité des corps finis + ajout dénombrement

Application 34

Construction de $\mathbb{F}_4 = \mathbb{F}_2[X]/(1 + X + X^2)$

II.D. Etude des carrés de $\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}$

Soit $p \in \mathcal{P}$, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, puis $\mathbb{F}_p^2 = \{x^2, x \in \mathbb{F}_p\}$ et $\mathbb{F}_p^{2*} = \mathbb{F}_p^2 \cap \mathbb{F}_p^*$.

Proposition 35

Si $p = 2$, on a $\mathbb{F}_2^2 = \mathbb{F}_2$. Sinon on a $|\mathbb{F}_p^2| = \frac{p+1}{2}$.

Lemme 36

On a $x \in \mathbb{F}_p^{2*} \iff x^{\frac{p-1}{2}} = 1$

Corollaire 37

-1 est un carré dans $\mathbb{F}_p \iff p \equiv 1[4]$

Théorème 38

Théorème des deux carrés.

On aimerait savoir si un entier a est un carré modulo p (classification des formes quadratiques sur les corps finis)

Définition 39 – Symbole de Legendre

Soit $a \in \mathbb{Z}$. On appelle symbole de Legendre de a mod p l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } a \in \mathbb{F}_p^{2*} \\ 0 \text{ si } p|a \\ -1 \text{ sinon} \end{cases}$$

Proposition 40

On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$

Théorème 41 – Loi de réciprocité quadratique

Soient $p \neq q$ des nombres premiers impairs. Alors :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Théorème 42 – Loi de réciprocité quadratique complémentaires

Soit p un nombre premier impair

—
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

—
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Théorème 43
Classification des formes quadratiques sur les corps finis.

III. Irréductibilité sur $\mathbb{Q}[X]$

Définition 44
Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, $a_n \neq 0$, on appelle contenu de P noté $C(P)$ l'entier $\text{pgcd}(a_i, i \in [\![0, n]\!])$

Proposition 45
Un polynôme de degré supérieur ou égal à 1 est irréductible dans $\mathbb{Z}[X]$ si et seulement si il est de contenu 1 et est irréductible sur $\mathbb{Q}[X]$

Théorème 46 – Critère D'Eisenstein
Soit $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $p \in \mathcal{P}$, si $p \not| a_r$ et $\forall i < r,\ p|a_i$ et $p^2 \not| a_0$. Alors P est irréductible sur $\mathbb{Q}[X]$.

Exemple 47
Si $m \in \mathbb{Z}$ est sans facteur premier carré alors $X^n - m$ est irréductible sur $\mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$.

Proposition 48
Soit $p \in \mathcal{P}$ et $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $\overline{P}$ la réduction de P modulo p. Si $p \nmid a_r$ et si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

Définition 49 – Polynômes cyclotomiques
On définit le $n$ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathcal{U}_n^\times} (X - \zeta)$

Proposition 50
$\Phi_n \in \mathbb{Z}[X]$

Proposition 51
Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.

Corollaire 52
On a $[\mathbb{Q}[e^{\frac{2i\pi}{n}}] : \mathbb{Q}] = \varphi(n)$

Références :
— Perrin,
— Rombaldi,
— Gourdon Algèbre,
— Demaruze Cours d'Algèbre
— H2G2
— Ulmer
— Francinou Algèbre 1
PLAN :

Table des matières

I Structure de $\mathbb{Z}/n\mathbb{Z}$ [Rombaldi p°279] **1**
I.A Le groupe $\mathbb{Z}/n\mathbb{Z}$ . . . 1
I.B. L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ . . . 1

II. Application dans différents domaines des mathématiques $\mathbb{Z}$ **1**
II.A. Test de primalité . . . 1
II.B. Equations arithmétiques . . . 2
II.C. Application à la théorie des corps . . . 2
II.D. Etude des carrés de $\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}$ . . . 2

III. Irréductibilité sur $\mathbb{Q}[X]$ **3**

Références : Gourdon algèbre, Perrin Algèbre, Rombaldi Algèbre, Felix Ulmer Groupe, Zemor cours de crypto

Leçon n° 121 : Nombres premiers. Applications.

Piroutet Alban

28 juillet 2026

On désigne par $\mathcal{P}$ l'ensemble des nombres premiers.

I Généralités et arithmétique dans $\mathbb{Z}$ [Rombaldi, Perrin]

Définition 1 – Entier premier

$p \in \mathbb{N}$ est dit premier (et on note $p \in \mathcal{P}$) s'il admet exactement deux diviseurs positifs 1 et p.

Remarque 2

$(\mathbb{Z}, +, \times)$ est un anneau euclidien donc principal, ses idéaux sont les $(n\mathbb{Z})_{n\in\mathbb{N}}$. Dire que $p \in \mathcal{P}$ revient à demander que $p\mathbb{Z}$ est un maximal.

Exemple 3

Les entiers 2,3,5 sont premiers, en revanche 6=2×3 n'est pas premier.

Définition 4

Deux entiers a et b sont dits premiers entre eux si le plus grand diviseur entier de a et b est 1. Des entiers $(a_i)_{i\in I}$ sont dits premiers dans leur ensemble si le plus grand diviseur entier de chacun des $(a_i)_{i\in I}$ est 1.

Exemple 5

Si $p \in \mathcal{P}$ et $n \in \mathbb{N}$, p et n sont premiers entre eux si et seulement si $p \nmid n$.
$\{6, 10, 15\}$ sont premiers dans leur ensemble bien que $\{6, 10\}, \{6, 15\}$ et $\{10, 15\}$ ne soient pas premiers entre eux.

Application 6

Deux groupes de cardinaux premiers entre eux sont d'intersection triviale.

Lemme 7 – Lemme D'Euclide

Tout entier relatif $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ a au moins un diviseur premier.

Théorème 8 – Décomposition en produit de facteurs premiers

Tout entier naturel $n \geq 2$ se décompose de manière unique sous la forme $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ où $r \in \mathbb{N}^*, p_1 < p_2 < \cdots < p_r \in \mathcal{P}$ et $(\alpha_i)_{1\leq i\leq r} \in (\mathbb{N}^*)^r$.

I.A) Arithmétique [Rombaldi]

Définition 9 – PGCD, PPCM

On définit le PGCD (resp. PPCM) d'une famille d'éléments comme le plus grand diviseur (resp. le plus petit multiple) commun à chacun de ses éléments.

Définition 10 – Valuation p-adique

Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}$, on définit $v_p(n) = \max\{k \in \mathbb{N}, p^k | n\}$

Remarque 11

L'écriture $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ est donc $n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}$

Application 12

Calcul du PGCD et PPCM en fonction de la décomposition en facteurs premiers.

Théorème 13 – Identité de Bézout

Soit $r \geq 2$ et $(a_1, \ldots, a_r)$ des entiers relatifs. Si $\delta = \text{pgcd}((a_i)_{1\leq i\leq r})$, alors il existe des entiers relatifs $u_1, \ldots, u_r$ tels que $\sum_{i=1}^r u_i a_i = \delta$.
Les $(a_i)_{1\leq i\leq r}$ sont premiers entre eux si et seulement si il existe des entiers relatifs $u_1, \ldots, u_r$ tels que $\sum_{i=1}^r u_i a_i = 1$.

Lemme 14 – Lemme de Gauss

Soient $a, b, c \in \mathbb{Z}$.

1. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.
2. Si $a \mid bc$ et $b \wedge c = 1$, alors $a \mid b$ et $a \mid c$.

Application 15

Pour $p \in \mathcal{P}$ et $k \in [\![1, p-1]\!], p | \binom{p}{k}$.

Théorème 16

On définit $\mathbb{Z}[i] = \{a + ib |\ a, b \in \mathbb{Z}\}$. Et on définit $\Sigma = \{n \in \mathbb{N}, \exists (a, b) \in \mathbb{N}^2, n = a^2 + b^2$. Pour $p \in \mathcal{P}$, on a $p \in \Sigma \iff p \equiv 1, 2 \mod 4$

I.B. Répartition des nombres premiers [Rombaldi]

Proposition 17

L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Application 18

Crible d'Eratosthène (permet de trouver les nombres premiers compris entre 2 et n pour $n \geq 2$).

Théorème 19

(admis) Notons card $\Pi(n) = \text{card}(\mathcal{P} \cap [\![1, n]\!])$ alors $\frac{\Pi(n)}{n} \sim \frac{1}{\ln(n)}$

II. Test de primalité [Rombaldi, Demazure]

Il y a une section du Rombaldi entièrement dédiée à ça.

Définition 20

Pour tout entier $n \geq 2$, on appelle $\mathbb{Z}/n\mathbb{Z}$ l'anneau des classes résiduelles modulo n.

Définition 21 – Indicatrice D'Euler

On note $\varphi(n)$ le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$.

Théorème 22 – Théorème D'Euler

Soit $a \in \mathbb{Z}$ premier avec n, alors $a^{\varphi(n)} \equiv 1 \mod n$

Théorème 23 – Théorème de Fermat

Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$ tel que $p \nmid a$ alors $a^{p-1} \equiv 1 \mod n$.

Remarque 24

La réciproque est fausse ! Par exemple avec 561. En revanche $\forall a \in \mathbb{Z}, a^p \equiv 1 \mod p$.

Définition 25 – Nombre de Carmichaël

On appelle nombre de Carmichaël tout entier $n \geq 3$ non premier tel que $a^{n-1} \equiv 1 \mod n$ pour tout entier a premier avec n.

Proposition 26

Un Nombre de Carmichaël est impair et sans facteur carré + s'écrit comment

Application 27

Alice veut envoyer un message privé à Bob.

- Bob choisit deux entiers premiers distincts $p, q \in \mathbb{P}$ et pose $n = pq$, puis il choisit ensuite $d, e \in \mathbb{Z}$ tels que
$$de \equiv 1 \pmod{\varphi(n)}$$
(on a $\varphi(n) = (p-1)(q-1)$ et il suffit de trouver d premier à $\varphi(n)$ et son inverse).
- Bob diffuse la clé publique (n, d) à tout le monde et conserve la clé secrète (n, e).
- Pour envoyer son message $m \mod n$, Alice envoie le message chiffré $M \equiv m^d \pmod n$.
- Bob déchiffre le message $m \equiv M^e \pmod n$ d'après le théorème d'Euler.

Le succès de cet algorithme réside dans la difficulté de factorisation d'un entier.

Théorème 28 – Théorème de Wilson

Soit $n \geq 2$, on a $n \in \mathcal{P} \iff (n-1)! \equiv -1 \mod n$

Théorème 29 – Test de primalité de Miller-Rabin

Théorème 30 – Test de Solovay-Strassen

III. Applications en algèbre

III.A. Théorie de Sylow [Perrin, Rombaldi]

Soit p un nombre premier diviseur de n. On notera $n = p^\alpha m$ avec $p \nmid m$.

Définition 31

Si n est une puissance de p ($m = 1$), on dit que G est un p-groupe.

Plus généralement, on appelle p-Sylow de G tout sous-groupe de G de cardinal p^α.

Application 32

Ainsi si G est un p-groupe alors son centre n'est pas trivial.

Théorème 33 – Théorème de Sylow 1

Il existe au moins un p-Sylow dans G

Corollaire 34

Il existe au moins un sous-groupe de G d'ordre p^i pour $i \in [\![1, \alpha]\!]$.

Théorème 35 – Théorème de Sylow 2

- Si $H < G$ est un p-groupe, alors il existe un p-Sylow tel que $H < S$,
- Les p-Sylow sont tous conjugués,
- Si on note n_p le nombre de p-Sylow de G, on a $n_p | m$ et $n_p \equiv 1 \mod p$.

Corollaire 36

Soit S un p-Sylow de G. Alors $S \lhd G \iff S$ est l'unique p-Sylow de G.

III.B. Propriétés des corps finis [Perrin, Rombaldi]

Pour $p \in \mathcal{P}$, on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Définition 37

Soit A un anneau commutatif unitaire. Il existe un unique entier positif, appelé caractéristique de A, noté car(A), tel que le sous-anneau premier de A est isomorphe à $\mathbb{Z}/car(A)\mathbb{Z}$.

Proposition 38

Si $\mathbb{K}$ est un corps fini, sa caractéristique est un nombre premier $p \in \mathcal{P}$ et son sous-corps premier est isomorphe à $\mathbb{F}_p$.

Proposition 39

Si $\mathbb{K}$ est un corps fini, alors $\mathbb{K}$ est un $\mathbb{F}_p$-espace vectoriel où $p = \text{car}(\mathbb{K})$, de cardinal p^n où $n = \dim_{\mathbb{F}_p}(K)$. De plus, tout sous-corps de K est de cardinal p^d pour un $d|n$ et réciproquement pour tout $d|n$ il existe un unique sous-corps de $\mathbb{K}$ de cardinal p^d.

Proposition 40

Pour tout $n \in \mathbb{N}^*$ pour tout $p \in \mathcal{P}$ il existe un corps fini de cardinal p^n. On peut le voir comme le corps de rupture de n'importe quel polynôme irréductible sur $\mathbb{F}_p$ de degré n. Ce corps est unique à isomorphisme près.

Définition 41

On définit Frob : $\mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^p$ est un morphisme de corps appelé morphisme de Frobenius

Proposition 42

Frob est un automorphisme et les sous-corps de $\mathbb{F}_q$ sont exactement les ensembles des points fixes de Frob^d pour $d|n$.

Théorème 43

Aut($\mathbb{F}_q$) est cyclique d'ordre n et on a Aut($\mathbb{F}_q$) =< Frob >

III.C. Résidus quadratiques modulo p [Perrin Rombaldi, H2G2]

Soit $p \in \mathcal{P}$, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, puis $\mathbb{F}_p^2 = \{x^2, x \in \mathbb{F}_p\}$ et $\mathbb{F}_p^{2*} = \mathbb{F}_p^2 \cap \mathbb{F}_p^*$.

Proposition 44

Si $p = 2$, on a $\mathbb{F}_2^2 = \mathbb{F}_2$. Sinon on a $|\mathbb{F}_p^2| = \frac{p+1}{2}$.

Lemme 45

On a $x \in \mathbb{F}_p^{2*} \iff x^{\frac{p-1}{2}} = 1$

On aimerait savoir si un entier a est un carré modulo p (classification des formes quadratiques sur les corps finis)

Définition 46 – Symbole de Legendre

Soit $a \in \mathbb{Z}$. On appelle symbole de Legendre de a mod p l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } a \in \mathbb{F}_p^{2*} \\ 0 \text{ si } p|a \\ -1 \text{ sinon} \end{cases}$$

Proposition 47

On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$

Théorème 48 – Loi de réciprocité quadratique

Soient $p \neq q$ des nombres premiers impairs. Alors :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Théorème 49 – Loi de réciprocité quadratique complémentaires

Soit p un nombre premier impair

— $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

— $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Remarque 50

Le nombre de solutions de $x^2 = a$ pour $a \in \mathbb{F}_p$ est $1 + \left(\frac{a}{p}\right)$

III.D. Irréductibilité des polynômes dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$, réduction modulo p [Perrin, Rombaldi, Francinou 1]

Définition 51

Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, $a_n \neq 0$, on appelle contenu de P noté $C(P)$ l'entier $\text{pgcd}(a_i, i \in [\![0, n]\!])$

Proposition 52

Un polynôme de degré supérieur ou égal à 1 est irréductible dans $\mathbb{Z}[X]$ si et seulement si il est de contenu 1 et est irréductible sur $\mathbb{Q}[X]$

Théorème 53 – Critère D'Eisenstein

Soit $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $p \in \mathcal{P}$, si $p \nmid a_r$ et $\forall i < r,\ p|a_i$ et $p^2 \nmid a_0$. Alors P est irréductible sur $\mathbb{Q}[X]$.

Exemple 54

Si $m \in \mathbb{Z}$ est sans facteur premier carré alors $X^n - m$ est irréductible sur $\mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$.

Proposition 55

Soit $p \in \mathcal{P}$ et $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $\overline{P}$ la réduction de P modulo p. Si $p \nmid a_r$ et si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

Définition 56 – Polynômes cyclotomiques

On définit le $n$ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathcal{U}_n^\times} (X - \zeta)$

Proposition 57

$\Phi_n \in \mathbb{Z}[X]$

Proposition 58

Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.

Corollaire 59

On a $[\mathbb{Q}[e^{\frac{2i\pi}{n}}] : \mathbb{Q}] = \varphi(n)$

Références :

— Rombaldi Algèbre,

— Perrin ,

— Gourdon Algèbre,

— Demazure Cours d'Algèbre

— Francinou 1

— H2G2

Table des matières

I Généralités et arithmétique dans $\mathbb{Z}$ [Rombaldi, Perrin] **1**

I.A Arithmétique [Rombaldi] . . . 1

I.B. Répartition des nombres premiers . . . 1

II. Test de primalité **1**

III. Applications en algèbre **2**

III.A. Théorie de Sylow . . . 2

III.B. Propriétés des corps finis . . . 2

III.C. Résidus quadratiques modulo p . . . 2

III.D. Irréductibilité des polynômes dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$, réduction modulo p . . . 3

Leçon n° 122 : Anneaux principaux. Applications

Piroutet Alban

28 juillet 2026

Soit A un anneau commutatif intègre.

I Arithmétique dans les anneaux principaux

I.A) Vocabulaire général [Rombaldi]

Définition 1
Idéal et idéal principal

Définition 2
Divisibilité

Définition 3
Eléments associés

Définition 4
Elements premiers et irréductibles

Proposition 5
Premier $\implies$ irréductible

Exemple 6
Dans $\mathbb{Z}$, les nombres premiers sont premiers.

Définition 7
PGCD et PPCM

Remarque 8
N'existent pas toujours ! Besoin d'anneau où il y a existence ! S'ils existent ils sont définis à un inversible près !

Proposition 9
Deux PGCD (resp deux PPCM) de $a, b \in A$ sont associés.

I.B) Cas des anneaux principaux [Rombaldi]

Définition 10
Anneau principal

Exemple 11
$\mathbb{Z}$ et $\mathbb{K}[X]$

Lemme 12
Dans un anneau $\mathbb{A}$ principal : $\forall p \in \mathbb{A}^* \setminus A^\times$, on a :

$$(p) \text{ premier} \iff p \text{ premier} \iff p \text{ irréductible} \iff (p) \text{ maximale}$$

Corollaire 13
Dans un anneau principal, premier équivaut à irréductible.

Proposition 14
- Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1 .
- Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré et ceux de degré deux sans racine réelle.
- $\mathbb{Q}[X]$ possède des irréductibles de degré arbitrairement grand.

Théorème 15
$\mathbb{A}[X]$ principal $\iff$ $\mathbb{A}$ est un corps.

Exemple 16
$\mathbb{Z}[X]$ n'est pas principal car l'idéal $(2, X)$ n'est pas principal.

Théorème 17
Existence du PGCD et PPCM dans les anneaux principaux.

Corollaire 18 – Lemme de Gauss

Théorème 19
Théorème des restes chinois

Remarque 20
C'est faux si les $(a_i)_i$ ne sont pas premiers entre eux. Par exemple $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

I.C. Anneaux factoriels [Rombaldi]

Définition 21
Anneaux factoriels.

Théorème 22
$\mathbb{A}$ est factoriel $\iff$ toute suite d'idéaux croissante stationne et tout élément premier est irréductible.

Corollaire 23
Les anneaux principaux sont factoriels.

Application 24
Décomposition en facteurs premiers.

Application 25
Calcul du PGCD et PPCM à l'aide de la décomposition.

Proposition 26
A factoriel $\implies$ $A[X]$ factoriel.

Remarque 27
Un anneau factoriel n'est pas nécessairement principal ! Considérer par exemple $\mathbb{Z}[X]$ et $(2, X)$ qui n'est pas principal.

II. Applications aux anneaux euclidiens

II.A. Généralités [Rombaldi]

Définition 28
Anneau euclidien + stathme

Remarque 29
$\mathbb{Z}$ muni de la valeur absolue et $\mathbb{K}[X]$ muni du degré sont euclidiens.

Proposition 30
euclidien $\implies$ principal $\implies$ factoriel

Exemple 31
$\mathbb{Z}$ et $\mathbb{K}[X]$ sont euclidiens.

Proposition 32
Algo d'Euclide Etendue dans $\mathbb{Z}$ et $\mathbb{K}[X]$

Remarque 33
$\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal mais n'est pas euclidien.

II.B. L'anneaux des entiers de Gauss $\mathbb{Z}[i]$ [Perrin, Rombaldi]

Définition 34
Entiers de Gauss $\mathbb{Z}[i]$

Proposition 35
Muni du stathme $N(a+ib) = a^2+b^2$, $\mathbb{Z}[i]$ est euclidien.

Proposition 36
$\mathbb{Z}[i]^\times = N^{-1}(\{1\}) = \{\pm 1, \pm i\}$

Lemme 37
Σ est stable par produit

Lemme 38
Soit $p \in \mathcal{P}$, alors $p \in \Sigma \iff p = 2$ ou $p \equiv 1[4]$

Théorème 39
Théorème des deux carrés.

Corollaire 40
Irréductibles de $\mathbb{Z}[i]$

III. Autres applications

III.A. Equations diophantiennes [Rombaldi]

Proposition 41
Résolution de $ax + by = c \iff a \wedge b | c$.
Soit $a, b, c \in A$ principal. On note $d = a \wedge b = au + bv$ et on écrit $a = da'$ et $b = db'$. L'équation $ax + by = c$ admet une solution si et seulement si $d|c$, disons $c = dc'$ et dans ce cas les solutions sont de la forme $(c'u + kb', c'v - ka')_{k\in A}$.

Remarque 42
Dans le cas où l'anneau est euclidien, on peut déterminer u et v par l'algorithme d'EUCLIDE

Application 43
Résolution de système de congruence à l'aide du théorème des restes chinois.

III.B. En algèbre linéaire [Rombaldi, Mansuy, Gourdon]

Définition 44 – Polynôme minimal
L'application

$$\varphi_M : \mathbb{K}[X] \longrightarrow \mathbb{K}[M]$$
$$P \longmapsto P(M)$$

est un morphisme d'algèbres.
Son noyau est un idéal de $\mathbb{K}[X]$, principal puisque $\mathbb{K}[X]$ est principal. Il est donc engendré par un unique polynôme unitaire π_M, appelé *polynôme minimal* de M.

Proposition 45
$\dim_{\mathbb{K}}(\mathbb{K}[M]) = \deg(\pi_M)$

Proposition 46
$\mathbb{K}[M]$ est un corps $\iff$ π_M est irréductible sur $\mathbb{K}[X]$.

Lemme 47 – Lemme des noyaux
Soit $(P_i)_{1\leq i\leq r}$ une famille de polynômes deux à deux premiers entre eux et $f \in \mathcal{L}(E)$.
En posant $P = \prod_{i=1}^r P_i$, on a $\ker(P(f)) = \bigoplus_{i=1}^r \ker(P_i(f))$. De plus, le projecteur de $\ker(P(f))$ sur l'un de ces sous-espaces, parallèlement à la somme des autres, est un polynôme en f.

Remarque 48
En pratique, on utilise souvent ce lemme avec P annulateur de u. On obtient alors une décomposition de E en sous-espaces stables, car $\ker(Q(u))$ est stable par u pour tout polynôme Q.

Proposition 49
M est trigonalisable (resp diagonalisable si et seulement si π_M est scindé (resp scindé à racines simples).

Théorème 50 – Décomposition de Dunford
Supposons M de polynôme caractéristique scindé. Alors il existe un unique couple (D, N) tel que D diagonalisable, N nilpotente, $M = D + N$, avec D et N commutent entre eux.

Application 51
Si $\pi_M$est scindé M est diagonalisable ssi e^M l'est.

Annexe

Soit A un anneau euclidien. L'algorithme d'Euclide détermine le PGCD de deux éléments.

Entrée :

$$a, b \in A, \qquad b \neq 0$$

Sortie :

$$d, u, v \text{ tels que } au + bv = d \quad \text{et} \quad d = a \wedge b$$

Algorithme :

$$u_0 = 1, \quad u_1 = 0, \quad v_0 = 0, \quad v_1 = 1,$$
$$r_0 = a, \quad r_1 = b, \quad i = 1$$

Tant que $r_i \neq 0$:

$$r_{i+1} \leftarrow r_{i-1} - q_i r_i \qquad \text{(division euclidienne de } r_{i-1} \text{ par } r_i)$$
$$u_{i+1} \leftarrow u_{i-1} - q_i u_i$$
$$v_{i+1} \leftarrow v_{i-1} - q_i v_i$$
$$i \leftarrow i + 1$$

Renvoyer :

$$r_{i-1}, \ u_{i-1}, \ v_{i-1}$$

Référence :

— Rombaldi Algèbre et géométrie

— Perrin Cours d'arithmétique

— Gourdon Algèbre

— Mansuy Réduction des endomorphismes

— Algèbre et calcul formel Odile Fleury

Table des matières

I Arithmétique dans les anneaux principaux **1**
I.A Vocabulaire général [Rombaldi] . . . 1
I.B Cas des anneaux principaux [Rombaldi] . . . 1
I.C.Anneaux factoriels [Rombaldi] . . . 1

II. Applications aux anneaux euclidiens **2**
II.A. Généralités . . . 2
II.B. L'anneaux des entiers de Gauss $\mathbb{Z}[i]$ . . . 2

III. Autres applications **2**
III.A. Equations diophantiennes . . . 2
III.B. En algèbre linéaire . . . 2

123 Corps finis et applications

Piroutet Alban

Agrégation de Mathématiques — 2025

Soit $\mathcal{P}$ l'ensemble des nombres premiers. Tous les corps seront supposés commutatifs sauf mention du contraire.

I Notions de corps finis

I.A) Premiers résultats [Perrin, Rombaldi]

Définition 1
Un corps fini est un corps de cardinal fini.

Proposition 2
Soit $p \in \mathcal{P}$, $\mathbb{F}_p = \mathbb{Z}/\mathbb{Z}p$ est un corps fini à p éléments.

Proposition 3
Soit $\mathbb{K}$ un corps. L'application $\mathbb{Z} \to \mathbb{K}$, $m \to m.1_{\mathbb{K}}$ est un morphisme d'anneaux de noyaux $n\mathbb{Z}$ pour un $n \in \mathbb{N}$.

Définition 4
L'image de ce morphisme est un sous-corps de $\mathbb{K}$ appelé sous-corps premiers de $\mathbb{K}$. n est la caractéristique de $\mathbb{K}$ que l'on note car($\mathbb{K}$).

Proposition 5
Si $\mathbb{K}$ est fini, on a car($\mathbb{K}$) $\in \mathcal{P}$.

Application 6
Le sous-corps premier de $\mathbb{K}$ est alors isomorphosme à $\mathbb{Z}/p\mathbb{Z}$

On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ pour tout $p \in \mathcal{P}$

Proposition 7
Si $\mathbb{K}$ est un corps fini de caractéristique p, alors $\mathbb{K}$ est un $\mathbb{F}_p$-espace vectoriel où $p = \text{car}(\mathbb{K})$, de cardinal p^n où $n = \dim_{\mathbb{F}_p}(\mathbb{K})$.

Application 8
Il n'existe aucun corps de cardinal 6.

I.B) Existence et unicité [Perrin, Rombaldi]

Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$. Soit $q = p^n$.

Définition 9
Soit $\mathbb{K}$ un corps de caractéristique p,

$$\text{Frob} : \mathbb{K} \to \mathbb{K}, x \mapsto x^p$$

est un morphisme de corps appelé morphisme de Frobenius

Proposition 10
Frob est injectif et si $\mathbb{K}$ est fini, c'est un automorphisme.

Proposition 11
Pour $\mathbb{K} = \mathbb{F}_p$, Frob=Id.

Proposition 12
Soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$. Alors l'ensemble des racines de $X^{p^n} - X$ dans $\overline{\mathbb{F}_p}$ est un sous-corps de $\overline{\mathbb{F}_p}$ à q éléments, contenant $\mathbb{F}_p$.

Corollaire 13
Il existe un corps fini à q éléments, unique à isomorphisme près : c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Théorème 14
Tout corps fini est commutatif.

I.C. Construction explicite [Rombaldi]

Théorème 15
$X^{p^n} - X = \prod_{d|n} \prod_{U_n(p)} P$ et dénombrement des polynômes irréductibles de degré donné.

Corollaire 16
Si on note $I_n(p)$ le nombre de polynôme irréductible de degré n sur $\mathbb{F}_p$, on a $nI_n(p) = \sum_{d|n} \mu(\frac{n}{d})p^d$ avec $I_n(p) \sim \frac{p^n}{n}$.

Remarque 17
Il existe des polynômes irréductibles de tout degré, ainsi en posant $\mathbb{F}_{\text{ll}} = \mathbb{F}/(P)$ où P irréductible de degré n, on obtient un corps de cardinal $q = p^n$. On peut donc créer tous les corps finis possibles.

Exemple 18
Construction de $\mathbb{F}_4$ par $\mathbb{F}_2/(X^2 + X + 1)$

II. Structure des corps finis [Perrin, Rombaldi]

Proposition 19
Les sous-corps de $\mathbb{F}_{p^n}$ sont les $\mathbb{F}_{p^d}$ avec $d|n$.

Théorème 20

Soient K, L, M des corps, $(e_i)_{i\in I}$ une base de L sur K, $(f_j)_{j\in J}$ une base de M sur L. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de M sur K.
En particulier, lorsque deux des degrés d'extensions sont finis, le troisième aussi et on a

$$[M : K] = [M : L]\,[L : K].$$

Application 21

$[\mathbb{F}_{p^n} : \mathbb{F}_{p^d}] = \frac{n}{d}$

Théorème 22

$\mathbb{F}_p^\times$ est cyclique d'ordre $p-1$, en particulier il est isomorphe $\mathbb{Z}/(p-1)\mathbb{Z}$.

Théorème 23

Le groupe des $\mathbb{F}_p$- automorphismes de $\mathbb{F}_q$ $(q = p^n)$ est cyclique d'ordre n engendré par le Frobenius.

III. Applications

III.A. Résolution d'équation de degré 2 [Perrin, Rombaldi, H2G2]

Soit $p \in \mathcal{P}$ et $q = p^n$ où $n \in \mathbb{N}^*$. On note $\mathbb{F}_q^2 = \{x^2, x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{2*} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

Proposition 24

Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$. Sinon $|\mathbb{F}_q^2| = \frac{q+1}{2}$

Application 25

Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p^2$.

On suppose désormais que p est un impair.

Lemme 26

On a $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$

Exemple 27

-1 est un carré modulo p si et seulement si $p \equiv 1[4]$.

On aimerait savoir facilement si un élément est un carré i.e l'équation $x^2 \equiv a[p]$ admet des solutions entières.

Définition 28

Soit $a \in \mathbb{Z}$, on appelle le symbole de Legendre (de a mod p) l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a[p] \text{ admet une solution et } p \nmid a \\ 0 & \text{si } p|a \\ -1 & \text{sinon} \end{cases}$$

Proposition 29

On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p]$

Remarque 30

Le nombre de solution de $x^2 \equiv a[p]$ est $1 + \left(\frac{a}{p}\right)$

Proposition 31

Soit p un nombre premier, $a, b \in \mathbb{Z}$ tels que $a \wedge b = 1$ alors $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Théorème 32 – Loi de réciprocité quadratique

Soient $p \neq q$ deux entiers premiers impairs. Alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$$

Proposition 33

On a $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ et $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Remarque 34

On peut donc calculer tous les symboles de Legendre.

Exemple 35

$\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2}\frac{307-1}{2}}\left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = -1$. Ainsi 26 n'est pas un carré mod 307.

III.B. Sur les polynômes [Francinou Algèbre 1, Perrin, Rombaldi]

Théorème 36 – Critère D'Einsenstein

Soit $P = \sum_{k=0}^{r} a_k X^k \in \mathbb{Z}[X]$ et $p \in \mathcal{P}$, tel que $\forall i \in [\![0, r-1]\!]$ $p|a_i$, $p \nmid a_r$ et $p^2 \nmid a_0$ alors P est irréductible sur $\mathbb{Q}$.

Exemple 37

Le polynôme $X^3 + 2X^2 + 4X + 2$ est irréductible sur $\mathbb{Q}[X]$.

Définition 38

Soit $n \in \mathbb{N}^*$, on définit $\phi_n(X) = \prod_{0\leq k\leq n, k\wedge n=1} (X - e^{\frac{2ik\pi}{n}})$

Proposition 39

Pour $n \in \mathbb{N}^*$, $\phi_n \in \mathbb{Z}[X]$ et ϕ_n irréductible sur $\mathbb{Q}$

Références :

— Perrin,

— Rombaldi Algèbre,

— Objectif Agreg,

— Francinou Algèbre 1,

— Tauvel Corps commutatif et théorie de Galois,

— H2G2

Table des matières

I Notions de corps finis **1**
I.A Premiers résultats [Perrin, Rombaldi] . . . 1
I.B Existence et unicité [Perrin, Rombaldi] . . . 1
I.C. Construction explicite . . . 1

II. Structure des corps finis **1**

III. Applications **2**
III.A. Résolution d'équation de degré 2 . . . 2
III.B. Sur les polynômes . . . 2

Leçon n° 125 : Extenions de corps. Exemples et applications

Piroutet Alban

28 juillet 2026

I. Généralités sur les extensions de corps [Perrin]

On ne considère que des corps commutatifs.

Définition 1 – Extension de corps, degré

Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps tels que $\mathbb{K} \subset \mathbb{L}$. On dit que $\mathbb{L}$ est une extension de corps de $\mathbb{K}$. $\mathbb{L}$ est alors un $\mathbb{K}$-espace vectoriel. Lorsque $\dim_{\mathbb{K}}(\mathbb{L})$ est fini, on note $[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}}(\mathbb{L})$ et on l'appelle le degré de $\mathbb{L}$ sur $\mathbb{K}$. On dit alors que l'extension est de degré finie.

Exemple 2

$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Théorème 3 – Théorème de la base télescopique

Soient $\mathbb{K}, \mathbb{L}, \mathbb{M}$ des corps, $(e_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$. En particulier, lorsque deux des degrés d'extensions sont finis, le troisième aussi et on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Définition 4 – Element algébriques, transcendants

Soit $\mathbb{L}$ une extension de $\mathbb{K}$, soit $\alpha \in \mathbb{L}$. Soit $\varphi : \mathbb{K}[T] \longrightarrow \mathbb{L}$ le morphisme d'anneaux tel que $\varphi_{|\mathbb{K}} = \mathrm{id}$ et $\varphi(T) = \alpha$.
Si φ est injectif, on dit que α est transcendant sur $\mathbb{K}$. Sinon, $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ et il existe $P \in \mathbb{K}[X]$ unitaire tel que $\ker(\varphi) = (P)$. Le polynôme P est appelé polynôme minimal de α.
Une extension $\mathbb{L}$ de $\mathbb{K}$ qui vérifie que tout élement $\alpha \in \mathbb{L}$ est algébrique est dite algébrique.

Exemple 5

$\sqrt{2}$, i sont algébriques sur $\mathbb{Q}$. π et e sont transcendants sur $\mathbb{Q}$.

Proposition 6

Une extension finie est algébrique. La réciproque est fausse (cf $\overline{\mathbb{Q}}$).

Définition 7

Soit $\mathbb{K} \subseteq \mathbb{L}$ une extension de corps et soit S une partie de $\mathbb{L}$. L'ensemble des sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et S est non vide (car il contient $\mathbb{L}$) et donc l'intersection de tous ces sous-corps est un sous-corps de $\mathbb{L}$, qui est le plus petit sous-corps contenant $\mathbb{K}$ et S. On l'appelle le sous-corps engendré par S sur $\mathbb{K}$ et on le note $\mathbb{K}(L)$, ou $\mathbb{K}(x_1, \dots, x_n)$ si $S = \{x_1, \dots, x_n\}$. On définit de même $\mathbb{K}[x_1, \dots, x_n]$ le plus petit sous-anneaux de $\mathbb{L}$ contenant $x_1, \dots, x_n$ et $\mathbb{K}$.

Proposition 8

Soit $\mathbb{K} \subseteq \mathbb{L}$ une extension de corps et soit $x_1, \dots, x_n \in \mathbb{L}$. Alors

$$\mathbb{K}(x_1, \dots, x_n) = \{\frac{P(x_1, \dots, x_n)}{Q(x_1, \dots, x_n)} | P, Q \in \mathbb{K}[X_1, \dots, X_n], Q(x_1, \dots, x_n) \neq 0\}$$

$$\mathbb{K}[x_1, \dots, x_n] = \{P(x_1, \dots, x_n) | P \in \mathbb{K}[X_1, \dots, X_n]\}$$

Théorème 9

Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Pour $\alpha \in \mathbb{L}$, on a :

$$\alpha \text{ est algébrique sur } \mathbb{K} \iff \mathbb{K}[\alpha] = \mathbb{K}(\alpha) \iff \dim(\mathbb{K}[\alpha]) < +\infty.$$

Proposition 10

Soit $\mathbb{L}/\mathbb{K}$ une extension et $\alpha \in \mathbb{L}$. Si α est transcendant sur $\mathbb{K}$, on a $\mathbb{K}[\alpha] \simeq \mathbb{K}[X]$ et $\mathbb{K}(\alpha) \simeq \mathbb{K}(X)$.

II. Extensions de corps et polynômes

II.A. Corps de rupture [Perrin]

Définition 11

Soit $\mathbb{K}$ un corps et soit $P \in \mathbb{K}[X]$ un polynôme irréductible sur $\mathbb{K}$. On appelle *corps de rupture* de P sur $\mathbb{K}$ toute extension $\mathbb{L}/\mathbb{K}$ telle que :
- P admet une racine dans $\mathbb{L}$;
- $\mathbb{L} = \mathbb{K}(\alpha)$ avec α une racine de P dans $\mathbb{L}$.

Théorème 12

Soit $P \in \mathbb{K}[X]$ irréductible. Il existe un corps de rupture de P sur $\mathbb{K}$. De plus, il est unique à isomorphisme près.

Exemple 13

Le corps $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$ est un corps de rupture de $X^2 + 1$.

II. B. Corps de décomposition [Perrin]

Définition 14

Soit $P \in \mathbb{K}[X]$ un polynôme, irréductible ou non, de degré n. On appelle *corps de décomposition* de P sur $\mathbb{K}$ une extension $\mathbb{L}$ de $\mathbb{K}$ qui est telle que :
1. dans $\mathbb{L}[X]$, P est produit de facteurs de degré 1 (ou encore, P a "toutes" ses racines dans $\mathbb{L}$),
2. le corps $\mathbb{L}$ est minimal pour cette propriété (ou encore, les racines de P engendrent $\mathbb{L}$).

Théorème 15

Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près.

Exemple 16

Un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}(j, \sqrt{2})$.

Exemple 29

Construction de $\mathbb{F}_4$ par $\mathbb{F}_2/(X^2 + X + 1)$

Définition 17
L'extension $\mathbb{L}/\mathbb{K}$ est dite séparable si elle est algébrique et que le polynôme minimal de chaque élément est premier avec son polynôme dérivée (ou encore est scindé à racines dans une clôture algébrique de $\mathbb{K}$).

Théorème 18 – Théorème de l'élément primitif
Toute extension finie séparable est simple, c'est-à-dire engendrée par un seul élément, appelé élément primitif.

II. C. Clôture algébrique [Perrin]

Définition 19
Une extension $\overline{\mathbb{K}}$ de $\mathbb{K}$ est appelée une *clôture algébrique* de $\mathbb{K}$ si elle vérifie :

1. $\overline{\mathbb{K}K}$ est algébriquement clos (i.e tout polynôme non-constant de $\mathbb{K}$ admet une racine dans $\overline{\mathbb{K}K}$),
2. $\overline{\mathbb{K}}$ est algébrique sur K.

Théorème 20 – Théorème de D'Alembert-Gauss
Tout polynôme non-constant de $\mathbb{C}$ admet une racine dans $\mathbb{C}$.

Corollaire 21
$\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

II.D Cas des corps finis [Rombaldi, Perrin]

Définition 22
Caractéristique et inclusion selon la caractéristique.

Remarque 23
Un corps fini est de cardinal une puissance d'un nombre premier.

Proposition 24
Morphisme de Frobenius

Théorème 25
$\mathbb{F}_q^*$ est cyclique.

III. Applications

III. A Construction des corps finis [Rombaldi, Perrin]

Théorème 26
$X^{p^n} - X = \prod_{d|n} \prod_{U_n(p)} P$ et dénombrement des polynômes irréductibles de degré donné.

Corollaire 27
Si on note $I_n(p)$ le nombre de polynôme irréductible de degré n sur $\mathbb{F}_p$, on a $nI_n(p) = \sum_{d|n} \mu(\frac{n}{d})p^d$ avec $I_n(p) \sim \frac{p^n}{n}$.

Remarque 28
Il existe des polynômes irréductibles de tout degré, ainsi en posant $\mathbb{F}_{\text{ll}} = \mathbb{F}/(P)$ où P irréductible de degré n, on obtient un corps de cardinal $q = p^n$. On peut donc créer tous les corps finis possibles.

III.B Nombres constructibles [Carega, Gozard]

Définition 30
Points constructibles à la règle et au compas.

Proposition 31
Construction des parallèles, médiatrices, bissectrices.

Théorème 32
L'ensemble $\mathcal{C}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.

Théorème 33
Théorème de Wantzel

Proposition 34
Réponses aux problèmes historiques

III.C. Applications aux polynômes cyclotomiques [Francinou Algèbre 1, Perrin, Rombaldi]

Définition 35 – Polynômes cyclotomiques
On définit le $n$ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathcal{U}_n^\times} (X - \zeta)$

Proposition 36
$\Phi_n \in \mathbb{Z}[X]$

Proposition 37
Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.

Corollaire 38
On a $[\mathbb{Q}[e^{\frac{2i\pi}{n}}] : \mathbb{Q}] = \varphi(n)$

Références :

— Perrin,

— Rombaldi Algèbre,

— Gozard,

— Objectif Agreg

— Francinou Algèbre 1

— Carrega Théorie des corps

— Tauvel Corps commutatif et théorie de Galois

Table des matières

I. Généralités sur les extensions de corps **1**

II. Extensions de corps et polynômes **1**

II.A. Corps de rupture 1
II.B. Corps de décomposition 1
II.C. Clôture algébrique 2
II.D Cas des corps finis 2

III. Applications **2**

III. A Construction des corps finis 2
III.B. Nombres constructibles 2
III.C. Applications aux polynômes cyclotomiques 2

Leçon n° 127 :Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications.

Piroutet Alban

28 juillet 2026

I Rationnalité et algébricité

I.A) Rationnels et irrationnels [Duverney]

Définition 1
$\mathbb{Q}$ comme corps de fraction de $\mathbb{Z}$, irrationnels

Exemple 2
$\sqrt{2}, e \in \mathbb{R} \setminus \mathbb{Q}$ et exemples de rationnels.

Définition 3
Définition de π comme le périmètre du demi-cercle unité.

Proposition 4
π se définit de manière équivalente comme le générateur du noyau du morphisme $t \mapsto e^{2it}$

Proposition 5
$\pi \in \mathbb{R} \setminus \mathbb{Q}$

Proposition 6
Si $\theta \in \mathbb{R} \setminus \mathbb{Q}$, alors $\mathbb{Z} + \theta\mathbb{Z}$ dense dans $\mathbb{R}$.

Proposition 7
Les applications continues 1 et $\sqrt{2}$ périodiques sont constantes.

I.B) Algébricité et transcendance [Perrin, Duverney]

Définition 8
Algébrique et transcendant avec application

Exemple 9
Dans $\mathbb{K}(T)$, T est transcendant sur $\mathbb{K}$.

Exemple 10
Exemples de nombres algébrique sur $\mathbb{Q}$.

Définition 11
Définition de $\mathbb{K}(\alpha)$ et $\mathbb{K}[\alpha]$

Proposition 12
α est algébrique sur $\mathbb{K} \iff [\mathbb{K}[\alpha] : \mathbb{K}] < +\infty$.

Théorème 13
L'ensemble $\mathbb{M} = \{x \in \mathbb{L} |\ x \text{ est algébrique sur } \mathbb{K}\}$ est un sous-corps.

Application 14
$\overline{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.

Théorème 15
(admis) π et e sont transcendants

Théorème 16
Condition vérifée par les algébriques

Définition 17
Nombres de Liouville

Proposition 18
Les nombres de Liouville sont transcendants

Application 19
Le réel $\sum_{k=0}^{+\infty} \frac{1}{10^{k!}}$ est transcendant.

II. Anneaux $\mathbb{Z}[w]$ et application en arithmétique

II.A. Généralités [Duverney, Perrin]

Proposition 20 – Corps quadratiques
$\mathbb{Q}[\sqrt{d}]$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ et ayant pour $\mathbb{Q}$-base $(1, \sqrt{d})$.

Proposition 21
Les anneaux des entiers de $\mathbb{Q}[\sqrt{d}]$ sont les $\mathbb{Z}[\omega]$, ω variant selon la congruence de d.

Exemple 22
Les entiers de Gauss $\mathbb{Z}[i]$ et les entiers d'Eisenstein $\mathbb{Z}[j]$.

Proposition 23
Les inverses de $\mathbb{Z}[w]$

Application 24
$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ et $\mathbb{Z}[j]^\times = \{\pm 1, \pm i, \pm j\}$

Théorème 25
Valeurs de d pour lesquelles $\mathbb{Z}[w]$ est euclédien.

Remarque 26
$\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel ($6 = 3 \times 2 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ donc n'est pas euclédien.

Définition 27
On définit l'ensemble $\Sigma = \{p \in \mathbb{N}, \exists (a,b) \in \mathbb{N}^2, p = a^2 + b^2\}$

Proposition 28
Σ est stable par produit

Théorème 29 – Théorème des deux carrés
Soit $p \in \mathcal{P}, p \in \Sigma \iff p = 2$ ou $p \equiv 1[4]$

Proposition 30
Soit n un entier, on a $n \in \Sigma \iff v_p(n)$ pair pour tout p premier avec $p \equiv 3[4]$

Proposition 31
Irréductibles de $\mathbb{Z}[i]$

II.B. Application : résolutions d'équations diophantiennes [Duverney]

Application 32
Résolution de l'équation de Mordell $y^2 = x^3 - 11$

Application 33
Résolution de $x^5 - y^2 = 1$

III.Construction à la règle et au compas

III.A. Définitions et propriétés [Carega]

Définition 34
Points constructibles

Proposition 35
Constructions des parallèles, médiatrices et bissectrices

Théorème 36
L'ensemble des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.

III.B. Lien avec la théorie des corps [Carega]

Lemme 37
Equations des droites et d'un cercle

Théorème 38 – Théorème de Wantzel
Théorème de Wantzel [admis]

Corollaire 39
Résultat de Wantzel

III. C. Réponses aux trois problèmes historiques [Carega]

Corollaire 40
La duplication du cube est impossible.

Corollaire 41
La quadrature du cercle est impossible.

Corollaire 42
La trissection de l'angle est impossible en général.

IV. Autres résultats [Francinou 1]

Théorème 43 – Kronecker
Soit $P \in \mathbb{Z}[X]$ unitaire avec $P(0) \neq 0$, si toutes les racines de P sont de module inférieur ou égal à 1, ce sont des racines de l'unité.

Corollaire 44
Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$. Si toutes les racines de P sont de module inférieur ou égal à 1, alors $P = X$ ou $P = \Phi_k$ pour un certain $k \in \mathbb{N}^*$.

Références :
— Perrin,

— Duverney théorie des nombres,

— Carréga Théorie des corps

— Francinou Algèbre 1

Table des matières

I Rationnalité et algébricité **1**
I.A Rationnels et irrationnels [Duverney] 1
I.B Algébricité et transcendance [Perrin, Duverney] 1

II. Anneaux $\mathbb{Z}[w]$ et application en arithmétique **1**
II.A. Généralités 1
II.B. Application : résolutions d'équations diophantiennes 2

III.Construction à la règle et au compas **2**
III.A. Définitions et propriétés 2
III.B. Lien avec la théorie des corps 2
III. C. Réponses aux trois problèmes historiques 2

IV. Autres résultats **2**

Leçon n° 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Piroutet Alban

28 juillet 2026

Soit $\mathbb{K}$ un corps et A un anneau intègre, tous deux commutatifs.

I Polynômes irréductibles

I.A) Irréductibilité [Perrin]

Définition 1 – Polynôme irréductible

Un polynôme est irréductible sur l'anneau A s'il n'est pas inversible et s'il n'est pas le produit de deux polynômes non inversibles.

Dans le cas d'un corps la définition peut être simplifiée :

Définition 2

Un polynôme P est irréductible sur le corps $\mathbb{K}$s'il est non constant, et si ses seuls diviseurs sont les polynômes constants et les polynômes qui lui sont associés, c'est-à-dire les polynômes de la forme $\lambda P, \lambda \in \mathbb{K}^*$.

Proposition 3

Dans un corps, les polynômes de degré un sont irréductibles.

Proposition 4

Soit $P \in \mathbb{K}[X]$, avec $2 \leq \deg(P) \leq 3$. On a P irréductible sur $\mathbb{K} \iff P$ sans racine dans $\mathbb{K}$.

Remarque 5

Le cas $2 \leq \deg(P) \leq 3$ est important, en effet le polynôme $(X^2+1)^2$ est réductible sur $\mathbb{R}$ avec aucune racine réelle.

Lemme 6 – Lemme d'Euclide

Soient $P \in \mathbb{K}[X]$ un polynôme irréductible . Si P divise un produit $\prod_{i=1}^{r} A_i$ de $r \geq 2$ polynômes non nuls, il divise alors l'un des A_k.

Théorème 7

Tout polynôme non constant $P \in K[X]$ est produit de polynômes irréductibles, et une telle décomposition est unique à l'ordre près des facteurs. Autrement dit, il existe une constante $\lambda \in \mathbb{K}^*$, un entier $r \geq 1$,
des polynômes unitaires $P_1, \ldots, P_r$ deux à deux distincts et irréductibles,
et des entiers naturels non nuls $m_1, \ldots, m_r$ tels que :

$$P = \lambda \prod_{k=1}^{r} P_k^{m_k}.$$

Proposition 8

Il y a un infinité de polynômes de $\mathbb{K}[X]$ irréductibles.

I.B. Propriétés de $A[X]$ [Perrin, Francinou 1]

Théorème 9

Soit A un anneau commutatif intègre et unitaire. On a :
$A[X]$ euclidien $\iff$ $A[X]$ est principal $\iff$ A est un corps

Proposition 10

A factoriel $\implies$ $A[X]$ factoriel.

Définition 11

Si A est factoriel, on définit le contenu d'un polynôme comme le PGCD de ses coefficients.

Un polynôme sera dit primitif si son contenu vaut 1.

Lemme 12 – Lemme de Gauss

On a $\forall P, Q \in A[X], C(PQ) = C(P)C(Q)$ modulo A^*.

I.C. Critère d'irréductibilité [Perrin, Francinou 1]

Proposition 13

Soit A un anneau factoriel unitaire, commutatif et intègre de corps de fraction $\mathbb{K}$. Les polynômes de $A[X]$ irréductible dans $A[X]$ sont :

1. les constantes $p \in A$, irréductibles dans A,
2. les polynômes P de degré 1, primitifs et irréductibles dans $\mathbb{K}[X]$.

Théorème 14 – Critère d'Eisenstein

Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. Soit $p \in A$ premier. Si $p \nmid a_n$, $\forall i < n$, $p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Exemple 15

Si $m \in \mathbb{Z}$ a un facteur premier sans carré, alors $X^n - m$ est irréductible dans $\mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$.

Proposition 16

Dans un corps P irréductible si et seulement si (P) est maximal.

Proposition 17 – Réduction

Soit I un idéal premier de A et $B = A/I$. Soit $P = \sum_{i=0}^{r} a_i X^i \in A[X]$ et $\overline{P}$ la réduction de P modulo I. Si $a_r \notin I$, et si $\overline{P}$ est irréductible sur B ou $\mathrm{Frac}(B)$, alors P est irréductible sur $\mathbb{K} = \mathrm{Frac}(A)$.

Que l'on reformule dans le cas $A = \mathbb{Z}, I = (p), B = \mathbb{F}_p$:

Proposition 18

Soit $p \in \mathbb{P}$ et $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $\overline{P}$ la réduction de P modulo p. Si $p \nmid a_r$ et si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 19

$\mathbb{Q}[X]$ admet des polynômes irréductibles de degré quelconque : $P_n = X^n - p$ avec p premier.

II. Extensions de corps et polynômes

II.A. Extensions de corps [Perrin]

Définition 20 – Extension de corps, degré

Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps tels que $\mathbb{K} \subset \mathbb{L}$. On dit que $\mathbb{L}$ est une extension de corps de $\mathbb{K}$. $\mathbb{L}$ est alors un $\mathbb{K}$-espace vectoriel. Lorsque $\dim_{\mathbb{K}}(\mathbb{L})$ est fini, on note $[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}}(\mathbb{L})$ et on l'appelle le degré de $\mathbb{L}$ sur $\mathbb{K}$. On dit alors que l'extension est de degré finie.

Exemple 21

$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Théorème 22 – Théorème de la base télescopique

Soient $\mathbb{K}, \mathbb{L}, \mathbb{M}$ des corps, $(e_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$. En particulier, lorsque deux des degrés d'extensions sont finis, le troisième aussi et on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Définition 23 – Element algébriques, transcendants

Soit $\mathbb{L}$ une extension de $\mathbb{K}$, soit $\alpha \in \mathbb{L}$. Soit $\varphi : \mathbb{K}[T] \longrightarrow \mathbb{L}$ le morphisme d'anneaux tel que $\varphi_{|\mathbb{K}} = \mathrm{id}$ et $\varphi(T) = \alpha$.
Si φ est injectif, on dit que α est transcendant sur $\mathbb{K}$. Sinon, $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ et il existe $P \in \mathbb{K}[X]$ unitaire tel que $\ker(\varphi) = (P)$. Le polynôme P est appelé polynôme minimal de α.
Une extension $\mathbb{L}$ de $\mathbb{K}$ qui vérifie que tout élement $\alpha \in \mathbb{L}$ est algébrique est dite algébrique.

Exemple 24

$\sqrt{2}$, i sont algébriques sur $\mathbb{Q}$. π et e sont transcendants sur $\mathbb{Q}$.

Proposition 25

Une extension finie est algébrique. La réciproque est fausse (cf $\overline{\mathbb{Q}}$).

Définition 26

Soit $\mathbb{K} \subseteq \mathbb{L}$ une extension de corps et soit S une partie de $\mathbb{L}$. L'ensemble des sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et S est non vide (car il contient $\mathbb{L}$) et donc l'intersection de tous ces sous-corps est un sous-corps de $\mathbb{L}$, qui est le plus petit sous-corps contenant $\mathbb{K}$ et S. On l'appelle le sous-corps engendré par S sur $\mathbb{K}$ et on le note $\mathbb{K}(L)$, ou $\mathbb{K}(x_1, \ldots, x_n)$ si $S = \{x_1, \ldots, x_n\}$. On définit de même $\mathbb{K}[x_1, \ldots, x_n]$ le plus petit sous-anneaux de $\mathbb{L}$ contenant $x_1, \ldots, x_n$ et $\mathbb{K}$.

Proposition 27

Soit $\mathbb{K} \subseteq \mathbb{L}$ une extension de corps et soit $x_1, \ldots, x_n \in \mathbb{L}$. Alors

$$\mathbb{K}(x_1, \ldots, x_n) = \{\frac{P(x_1, \ldots, x_n)}{Q(x_1, \ldots, x_n)} | P, Q \in \mathbb{K}[X_1, \ldots, X_n], Q(x_1, \ldots, x_n) \neq 0\}$$

$$\mathbb{K}[x_1, \ldots, x_n] = \{P(x_1, \ldots, x_n) | P \in \mathbb{K}[X_1, \ldots, X_n]\}$$

Théorème 28

Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Pour $\alpha \in \mathbb{L}$, on a :

$$\alpha \text{ est algébrique sur } \mathbb{K} \iff \mathbb{K}[\alpha] = \mathbb{K}(\alpha) \iff \dim(\mathbb{K}[\alpha]) < +\infty.$$

Proposition 29

Soit $\mathbb{L}/\mathbb{K}$ une extension et $\alpha \in \mathbb{L}$. Si α est transcendant sur $\mathbb{K}$, on a $\mathbb{K}[\alpha] \simeq \mathbb{K}[X]$ et $\mathbb{K}(\alpha) \simeq \mathbb{K}(X)$.

II.B. Corps de rupture et de décomposition [Perrin]

Définition 30

Soit $\mathbb{K}$ un corps et soit $P \in \mathbb{K}[X]$ un polynôme irréductible sur $\mathbb{K}$. On appelle *corps de rupture* de P sur $\mathbb{K}$ toute extension $\mathbb{L}/\mathbb{K}$ telle que :
- P admet une racine dans $\mathbb{L}$;
- $\mathbb{L} = \mathbb{K}(\alpha)$ avec α une racine de P dans $\mathbb{L}$.

Théorème 31

Soit $P \in \mathbb{K}[X]$ irréductible. Il existe un corps de rupture de P sur $\mathbb{K}$. De plus, il est unique à isomorphisme près.

Exemple 32

Le corps $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$ est un corps de rupture de $X^2 + 1$.

Définition 33

Soit $P \in \mathbb{K}[X]$ un polynôme, irréductible ou non, de degré n. On appelle *corps de décomposition* de P sur $\mathbb{K}$ une extension $\mathbb{L}$ de $\mathbb{K}$ qui est telle que :
1. dans $\mathbb{L}[X]$, P est produit de facteurs de degré 1 (ou encore, P a "toutes" ses racines dans $\mathbb{L}$),
2. le corps $\mathbb{L}$ est minimal pour cette propriété (ou encore, les racines de P engendrent $\mathbb{L}$).

Théorème 34

Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près.

Exemple 35

Un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}(j, \sqrt{2})$.

Définition 36

L'extension $\mathbb{L}/\mathbb{K}$ est dite séparable si elle est algébrique et que le polynôme minimal de chaque élément est premier avec son polynôme dérivée (ou encore est scindé à racines dans une clôture algébrique de $\mathbb{K}$).

Théorème 37 – Théorème de l'élément primitif

Toute extension finie séparable est simple, c'est-à-dire engendrée par un seul élément, appelé élément primitif.

II. C. Clôture algébrique [Perrin]

Définition 38

Une extension $\overline{\mathbb{K}}$ de $\mathbb{K}$ est appelée une *clôture algébrique* de $\mathbb{K}$ si elle vérifie :
1. $\overline{\mathbb{K}}$ est algébriquement clos (i.e tout polynôme non-constant de $\overline{\mathbb{K}}$ admet une racine dans $\overline{\mathbb{K}}$),
2. $\overline{\mathbb{K}}$ est algébrique sur $\mathbb{K}$.

Théorème 39 – Théorème de D'Alembert-Gauss

Tout polynôme non-constant de $\mathbb{C}$ admet une racine dans $\mathbb{C}$.

Corollaire 40

$\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Proposition 41

Dans un corps algébriquement clos, les polynômes irréductibles sont les polynômes de degré 1.

Application 42

Dans $\mathbb{R}$ les polynômes irréductibles sont les polynômes de degré 1 et ceux de degré 2 à discriminants strictement négatif.

Application 43

Tout matrice à coefficients complexes est trigonalisables.

II.D.Construction des corps finis [Perrin]

Proposition 44

$\forall n \in \mathbb{N}^*$, $I_n(p) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})p^d$.

Théorème 45

Il existe des corps finis de cardinal égal à n'importe quelle puissance d'un nombre premier.

III. Polynômes cyclotomiques [Perrin, Francinou 1]

Définition 46 – Polynômes cyclotomiques

On définit le $n$ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathcal{U}_n^\times}(X - \zeta)$

Proposition 47

Φ_n est unitaire de degré $\varphi(n)$
$X^n - 1 = \prod_{d|n} \Phi_d$.

Corollaire 48

On en déduit la formule $\varphi(n) = \sum_{d|n} \varphi(d)$

Proposition 49

$\Phi_n \in \mathbb{Z}[X]$

Proposition 50

Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.

Corollaire 51

On a $[\mathbb{Q}[e^{\frac{2i\pi}{n}}] : \mathbb{Q}] = \varphi(n)$

Références :

— Perrin Algèbre voir partie anneaux et partie polynôme,

— ROMBALDI,

— FRANCINOU 1

— TAUVEL Corps commutatifs et théorie de Galois

Table des matières

I Polynômes irréductibles **1**
I.A Irréductibilité [Perrin] . . . 1
I.B. Propriétés de $A[X]$ . . . 1
I.C. Critère d'irréductibilité . . . 1

II. Extensions de corps et polynômes **2**
II.A. Extensions de corps . . . 2
II.A. Corps de rupture . . . 2
II.C. Clôture algébrique . . . 2

III. Polynômes cyclotomiques **3**

Leçon n°142: PGCD et PPCM, algorithmes de calcul. Applications.

Piroutet Alban

28 juillet 2026

Soit A un anneau unitaire commutatif intègre et $\mathbb{K}$ un corps.

I.Notion de PGCD et PPCM sur un anneau factoriel

I.A. Généralités [Rombaldi+Perrin]

Définition 1 – divisibilité

Pour $a, b \in A$, on dit que a divise b ou encore $a|b$ s'il existe $c \in A$ tel que $b = ac$, ou encore $(b) \subset (a)$.

Définition 2

$a, b \in A$ sont associés s'ils se divisent mutuellement ou encore s'il existe $u \in A^\times$ tel que $a = bu$.

Remarque 3

C'est une relation d'équivalence notée $\sim$. Deux éléments associés sont indiscernables du point de vue de la divisibilité.

Définition 4

$a \in A$ non inversible et non nul est dit irréductible si pour tout $b, c \in A$ tels que $a = bc$, alors $b \in A^\times$ ou $c \in A^\times$.

Remarque 5

Dans $\mathbb{Z}$, les éléments irréductibles sont les nombres premiers et leurs opposés.

Définition 6

Soient $a, b \in A$. On dit que

— $d \in A$ est un PGCD de a et b et on note $d = a \wedge b$ si $\forall c \in A,\ (c \mid a \text{ et } c \mid b) \Rightarrow c \mid d$,

— $m \in A$ est un PPCM de a et b et on note $m = a \vee b$ si $\forall c \in A,\ (a \mid c \text{ et } b \mid c) \Rightarrow m \mid c$.

On dit que a et b sont premiers entre eux si $a \wedge b = 1$.

Remarque 7

L'existence d'un PGCD et d'un PPCM n'est pas garantie en général. S'ils existent ils sont définis à un inversible près. On peut généraliser la définition pour une famille quelconque d'éléments.

Proposition 8

Deux PGCD (resp deux PPCM) de a et $b \in A$ sont associés.

Proposition 9

$ab = (a \wedge b)(a \vee b)$

Remarque 10

On en déduit qu'un anneau est un anneau à PGCD si, et seulement si, c'est un anneau à PPCM.

Définition 11

L'anneau A est dit factoriel s'il est intègre et si tout élement non nul de A s'écrit de manière unique comme produit d'un élément inversible et d'éléments irréductibles.

Théorème 12

Un anneau factoriel A est un anneau à PGCD. Plus précisément pour $a = u\prod_{i=1}^{r} p_k^{m_k}$, $b = v\prod_{i=1}^{r} p_k^{n_k}$ dans $A^* \setminus A^\times$, où u, v sont inversibles, les p_k irréductibles deux à deux non associés et les n_k et m_k sont des entiers naturels (certains pouvant être nuls), on a $a \wedge b = \prod_{k=1}^{r} p_k^{\min(n_k, m_k)}$

Corollaire 13

Du théorème précédent, on en déduit que dans un anneau factoriel, pour tous $\lambda, a_0, \dots, a_n \in A^*$, on a $\text{pgcd}(\lambda a_0, \dots, \lambda a_n) = \lambda \text{pgcd}(a_0, \dots, a_n)$.

Définition 14

En écrivant $a = u\prod_{i=1}^{r} p_k^{m_k}$, u inversible, les p_k irréductibles deux à deux non associés et les n_k sont des entiers naturels (certains pouvant être nuls) on définit la valuation p_k adique de a l'entier n_k.

Exemple 15

$\mathbb{Z}$ et $\mathbb{K}[X]$ sont factoriels.

Il est aussi possible d'exprimer le PPCM en terme d'idéaux.

Proposition 16

m est un PPCM de a et b si $(a) \cap (b) = (m)$.

Remarque 17

Pour le PGCD, de manière général $(a) + (b) \neq (d)$ où d un est PGCD de a et de b.
Le théorème de Bézout est en défaut dans un anneau factoriel non principal

Application 18

Soit G un groupe abélien fini, alors il existe un élément dont l'ordre est égal à l'exposant du groupe.

Définition 19

Soient $r \in \mathbb{N}_{\geq 2}$ et $a_1, \dots, a_r$ des éléments tous non nuls dans un anneau à PGCD A. On dit que $a_1, \dots, a_r$ sont premiers entre eux si leur PGCD est dans $A^\times$.

Théorème 20

Soient $r \in \mathbb{N}_{\geq 2}$ et $a_1, \dots, a_r$ des éléments tous non nuls dans un anneau à PGCD A. Soit d un diviseur commun à $a_1, \dots, a_r$ et en écrivant $a_k = d\alpha_k$ pour tout $k \in [\![1, r]\!]$, on a :

$$(d = \text{pgcd}(a_1, \dots, a_r)) \iff (\text{pgcd}(\alpha_1, \dots, \alpha_r) = 1)$$

Théorème 21 – Théorème de Gauss

Deux éléments non nuls a, b d'un anneau à PGCD A sont premiers entre eux si, et seulement si, pour tout $c \in A^*$, on a $a|bc \implies a|c$.

I.B .Contenu d'un polynôme [Francinou 1 + Perrin]

Définition 22

Soient A un anneau factoriel et $P \in A[X]$, on définit le contenu de P comme le PGCD de ses coefficients. On le note $C(P)$.
P sera dit primitif si $C(P) = 1$.

Lemme 23

Soient A un anneau factoriel, $P, Q \in A[X]$, on a $C(PQ) = C(P)C(Q)$

Proposition 24 – Critère d'Eisenstein

Soit A un anneau factoriel. Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. Soit $p \in A$ premier. Si $p \nmid a_n$, $\forall i < n$, $p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Théorème 25 – Théorème de Gauss

$A[X]$ est factoriel si A l'est.

II. Vers le théorème de Bézout : PGCD sur un anneau principal [Rombaldi + Perrin+ Mansuy]

Définition 26

Un anneau intègre est dit principal si tous ses idéaux non triviaux sont engendrés par un élément.

Exemple 27

$\mathbb{Z}$, $\mathbb{K}[X]$ sont principaux.

Théorème 28

Un anneau principal A est un anneau à PGCD. Précisément, pour toute famille $\{a_1, \dots, a_r\}$ de $r \geq 2$ éléments de $A^\times$, il existe un élément $\delta \in A^\times$ tel que $(a_1, \dots, a_r) = (\delta)$ et cet élément s'écrit

$$\delta = \sum_{k=1}^{r} u_k a_k$$

où $u_1, \dots, u_r$ sont des éléments de A et δ un PGCD de $a_1, \dots, a_r$.

Remarque 29

Dans un anneau principal, on a bien $(a) + (b) = (d)$ où d est un PGCD de a et de b. C'est faux si l'anneau est factoriel sans être principal, par exemple $\mathbb{K}[X, Y]$, on a $X \wedge Y = 1$ pourtant $(X) + (Y) = (X, Y) \neq (1)$.

Corollaire 30 – Bézout

Soient $r \in \mathbb{N}_{\geq 2}$ et $a_1, \dots, a_r$ tous non-nuls dans un anneau principal A. Ces éléments sont premiers entre eux dans leur ensemble si, et seulement si, il existe $(u_1, \dots, u_r) \in A^r$ tel que $\sum_{i=1}^{r} u_i a_i = 1$.

Application 31 – Lemme des noyaux

Soient E un espace vectoriel sur un corps commutatif K et f un endomorphisme de E. Si $P_1, \dots, P_n \in K[X]$ (avec n entier strictement positif) sont premiers entre eux deux à deux, alors les sous-espaces vectoriels

$$V_i = \ker(P_i(f)) \quad \text{pour } 1 \leq i \leq n$$

sont en somme directe, et l'on a :

$$\bigoplus_{i=1}^{n} V_i = \ker\left[\left(\prod_{i=1}^{n} P_i\right)(f)\right].$$

De plus, la projection de la somme directe $V = \bigoplus_{i=1}^{n} V_i$ sur V_i parallèlement à $\bigoplus_{j \neq i} V_j$ est la restriction à V d'un polynôme en f.

III. Algorithmes de calcul dans les anneaux euclidiens

III.A. Obtention du PGCD [Rombaldi]

Définition 32

On appelle stathme sur un anneau A commutatif et intègre une application $\varphi : A^* \to \mathbb{N}$.

Exemple 33

Le degré sur $\mathbb{K}[X]$ est un stathme.

Définition 34

Un anneau commutatif et intègre A est dit euclidien, s'il existe un stathme φ tel que pour tout couple (a, b) de A avec $b \neq 0$, il existe un couple $(q, r) \in A^2$ tel que $a = bq + r$ avec $r = 0$ ou $r \neq 0$ et $\varphi(r) < \varphi(b)$.

Proposition 35

Euclidien $\implies$ principal $\implies$ factoriel.

Exemple 36

On note $\alpha = \frac{1+i\sqrt{19}}{2}$ et $A = \mathbb{Z}[\alpha]$. Alors A est un anneau principal, non euclidien.

Application 37 – Algorithme D'Euclide

L'algorithme est entièrement basé sur le lemme suivant :

Lemme 38

Soient $a, b \in A^*$ et r un reste dans la division euclidienne de a par b. On a alors $a \wedge b = b$ si $r = 0$ ou $a \wedge b = b \wedge r$ si $r \neq 0$ (à un multiplicateur inversible près).

Exemple 39

Application de l'algo d'Euclide

III.B. Recherche d'une relation de Bézout

Algorithme d'EUCLIDE étendu : en remontant dans l'algorithme, on obtient une relation de BÉZOUT. Exemple avec le PGCD de polynômes

IV. Applications aux équations en arithmétique

IV.A. Equations diophantiennes [Rombaldi]

Définition 40

Soient $n \geq 2$ un entier, a un entier naturel non nul et b un entier relatif. L'équation d'inconnu x, $ax \equiv b[n]$ est une équation diophantienne.

Théorème 41

L'équation diophantienne $ax \equiv b[n]$ a des solutions entières si, et seulement si $\delta = (a \wedge n)|b$. On note alors $n = n'\delta$ et $a = \delta a'$ avec $a' \wedge n' = 1$. Dans ce cas, l'ensemble des solutions de cette équation est $S = \{b'x'_0 + kn' | k \in \mathbb{Z}\}$, où x'_0 est une solution particulière de $a'x \equiv 1[n']$.

IV. B. Systèmes de congruence [Rombaldi]

Théorème 42 – Reste chinois

Soient $n_1, \ldots, n_r \in \mathbb{N}$ des entiers distincts premiers entre eux L'application

$$\varphi : \overline{k} \in \mathbb{Z}/n\mathbb{Z} \longmapsto (\overline{k}^{n_i})_{1 \leq i \leq r}$$

est un isomorphisme d'anneaux.

Exemple 43

$\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

Théorème 44

L'isomorphisme inverse est donné par

$$(k_i \bmod n_i)_{1 \leq i \leq r} \longmapsto \sum_{j=1}^{r} k_j u_j \frac{n}{n_j},$$

où l'on a choisi $(u_j)_{1 \leq j \leq r}$ tels que

$$\sum_{j=1}^{r} u_j \frac{n}{n_j} = 1.$$

Application 45

Soient $a, b \in \mathbb{Z}$ et (S) le système d'équations

$$\begin{cases} x \equiv a \pmod{n}, \\ x \equiv b \pmod{m}, \end{cases}$$

d'inconnue $x \in \mathbb{Z}$.
Si $\gcd(n, m) = 1$, alors :

- on cherche une relation de Bézout $un + vm = 1$ avec $u, v \in \mathbb{Z}$,
- on a alors une solution particulière de (S) : $x_0 = unb + vma$,
- les solutions de (S) sont données par $(x_0 + knm)_{k \in \mathbb{Z}}$.

Exemple 46

Les solutions du système $\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 4 \pmod{5}, \end{cases}$ sont données par $x = 14 + 15k, \quad k \in \mathbb{Z}$.

Proposition 47 – Décomposition en base mixte

ANNEXE

Algorithme d'Euclide. Soit A un anneau euclidien. L'algorithme d'Euclide détermine le PGCD de deux éléments.

Entrée : $a, b \in A,\ b \neq 0$

Sortie : d, u, v tels que $au + bv = d$ et $d = \gcd(a, b)$

Algorithme :

$u_0 = 1,\ u_1 = 0, \quad v_0 = 0,\ v_1 = 1, \quad r_0 = a,\ r_1 = b, \quad i = 1$

Tant que $r_i \neq 0$:

$r_{i+1} \leftarrow r_{i-1} - q_i r_i$ (division euclidienne de r_{i-1} par r_i)

$u_{i+1} \leftarrow u_{i-1} - q_i u_i$

$v_{i+1} \leftarrow v_{i-1} - q_i v_i$

$i \leftarrow i + 1$

Renvoyer $r_{i-1}, u_{i-1}, v_{i-1}$

Références :

— Rombaldi,

— Perrin ,

— Oraux X-ens 1 Cassini,

— Algèbre et calcul formel Odile Fleury

Table des matières

I.Notion de PGCD et PPCM sur un anneau factoriel **1**

I.A. Généralités . . . 1

I.B .Contenu d'un polynôme . . . 2

II. Vers le théorème de Bézout : PGCD sur un anneau principal **2**

III. Algorithmes de calcul dans les anneaux euclidiens **2**

III.A. Obtention du PGCD . . . 2

III.B. Recherche d'une relation de Bézout . . . 2

IV. Applications aux équations en arithmétique **3**

IV.A. Equations diophantiennes . . . 3

IV. B. Systèmes de congruence . . . 3

Leçon n° 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

Piroutet Alban

28 juillet 2026

Soit $\mathbb{K}$ un corps commutatif.

I Racines d'un polynôme

I.A) Premières propriétés [Gourdon, Rombaldi]

Définition 1
Racine d'un polynôme

Proposition 2
a est racine de $P \iff X - a | P$

Exemple 3
Les polynômes réels de degré impair ont une racine réelle

Définition 4
Multiplicité d'une racine

Proposition 5
Expression des polynômes en fonctions de leurs racines et de leurs multiplicités.

Corollaire 6
Un polynôme de degré n sur un corps a au plus n racines comptés avec multiplicités.

Exemple 7
C'est faux si $\mathbb{K}$ n'est pas un corps : $P = 4X$ sur $\mathbb{Z}/8\mathbb{Z}$.

Proposition 8
Si $\mathbb{K}$ est infini alors si $P \in \mathbb{K}[X]$ vérifie que $P(x) = 0, \forall x \in \mathbb{K}$ alors $P = 0$.

Corollaire 9
Lorsque $\mathbb{K}$ est infini, on peut confondre polynôme et fonction polynômiale.

Proposition 10
Formule de Taylor pour les polynômes.

Corollaire 11
Relation entre la dérivée et la multiplicité d'une racine.

Définition 12
Polynôme scindé

Théorème 13
Théorème de d'Alembert-Gauss

Application 14
Toute matrice carrée à coefficients complexes est trigonalisable.

I.B. Relations coefficients-racines [Gourdon, Rombaldi, Francinou 2]

Définition 15
Polynômes symétriques élémentaires

Théorème 16
Relation coefficients-racines

Proposition 17
Formules de Newton

Théorème 18
Théorème de structure des polynômes symétriques

Exemple 19
$P = X^2 + Y^2 + Z^2 = (X + Y + Z)^2 - 2(XY + XZ + YZ)$

II. Localisation des racines d'un polynôme

II.A. Premiers résultats [Francinou 1]

Théorème 20
Théorème de Gauss-Lucas

Théorème 21
Théorème de Kronecker

Corollaire 22
Soit P un polynôme irréductible sur $\mathbb{Q}$ de degré ≥ 1 tel que toutes ses racines soient de modules <1 alors $P = X$ ou $P = \Phi_n$ pour un certain n.

II.B. Disques de Gershgörin [Francinou 2]

Définition 23
Matrice compagnon

Proposition 24
Si C_P est une matrice compagnon alors $\chi_{C_P} = P$

Proposition 25
Disques de Gershgörin

Application 26
On applique les disques de Gershgörin sur les matrices compagnons pour localiser les racines d'un polynôme.

Proposition 27

Si un disque est isolé, alors il y a une unique racine du polynôme dans ce disque.

II.C. Approximation de racines [PGCD+H2G2]

Proposition 28

Méthode de Newton

Proposition 29 – Forme de Hankel

Soit $P \in \mathbb{R}[X]$ de degré n. On note $x_1, \dots, x_t$ ses racines distinctes et $m_1, \dots, m_t$ leur multiplicités respectives.

On définit, pour $k \in \mathbb{N}$, $s_k = \sum_{l=1}^{t} m_l x_l^k$, puis on pose :

$$\forall (X_0, \dots, X_{n-1}) \in \mathbb{C}^n, s(X_0, \dots, X_{n-1}) = \sum_{0 \leq i,j \leq n-1} s_{i+j} X_i X_j$$

Alors la restriction s_R de s à $\mathbb{R}^n$ est une forme quadratique sur $\mathbb{R}^n$, de signature (p, q) où

$$p + q = t$$

et $p - q$ est le nombre de racines réelles de P.

Remarque 30

A quoi servent les formes de HANKEL ? On peut calculer le nombre de racines réelles/complexes d'un polynôme sans les connaître. En effet :

- on peut calculer les $(s_k)_{k\in\mathbb{N}}$ par récurrence en utilisant les polynômes symétriques élémentaires, sans avoir besoin des racines (voir par exemple [Gou09, §2.5, p80]),
- puis on a un algorithme pour trouver la réduction de GAUSS, donc la signature, d'une forme quadratique

Il vaut au moins savoir faire ces calculs sur des exemples simples !

III. Racines de polynôme et extension de corps

III.A. Eléments algébriques [Perrin]

Définition 31 – Extension de corps, degré

Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps tels que $\mathbb{K} \subset \mathbb{L}$. On dit que $\mathbb{L}$ est une extension de corps de $\mathbb{K}$. $\mathbb{L}$ est alors un $\mathbb{K}$-espace vectoriel. Lorsque $\dim_{\mathbb{K}}(\mathbb{L})$ est fini, on note $[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}}(\mathbb{L})$ et on l'appelle le degré de $\mathbb{L}$ sur $\mathbb{K}$. On dit alors que l'extension est de degré finie.

Exemple 32

$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Théorème 33 – Théorème de la base télescopique

Soient $\mathbb{K}, \mathbb{L}, \mathbb{M}$ des corps, $(e_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$. En particulier, lorsque deux des degrés d'extensions sont finis, le troisième aussi et on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Définition 34 – Element algébriques, transcendants

Soit $\mathbb{L}$ une extension de $\mathbb{K}$, soit $\alpha \in \mathbb{L}$. Soit $\varphi : \mathbb{K}[T] \longrightarrow \mathbb{L}$ le morphisme d'anneaux tel que $\varphi_{|\mathbb{K}} = \mathrm{id}$ et $\varphi(T) = \alpha$.
Si φ est injectif, on dit que α est transcendant sur $\mathbb{K}$. Sinon, $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ et il existe $P \in \mathbb{K}[X]$ unitaire tel que $\ker(\varphi) = (P)$. Le polynôme P est appelé polynôme minimal de α.
Une extension $\mathbb{L}$ de $\mathbb{K}$ qui vérifie que tout élement $\alpha \in \mathbb{L}$ est algébrique est dite algébrique.

Exemple 35

$\sqrt{2}$, i sont algébriques sur $\mathbb{Q}$. π et e sont transcendants sur $\mathbb{Q}$.

Proposition 36

Une extension finie est algébrique. La réciproque est fausse (cf $\overline{\mathbb{Q}}$).

Définition 37

Soit $\mathbb{K} \subseteq \mathbb{L}$ une extension de corps et soit S une partie de $\mathbb{L}$. L'ensemble des sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et S est non vide (car il contient $\mathbb{L}$) et donc l'intersection de tous ces sous-corps est un sous-corps de $\mathbb{L}$, qui est le plus petit sous-corps contenant $\mathbb{K}$ et S. On l'appelle le sous-corps engendré par S sur $\mathbb{K}$ et on le note $\mathbb{K}(L)$, ou $\mathbb{K}(x_1, \dots, x_n)$ si $S = \{x_1, \dots, x_n\}$. On définit de même $\mathbb{K}[x_1, \dots, x_n]$ le plus petit sous-anneaux de $\mathbb{L}$ contenant $x_1, \dots, x_n$ et $\mathbb{K}$.

Proposition 38

Soit $\mathbb{K} \subseteq \mathbb{L}$ une extension de corps et soit $x_1, \dots, x_n \in \mathbb{L}$. Alors

$$\mathbb{K}(x_1, \dots, x_n) = \{\frac{P(x_1, \dots, x_n)}{Q(x_1, \dots, x_n)} | P, Q \in \mathbb{K}[X_1, \dots, X_n], Q(x_1, \dots, x_n) \neq 0\}$$

$$\mathbb{K}[x_1, \dots, x_n] = \{P(x_1, \dots, x_n) | P \in \mathbb{K}[X_1, \dots, X_n]\}$$

III.B. Corps de rupture, corps de décomposition, Corps finis [Perrin + Rombaldi]

Théorème 39

Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Pour $\alpha \in \mathbb{L}$, on a :

$$\alpha \text{ est algébrique sur } \mathbb{K} \iff \mathbb{K}[\alpha] = \mathbb{K}(\alpha) \iff \dim(\mathbb{K}[\alpha]) < +\infty.$$

Proposition 40

Soit $\mathbb{L}/\mathbb{K}$ une extension et $\alpha \in \mathbb{L}$. Si α est transcendant sur $\mathbb{K}$, on a $\mathbb{K}[\alpha] \simeq \mathbb{K}[X]$ et $\mathbb{K}(\alpha) \simeq \mathbb{K}(X)$.

Définition 41

Soit $\mathbb{K}$ un corps et soit $P \in \mathbb{K}[X]$ un polynôme irréductible sur $\mathbb{K}$. On appelle *corps de rupture* de P sur $\mathbb{K}$ toute extension $\mathbb{L}/\mathbb{K}$ telle que :

- P admet une racine dans $\mathbb{L}$;
- $\mathbb{L} = \mathbb{K}(\alpha)$ avec α une racine de P dans $\mathbb{L}$.

Théorème 42

Soit $P \in \mathbb{K}[X]$ irréductible. Il existe un corps de rupture de P sur $\mathbb{K}$. De plus, il est unique à isomorphisme près.

Exemple 43

Le corps $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$ est un corps de rupture de $X^2 + 1$.

Définition 44

Soit $P \in \mathbb{K}[X]$ un polynôme, irréductible ou non, de degré n. On appelle *corps de décomposition* de P sur $\mathbb{K}$ une extension $\mathbb{L}$ de $\mathbb{K}$ qui est telle que :

1. dans $\mathbb{L}[X]$, P est produit de facteurs de degré 1 (ou encore, P a "toutes" ses racines dans $\mathbb{L}$),
2. le corps $\mathbb{L}$ est minimal pour cette propriété (ou encore, les racines de P engendrent $\mathbb{L}$).

Théorème 45

Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près.

Exemple 46

Un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}(j, \sqrt{2})$.

Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$. Soit $q = p^n$.

Définition 47

Soit $\mathbb{K}$ un corps de caractéristique p,

$$\text{Frob} : \mathbb{K} \to \mathbb{K}, x \mapsto x^p$$

est un morphisme de corps appelé morphisme de Frobenius

Proposition 48

Frob est injectif et si $\mathbb{K}$ est fini, c'est un automorphisme.

Proposition 49

Pour $\mathbb{K} = \mathbb{F}_p$, Frob=Id.

Proposition 50

Soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$. Alors l'ensemble des racines de $X^{p^n} - X$ dans $\overline{\mathbb{F}_p}$ est un sous-corps de $\overline{\mathbb{F}_p}$ à q éléments, contenant $\mathbb{F}_p$.

Corollaire 51

Il existe un corps fini à q éléments, unique à isomorphisme près : c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Théorème 52

Tout corps fini est commutatif.

Théorème 53

$X^{p^n} - X = \prod_{d|n} \prod_{U_n(p)} P$ et dénombrement des polynômes irréductibles de degré donné.

Corollaire 54

Si on note $I_n(p)$ le nombre de polynôme irréductible de degré n sur $\mathbb{F}_p$, on a $nI_n(p) = \sum_{d|n} \mu(\frac{n}{d}) p^d$ avec $I_n(p) \sim \frac{p^n}{n}$.

Remarque 55

Il existe des polynômes irréductibles de tout degré, ainsi en posant $\mathbb{F}_{\text{ll}} = \mathbb{F}/(P)$ où P irréductible de degré n, on obtient un corps de cardinal $q = p^n$. On peut donc créer tous les corps finis possibles.

Exemple 56

Construction de $\mathbb{F}_4$ par $\mathbb{F}_2/(X^2 + X + 1)$

Références :

— Rombaldi,

— Perrin,

— Petit guide calcul diff,

— Francinou Algèbre 1 et 2,

— Gourdon Algèbre,

— H2G2 TOME PREMIER

Table des matières

I Racines d'un polynôme **1**

I.A Premières propriétés [Gourdon, Rombaldi] . . . 1

I.B. Relations coefficients-racines . . . 1

II. Localisation des racines d'un polynôme **1**

II.A. Premiers résultats . . . 1

II.B. Disques de Gershgörin . . . 1

II.C. Approximation de racines . . . 2

III. Racines de polynôme et extension de corps **2**

III.A. Eléments algébriques . . . 2

III.B. Corps de rupture, corps de décomposition, Corps finis . . . 2

Leçon n° 148 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

Piroutet Alban

28 juillet 2026

Soit $\mathbb{K}$ un corps commutatif. Soit E un $\mathbb{K}$-espace vectoriel dont on rapelle la définition.

I Espaces vectoriels et dimension [Gourdon]

Définition 1 – espace vectoriel, sous-espace vectoriel

$(E,+,.)$ est un K-espace vectoriel si $(E,+)$ est un groupe commutatif et si la loi externe satisfait pour tout $\lambda,\mu \in K$ et $x,y \in E$:

$$(\lambda+\mu)\cdot x = \lambda\cdot x + \mu\cdot x, \quad \lambda\cdot(x+y) = \lambda\cdot x + \lambda\cdot y, \quad \lambda\cdot(\mu\cdot x) = (\lambda\mu)\cdot x, \quad 1_K\cdot x = x.$$

Un sous-ensemble non vide F de E est un sous-espace vectoriel de E s'il est stable par les lois de E, c'est-à-dire si pour tout $\lambda \in K$ et $x,y \in F$, on a $\lambda\cdot x + y \in F$.

Exemple 2

Une intersection et une somme de sous-espaces vectoriels de E est un s.e.v de E. On peut donc définir $\mathrm{Vect}(A)$.

Définition 3

Soit $(e_i)_{i\in I}$ une famille d'éléments de E.

- La famille $(e_i)_{i\in I}$ est dite **génératrice** de E lorsque $\mathrm{Vect}((e_i)_{i\in I}) = E$. Lorsque E possède une famille génératrice finie, on dit que E est de dimension finie.
- La famille $(e_i)_{i\in I}$ est dite **libre** lorsque $\forall (\lambda_i)_{i\in I} \in K^I, \quad \sum_{i\in I}\lambda_i e_i = 0 \ \Rightarrow\ \forall i\in I,\ \lambda_i = 0$. Si ce n'est pas le cas, la famille est dite **liée**.
- Si $(e_i)_{i\in I}$ est libre et génératrice, on dit que c'est une **base** de E.
- Soient $(E_i)_{i\in I}$ des sous-espaces vectoriels de E. On dit que E est la **somme directe** des $(E_i)_{i\in I}$ si $\sum_{i\in I} E_i = E$ et si la décomposition de tout vecteur de E dans $(E_i)_{i\in I}$ est unique.

Exemple 4

1. $\{1,\sqrt{2},\sqrt{3}\}$ est libre sur le $\mathbb{Q}$-espace vectoriel $\mathbb{R}$.
2. La base canonique de $E = \mathbb{K}^n$
3. Une sous-famille(/sur) d'une famille libre(/génératrice) de E est libre (/génératrice)
4. $\mathbb{K}[X]$ n'est pas de dimension finie,
5. Il y a unicité de la décomposition de $x \in \mathrm{Vect}((e_i)_{i\in I})$ lorsque $(e_i)_{i\in I}$ est libre.

Théorème 5 – Théorème de la base incomplète/extraite

Soient L une famille libre et G une famille génératrice de E. Alors il existe une base B de E telle que $L \subset B \subset L \cup G$.

Corollaire 6

Si E est de dimension finie, il admet une base. De plus, toute base de E a même cardinal, appelé **dimension** de E, et noté $\dim(E)$. Toute famille libre (resp. génératrice) est de cardinal inférieur (resp. supérieur) ou égal à $\dim(E)$ et en cas d'égalité, c'est une base.

Proposition 7

Soient E de dimension finie n, et F_1, F_2 des sous-espaces vectoriels de E.

- F_1 est de dimension finie et $\dim(F_1) \le \dim(E)$, et
$$\dim(F_1) = \dim(E) \iff F_1 = E.$$
- **Formule de Grassmann :**
$$\dim(F_1+F_2) + \dim(F_1\cap F_2) = \dim(F_1) + \dim(F_2).$$
- F_1 et F_2 sont **supplémentaires** dans E (c'est-à-dire $E = F_1 \oplus F_2$) si et seulement si au moins deux des trois propriétés suivantes sont vérifiées :
$$\dim(E) = \dim(F_1) + \dim(F_2), \qquad F_1 \cap F_2 = \{0\}, \qquad E = F_1 + F_2.$$

II. Rang d'une application linéaire [Gourdon]

Soient E, G des espaces vectoriels de dimension finie n et m.

II.A. Applications linéaires [Gourdon, Mansuy, Objectif Agreg]

Définition 8

$f : E \to G$ est linéaire si $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$ pour $\lambda,\mu \in K$ et $x,y \in E$.
On note $L(E,G)$ l'ensemble des applications linéaires de E dans G et $L(E) = L(E,E)$.

Remarque 9

$\mathrm{Im}(f)$ et $\ker(f)$ sont des s.e.v. et $\dim(\mathrm{Im}(f)) \le \dim(E) < +\infty$.
Une application linéaire est entièrement déterminée par ses valeurs sur une base de E.

Définition 10

Pour $f \in L(E,G)$, on note $\mathrm{rg}(f)$ et on appelle *rang* de f l'entier $\dim(\mathrm{Im}(f))$.

Théorème 11 – Théorème du rang

Soit $f \in L(E,G)$. Alors $\dim(\ker(f)) + \mathrm{rg}(f) = \dim(E)$.

Application 12

PREUVE DANS R.MANSUY et R.MNEIMNÉ : Algèbre linéaire : Réduction des endomorphismes Pour $f \in L(E)$:

- $(\mathrm{rg}(f^k))_{k\in\mathbb{N}}$ est décroissante stationnaire et $(\mathrm{rg}(f^k) - \mathrm{rg}(f^{k+1}))_{k\in\mathbb{N}}$ est décroissante.
- Il existe $P \in K_{\dim(E)^2+1}[X]$ tel que $P(f) = 0_{L(E)}$.

Corollaire 13

Lorsque $n = m$, on a f bijective $\iff$ f surjective $\iff$ f injective.

Application 14

Contre-exemple en dimension finie : $P \mapsto P'$. BONUS : Existence et unicité du polynôme interpolateur de Lagrange (OBJECTIF AGREG).

II.B. Représentations matricielles d'une application linéaire

Définition 15

Soit $f \in L(E,G)$. Si $B = (e_1, \dots, e_n)$ et C sont des bases de E et G, on définit la matrice $M_{B,C}(f) \in M_{m,n}(K)$ de f dans les bases B et C comme la matrice de vecteurs colonnes $(f(e_i))_{1 \leq i \leq n}$ exprimés dans la base C.

Définition 16

On définit $\mathrm{rg}(A)$, le rang de $A \in M_{m,n}(K)$, comme le rang de la famille de ses vecteurs colonnes $(x_1, \dots, x_n)$, c'est-à-dire l'entier $\dim(\mathrm{Vect}((x_i)_{1 \leq i \leq n}))$.

Proposition 17

Si $A \in M_{m,n}(K)$ est de rang r, alors A est équivalente à $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

Corollaire 18

Deux matrices sont équivalentes si et seulement si elles ont même rang.

Proposition 19

Le rang d'une matrice est l'ordre du plus grand mineur non nul

Proposition 20

- Pour tout $A \in M_{n,m}(K)$, il existe E, G, f et des bases B, C telles que $A = M_{B,C}(f)$.
- Deux matrices de $M_{n,m}(K)$ représentent une même application linéaire $f \in L(E,G)$ dans des bases différentes si et seulement si elles sont équivalentes.
- $\mathrm{rg}(A) = \mathrm{rg}(f)$ lorsque A est une matrice de f.

Application 21

- La méthode du pivot de GAUSS permet d'obtenir le rang d'une matrice. $O(n^3)$
- Soient $M \in M_n(K)$ et $N \in GL_n(K)$. Alors $\mathrm{rg}(MN) = \mathrm{rg}(NM) = \mathrm{rg}(M)$.

II.C. Déterminant [Rombaldi]

Proposition 22

L'espace vectoriel $\mathcal{A}_n(E, \mathbb{K})$ des formes n-linéaires alternées est de dimension 1 engendré par l'application $\det_{\mathcal{B}} : E^n \to \mathbb{K}$ définie par :

$$\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod x_{\sigma(i),i}$$

où $x_j = \sum_{i=1}^{n} x_{ij} e_i$.

On dit alors que $\det_{\mathcal{B}}(x_1, \dots, x_n)$ est le déterminant dans la base $\mathcal{B}$ de $(x_1, \dots, x_n)$.

Proposition 23 – Relation de Chasles

Si $\mathcal{B}' = (e'_i)_{i \in [\![1,n]\!]}$ est une autre base de E, on a alors que pour tout $(x_i)_{i \in [\![1,n]\!]} \in E^n$:

$$\det_{\mathcal{B}'}(x_1, \dots, x_n) = \det_{\mathcal{B}'}(e_1, \dots, e_n) \times \det_{\mathcal{B}}(x_1, \dots, x_n) = \det(\mathcal{B})_{\mathcal{B}'} \times \det_{\mathcal{B}}(x_1, \dots, x_n)$$

Proposition 24

Soit $\mathcal{B}' = (x_i)_{i \in [\![1,n]\!]}$, les assertions suivantes sont équivalentes :

- la famille $\mathcal{B}'$ est liée ;
- pour toute base $\mathcal{B}$ de E, $\det_{\mathcal{B}}(\mathcal{B}') = 0$;
- il existe une base $\mathcal{B}$ de E, $\det_{\mathcal{B}}(\mathcal{B}') = 0$.

Corollaire 25

Soit $\mathcal{B}' = (x_i)_{i \in [\![1,n]\!]}$. Cette famille est une base de E si, et seulement si, il existe une base $\mathcal{B}$ de E tel que $\det_{\mathcal{B}}(\mathcal{B}') \neq 0$

Théorème 26

Pour tout endomorphisme $u \in \mathcal{L}(E)$, il existe un scalaire λ_u tel que pour toute forme $\varphi \in \mathcal{A}_n(E, \mathbb{K}) \setminus \{0\}$ et tout $(x_i) \in E^n$, on a :

$$\varphi(u(x_1), \dots, u(x_n)) = \lambda_u \varphi(x_1, \dots, x_n)$$

En particulier, on a $\lambda_u = \det_{\mathcal{B}}(u(e_1), \dots, u(e_n))$, où $\mathcal{B} = (e_i)_{i \in [\![1,n]\!]}$ est une base quelconque de E.

III. Les conséquences de la dimension finie

III.A. Espaces vectoriels normés [Gourdon, Rombaldi]

Soit $(E, \|.\|)$ un espace vectoriel normé réel ou complexe de dimension quelconque (on suppose la notion de norme connue).

Théorème 27 – Théorème de Riesz

E est de dimension finie si et seulement si $B_E(0,1)$ est compacte.

Théorème 28

Si E est de dimension finie, alors toutes les normes sur$E$ sont équivalentes

Exemple 29

Contre-exemple en dimension infinie : $\|\|_1$ et $\|\|_\infty$ sur $\mathcal{C}([0,1], \mathbb{R})$. Ou sur un corps non-complet $\mathbb{Q}[\sqrt{2}], N_1(a + b\sqrt{2}) = |a| + |b|$ et $N_2 = |.|$

Corollaire 30

Si E est de dimension finie, les compacts de E sont les fermés bornés.

Théorème 31 – Orthogonalisation de Gram-Schmidt (ROMBALDI)

Supposons que $\|.\|$ dérive d'un produit scalaire $\langle ., . \rangle$ (E est alors un espace euclidien).
Pour toute famille libre $(x_i)_{1 \leq i \leq p}$ de E, il existe une unique famille orthonormée $(e_i)_{1 \leq i \leq p}$ telle que, pour tout $k \in \{1, \dots, p\}$, $\mathrm{Vect}(e_1, \dots, e_k) = \mathrm{Vect}(x_1, \dots, x_k)$ et $\langle x_k, e_k \rangle > 0$.

III.B. Dualité [Rombaldi]

Définition 32

On note $E^* = L(E, K)$ l'espace dual de E.
À toute base $B = (e_1, \dots, e_n)$ de E, on associe la famille $B^* = (e_1^*, \dots, e_n^*)$ de E^*, où e_i^* est la projection sur $\mathrm{Vect}(e_i)$ parallèlement à $\mathrm{Vect}((e_j)_{j \neq i})$.

Proposition 33

B^* est une base de E^*, appelée **base duale** de B. Ainsi, E^* est de dimension finie et $\dim(E^*) = \dim(E)$.
Par ailleurs, toute base de E^* est la base duale d'une unique base B de E.

Application 34

Application théorème du rang : Si $\phi \in E^*$ est non identiquement nulle, son noyau est un **hyperplan** H.
Si $\phi_1, \dots, \phi_p \in E^*$, alors $\dim\left(\bigcap_{i=1}^p \ker(\phi_i)\right) = \dim\left(\bigcap_{i=1}^p H_i\right) \geq n - p$.

Définition 35

— L'orthogonal dans E^* de $\{0\} \subset X \subset E$ est $X^\perp = \{\phi \in E^* \mid \forall x \in X,\ \phi(x) = 0\}$.
— L'orthogonal dans E de $\{0\} \subset Y \subset E^*$ est $Y^\circ = \{x \in E \mid \forall \phi \in Y,\ \phi(x) = 0\}$.
Ce sont des sous-espaces vectoriels de E^* et E respectivement.

Proposition 36

Si F est un sous-espace vectoriel de E, alors $\dim(F) + \dim(F^\perp) = \dim(E)$.
De même, si G est un sous-espace vectoriel de E^*, $\dim(G) + \dim(G^\circ) = \dim(E)$.

Définition 37

Pour $f \in L(E, F)$, on définit l'application transposée ${}^t f : F^* \to E^*$, $\phi \mapsto \phi \circ f$.

Application 38

Si $A = M_{B,C}(f)$, alors $M_{B^*,C^*}({}^t f) = A^\top$.
On en déduit que ${}^t(v \circ u) = {}^t u \circ {}^t v$.

IV. Applications des espaces vectoriels de dimension finie

IV.A. Réduction des endomorphismes[Mansuy, ROMBALDI]

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n. On suppose les notions de polynôme d'endomorphisme et de valeurs/vecteurs/espaces propres connues.

Lemme 39

Soit $f \in L(E)$ et $(P_k)_{1 \leq k \leq N}$ une famille de polynômes deux à deux premiers entre eux. On pose $P = \prod_{k=1}^N P_k$.
Alors :

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

De plus, le projecteur de $\ker(P(f))$ sur l'un de ces sous-espaces parallèlement à la somme des autres est un polynôme en f.

Exemple 40

En pratique, on utilise souvent ce lemme avec P tel que $\ker(P(f)) = E$. On obtient alors une décomposition de E en sous-espaces stables, car $\ker(Q(f))$ est stable par f pour tout polynôme Q.

Définition 41

On définit le polynôme caractéristique de $A \in M_n(K)$ par $\chi_A(X) = \det(XI_n - A)$.
On définit le polynôme caractéristique de $f \in L(E)$ comme le polynôme caractéristique d'une matrice de f dans n'importe quelle base de E (en remarquant que χ_A est invariant par similitude). On le note χ_f.

Théorème 42 – Théorème de Cayley-Hamilton

Pour tout $f \in L(E)$, $\chi_f(f) = 0$ ou encore $\pi_f | \chi_f$.

Théorème 43 – Caractérisation d'un endomorphisme trigonalisable

Un endomorphisme $f \in L(E)$ est trigonalisable si et seulement si χ_f est scindé.

Théorème 44

Caractérisation des endomorphismes diagonalisables avec la multiplicité géométriques et algébriques.

Théorème 45

Réduction des endomorphismes normaux

Théorème 46

Réduction de Frobenius + application au commutant

IV.B. Extensions de corps et nombres algébriques

On ne considère que des corps commutatifs.

Définition 47

Soient K et L deux corps tels que $K \subset L$. On dit que L est une **extension de corps** de K.
L est alors un K-espace vectoriel. Lorsque $\dim(L)$ est fini, on note $[L : K] = \dim(L)$ et on l'appelle le **degré de L sur K**. On dit alors que l'extension est **finie**.

Exemple 48

$\mathbb{R} \subset \mathbb{C}, \mathbb{Q} \subset \mathbb{Q}(i)$.

Théorème 49 – Théorème de la base télescopique

Soient $\mathbb{K}, \mathbb{L}, \mathbb{M}$ des corps, $(e_i)_{i \in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j \in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors $(e_i f_j)_{(i,j) \in I \times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.
En particulier, lorsque deux des degrés d'extensions sont finis, le troisième l'est aussi et on a

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$$

Définition 50

Soit $\mathbb{L}$ une extension de $\mathbb{K}$, soit $\alpha \in \mathbb{L}$. Soit $\phi : \mathbb{K}[T] \to \mathbb{L}$ le morphisme d'anneaux tel que $\phi|_{\mathbb{K}} = \mathrm{id}$ et $\phi(T) = \alpha$.
Si ϕ est injectif, on dit que α est **transcendant** sur $\mathbb{K}$. Sinon, $\alpha \in \mathbb{L}$ est **algébrique** sur $\mathbb{K}$ et $P \in \mathbb{K}[X]$ unitaire tel que $\ker(\phi) = (P)$. P est appelé **polynôme minimal** de α.

Exemple 51

$\sqrt{2}, i$ sont algébriques sur $\mathbb{Q}$. e et π sont transcendants sur $\mathbb{Q}$.

Théorème 52 – Caractérisation d'un algébrique

Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Pour $\alpha \in \mathbb{L}$, on a : α est algébrique sur $\mathbb{K} \iff \mathbb{K}[\alpha] = \mathbb{K}(\alpha) \iff \dim(\mathbb{K}[\alpha]) < +\infty$.

Annexe

Exemple du pivot de Gauss, shcémas de degrés d'extensions de corps
Références :
— Gourdon Algèbre,

— R.MANSUY et R.MNEIMNÉ : Algèbre linéaire Réduction des endomorphismes

— Perrin,

— Rombaldi ,

— Objectif agreg
— Odile Fleury Algèbre et calcul Formel

Table des matières

I Espaces vectoriels et dimension [Gourdon] **1**

II. Rang d'une application linéaire[Gourdon] **1**
II.A. Applications linéaires 1
II.B. Représentations matricielles d'une application linéaire 2

III. Les conséquences de la dimension finie **2**
III.A. Espaces vectoriels normés 2
III.B. Dualité 2

IV. Applications des espaces vectoriels de dimension finie **3**
IV.A. Réduction des endomorphismes 3
IV.B. Extensions de corps et nombres algébriques 3

Leçon n° 149 : Déterminant Exemples et applications.

Piroutet Alban

28 juillet 2026

Soit $\mathbb{K}$ un corps et E un $\mathbb{K}$-espace vectoriel de dimension $n \geq 1$.

I Notions de déterminant

I.A) Des formes p-linéaires au déterminant [Gourdon]

Définition 1
Forme p-linéaire et espace $\mathcal{L}_p(E, \mathbb{K})$

Définition 2
Formes alternées ($\mathcal{A}_p(E, \mathbb{K})$) et formes antisymétrique.

Théorème 3
Si car($\mathbb{K}$) $\neq 2$, une forme est antisymétrique si et seulement si elle est alternée.

Corollaire 4
Si $(x_1, \ldots, x_p)$ est une famille liée, alors $f(x_1, \ldots, x_p) = 0$.

Théorème 5
$\dim(\mathcal{A}_n(E, \mathbb{K})) = 1$, on définit le déterminant d'une base et l'expression du déterminant pour une famille de vecteurs quelconque.

Proposition 6
Changement de base

Proposition 7
Une famille est liée si, et seulement si, son déterminant est nul.

I.B) Déterminant d'une matrice carrée, d'un endomorphisme[Gourdon]

Définition 8
Déterminant d'une matrice carrée.

Remarque 9
On peut considérer les matrices à coefficients dans un anneau A intègre car A se prolonge dans $Frac(A)$.

Proposition 10
Propriétés du déterminant d'une matrice

Définition 11
Déterminant d'un endomorphisme indépendant du choix de la base

Remarque 12
Lien entre le déterminant d'un endomorphisme et d'une matrice : $\det(f) = \det(\mathcal{M}_{\mathcal{B}}(f))$.

Remarque 13
On peut définir le déterminant dans un anneau intègre quelconque en passant dans le corps des fractions.

I.C. Propriétés analytiques et topologiques [Gourdon Analyse, PGCD]

Proposition 14
Le déterminant est une application polynômiale donc est de classe $\mathcal{C}^\infty$.

Corollaire 15
$\mathcal{GL}_n(\mathbb{K})$ est ouvert et $\mathcal{SL}_n(\mathbb{K})$ est fermé.

Proposition 16
Différentielle du déterminant sur $\mathcal{M}_n(\mathbb{R})$: $d_M(\det)(H) = Tr(Com(M)^T\ H)$

II.Méthodes de calcul de déterminant

II.A. Mineurs, cofacteur [Gourdon]

Définition 17
Mineurs

Proposition 18
Développement par rapport à une ligne ou à une colonne.

Définition 19
Commatrice

Proposition 20
Relation : $A\ {}^t(Com(A)) = \det(A) I_n$

Corollaire 21
Expression de l'inverse en fonction de la commatrice.

Application 22
$A \mapsto A^{-1}$ est continue + calcul de la différentielle

II.B. Cas simple, Pivot de Gauss [Gourdon, Objectif agreg]

Exemple 23
Matrice carrée de taille 2 et 3

Proposition 24
Déterminant d'une matrice triangulaire supérieure.

Application 25
Pivot de Gauss et complexité du calcul du déterminant dans un corps.

Application 26

Soit $M \in \mathcal{M}_n(\mathbb{Z})$, on considère

$$H = \max_{i,j \in \{1,\dots,n\}} |m_{i,j}|$$

et prenons des nombres premiers distincts $p_1, \dots, p_r$ tels que

$$p_1 \cdots p_r > 2n! H^n$$

(de telle sorte que $|\det(M)| < p_1 \cdots p_r$).
On calcule ensuite $\det(M)$ dans $\mathbb{F}_{p_i}$ pour tout i, et, par le théorème des restes chinois, on obtient $\det(M)$ dans $\mathbb{Z}$.

Exemple 27

Calcul de déterminant à l'aide du pivot de Gauss.

II.C. Déterminants remarquables [Gourdon]

Exemple 28

Déterminant de Vandermonde

Exemple 29

Déterminant circulant

Application 30

Suite de polygones.

III. Applications à d'autres domaines des mathématiques

III.A. Interprétation géométrique du déterminant [Objectif agreg, Francinou 3]

Théorème 31

Volume et déterminant dans $\mathbb{R}^n$.

Application 32

Volume d'un parallélépipède

Proposition 33

Volume maximal via l'inégalité de Hadamard.

Proposition 34

Déterminant de Gram et distance à un sev.

Théorème 35

Théorème de changement de variable et Jacobienne

III.B. Résultant [Rombaldi+ SAUX-Picard calcul formel]

Définition 36

Résultant

Théorème 37

A et B sont premiers entre eux si, et seulement si $Res(A, B) \neq 0$.

Application 38

Si $\mathbb{K}$ est un corps et $\mathbb{L}$ une extension, $\mathbb{M} = \{x \in \mathbb{L}, x \text{ algébrique sur } \mathbb{K}\}$ est un sous-corps de $\mathbb{L}$.

Application 39

L'ensemble $D_n'(\mathbb{C})$ des matrices diagonalisables admettant n valeurs propres distinctes est ouvert.

Application 40

Paramétrisation rationnelle du cercle

III.C. En algèbre linéaire [Rombaldi]

Définition 41

Polynôme caractéristique

Théorème 42

Théorème de Cayley-Hamilton

Application 43

Les valeurs propres sont les racines, $A \mapsto \chi_A$ est continue, et l'ensemble des matrices nilpotentes est fermé.

Références :

— Gourdon Algèbre, Analyse

— Rombaldi,

— Francinou Algèbre 3,

— Objectif Agreg,

— PGCD Rouvière

Table des matières

I Notions de déterminant **1**

I.A Des formes p-linéaires au déterminant [Gourdon] 1

I.B Déterminant d'une matrice carrée, d'un endomorphisme[Gourdon] 1

I.C Propriétés analytiques et topologiques [Gourdon Analyse, PGCD] 1

II.Méthodes de calcul de déterminant **1**

II.A. Mineurs, cofacteur [Gourdon] 1

II.B. Cas simple, Pivot de Gauss[Gourdon, Objectif agreg] 1

II.C. Déterminants remarquables[Gourdon] 2

III. Applications à d'autres domaines des mathématiques **2**

III.A. Interprétation géométrique du déterminant [Objectif agreg, Francinou 3] 2

III.B. Résultant[Rombaldi] 2

III.C. En algèbre linéaire [Rombaldi]2

Leçon n° 150 : Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

Piroutet Alban

28 juillet 2026

Soit $\mathbb{K}$ un corps commutatif, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$. Soit $f \in \mathcal{L}(E)$.
Pour $P = \sum_{k=0}^{p} a_k X^k \in \mathbb{K}[X]$, on définit $P(f) = \sum_{k=0}^{p} a_k f^k \in \mathcal{L}(E)$.

I Polynômes d'endomorphisme

I.A) L'algèbre $\mathbb{K}[f]$ et polynôme minimal [Mansuy]

Définition 1

L'application $\varphi_f : \mathbb{K}[X] \longrightarrow \mathcal{L}(E), \quad P \longmapsto P(f)$ est un morphisme d'algèbres.
Son noyau, c'est-à-dire l'ensemble des polynômes annulateurs de f, est un idéal de $\mathbb{K}[X]$ principal, donc engendré par un unique polynôme unitaire π_f, appelé polynôme minimal de f.
Son image $\mathbb{K}[f]$ est une sous-algèbre de $\mathcal{L}(E)$.

Remarque 2

Le noyau est non réduit à $\{0\}$ puisque $\mathcal{L}(E)$ est de dimension finie n^2. En dimension infinie, c'est faux (considérer par exemple l'opérateur de dérivation).

Proposition 3

On a $\dim(\mathbb{K}[f]) = \deg(\pi_f)$.

Remarque 4

Se donner $f \in \mathcal{L}(E)$ revient à se donner sa matrice M dans une base de E. On a donc les mêmes résultats pour les matrices, et si M est une matrice de f dans une certaine base, on a $\pi_f = \pi_M$ (donc deux matrices semblables ont même polynôme minimal).

I.B) Polynôme caractéristique [Gourdon, Mansuy, Objectif Agreg]

Définition 5

On définit le polynôme caractéristique de $M \in \mathcal{M}_n(\mathbb{K})$ par $\chi_M(X) = \det(XI_n - M)$.

Exemple 6

En dimension 2, on a $\chi_M = X^2 - \mathrm{Tr}(M)X + \det(M)$ et $\chi_M(M) = 0$.
En dimension quelconque, si $\chi_M = \sum_{k=0}^{n} a_k X^k$, on a $a_n = 1$, $a_{n-1} = -\mathrm{Tr}(M)$ et $a_0 = (-1)^n \det(M)$.

Proposition 7

Deux matrices semblables ont même polynôme caractéristique. On peut donc définir le polynôme caractéristique de f.

Exemple 8

Polynômes caractéristiques usuels

Proposition 9

Pour $A, B \in \mathcal{M}_n(\mathbb{C})$, on a $\chi_{AB} = \chi_{BA}$.

Proposition 10

Pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $M \mapsto \chi_M$ est continue.

Application 11

L'ensemble des matrices nilpotentes est fermé pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I.C. Polynômes d'endomorphisme et sous-espaces stables [Mansuy]

Proposition 12

Soient $f, g \in \mathcal{L}(E)$ tels que f et g commutent. Alors $\ker(f)$ et $\mathrm{Im}(f)$ sont stables par g. En particulier, $\ker(P(f))$ et $\mathrm{Im}(P(f))$ sont stables par f pour tout $P \in \mathbb{K}[X]$.

Lemme 13

Soit $(P_i)_{1 \le i \le r}$ une famille de polynômes deux à deux premiers entre eux. Alors en posant $P = \prod_{i=1}^{r} P_i$, on a

$$\ker(P(f)) = \bigoplus_{i=1}^{r} \ker(P_i(f)).$$

De plus, le projecteur de $\ker(P(f))$ sur l'un de ces sous-espaces parallèlement à la somme des autres est un polynôme en f.

Application 14

Soit P un polynôme annulateur de f. Si $P = \prod_{i=1}^{r} P_i^{\alpha_i}$ où les $(P_i)_{1 \le i \le r}$ sont deux à deux premiers entre eux, alors on a la décomposition en sous-espaces f-stables

$$E = \bigoplus_{i=1}^{r} \ker(P_i^{\alpha_i}(f)).$$

I.D. Liens entre polynômes et valeurs propres [Mansuy]

Proposition 15

Soit F un sous-espace f-stable de E. On pose f_F l'endomorphisme induit sur F par f. Alors :

$$\pi_{f_F} \mid \pi_f \quad \text{et} \quad \chi_{f_F} \mid \chi_f.$$

Si $E = \bigoplus_{i=1}^{r} E_i$ est une décomposition en sous-espaces stables de E, alors

$$\chi_f = \prod_{i=1}^{r} \chi_{f|E_i}.$$

Exemple 16

Ce dernier résultat n'est pas vrai pour le polynôme minimal ! Si $f = \mathrm{Id}_E$ et $(e_1, \ldots, e_n)$ est une base de E, alors

$$E = \bigoplus_{i=1}^{n} \mathrm{Vect}(e_i), \quad \pi_{f|\,\mathrm{Vect}(e_i)} = X - 1 \quad \text{mais} \quad \pi_f = X - 1.$$

Proposition 17

$\lambda \in \mathbb{K}$ est une valeur propre de f si et seulement si $\chi_f(\lambda) = 0$ si et seulement si $\pi_f(\lambda) = 0$.

Exemple 18

Pour $P = X^n + \sum_{k=0}^{n-1} a_k X^k$, on définit $C(P)$, la matrice compagnon de P, par

$$C(P) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

On a alors $\chi_{C(P)} = \pi_{C(P)} = P$.

Théorème 19 – Caley-Hamilton

χ_f est un polynôme annulateur de f. Autrement dit, $\pi_f \mid \chi_f$.

II. Application à la réduction d'endomorphismes

II.A. Trigonalisation et diagonalisation [Mansuy, Gourdon]

Définition 20

Soit $\lambda \in \mathbb{K}$ une valeur propre de f. On appelle :
- multiplicité géométrique de λ : la dimension de $E_\lambda = \ker(f - \lambda \mathrm{Id})$, notée $\mathrm{mg}(\lambda)$,
- multiplicité algébrique de λ : la multiplicité de λ en tant que racine de χ_f, notée $\mathrm{ma}(\lambda)$,
- multiplicité minimale de λ : la multiplicité de λ en tant que racine de π_f, notée $\mathrm{mm}(\lambda)$.

Proposition 21

On a $\mathrm{mm}(\lambda) \leq \mathrm{mg}(\lambda)$ et $\mathrm{ma}(\lambda) \leq \mathrm{mg}(\lambda)$.

Définition 22

On dit que f est trigonalisable (resp. diagonalisable) s'l existe une base de E telle que la matrice de f dans cette base soit triangulaire (resp. diagonale).

Théorème 23

f est trigonalisable si et seulement si χ_f est scindé si et seulement si π_f est scindé si et seulement si f admet un polynôme annulateur scindé.

Exemple 24

Un endomorphisme nilpotent est trigonalisable. Dans une base adéquate, la matrice est même triangulaire supérieure puisque les valeurs propres d'un endomorphisme trigonalisable sont les coefficients diagonaux de sa matrice dans une base de trigonalisation.

Théorème 25

f est diagonalisable si et seulement si π_f est scindé à racines simples ($\mathrm{mm}(\lambda) = 1$ pour toute valeur propre λ de f), si et seulement si f admet un polynôme annulateur scindé à racines simples, si et seulement si $\mathrm{ma}(\lambda) = \mathrm{mg}(\lambda)$ pour toute valeur propre λ.

Exemple 26

Un endomorphisme trigonalisable ayant des valeurs propres deux à deux distinctes ($m_g(\lambda) = 1$) est diagonalisable.

Théorème 27 – Décomposition de Dunford

Supposons f de polynôme caractéristique scindé. Alors il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que d est diagonalisable, n est nilpotent, $f = d + n$ et d commute avec n. De plus, d et n sont des polynômes en f.

Application 28

Soit $M \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique scindé. On note $\mu_1, \ldots, \mu_n$ les n racines de χ_M (pas nécessairement distinctes). Soit (D, N) la décomposition de Dunford de M. Soit $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $P^{-1}DP = \Delta = \mathrm{diag}(\mu_1, \ldots, \mu_n)$ soit diagonale.
Alors on a :

$$\exp(A) = P\,\mathrm{diag}(e^{\mu_1}, \ldots, e^{\mu_n})P^{-1} \sum_{k=0}^{n-1} \frac{N^k}{k!}.$$

II.B. Décomposition de sous-espaces stables [Mansuy]

Théorème 29 – Décomposition de Jordan

Supposons f de polynôme caractéristique scindé. Notons $\lambda_1, \ldots, \lambda_r$ ses valeurs propres.
Il existe des entiers $d_{j,1} \geq \cdots \geq d_{j,\ell_j}$ pour $j \in \{1, \ldots, r\}$ tels que dans une certaine base B de E, $M_B(f)$ soit diagonale par blocs avec les blocs $(B_{j,k})_{1 \leq j \leq r,\, 1 \leq k \leq \ell_j}$, où

$$B_{j,k} = \lambda_j \mathrm{Id}_{d_{j,k}} + J_{d_{j,k}}, \quad \text{avec } J_d = C(X^d) \in \mathcal{M}_d(\mathbb{K}).$$

Application 30

Deux endomorphismes scindés sont semblables si et seulement si ils ont même décomposition de JORDAN.

Définition 31

Soit $x \in E$. $\varphi_{f,x} : \mathbb{K}[X] \longrightarrow E$, $P \mapsto P(f)(x)$ est un morphisme d'espaces vectoriels.
Son noyau est un idéal de $\mathbb{K}[f]$ engendré par un unique polynôme unitaire $\pi_{f,x}$, appelé **polynôme minimal local** de f en x. On note $E_{f,x}$ son image.
Lorsque $E = E_{f,x}$ pour au moins un $x \in E$, on dit que f est cyclique.

Proposition 32

Pour tout $x \in E$, $E_{f,x}$ est un sous-espace f-stable et $B_x = (x, f(x), \ldots, f^p(x))$, où $p = \dim(E_{f,x})$, en est une base.

Lemme 33

Il existe $x \in E$ tel que $\mu_{f,x} = \mu_f$. Pour un tel x, $E_{f,x}$ admet alors un supplémentaire f-stable.

Théorème 34 – Décomposition de Frobenius

Il existe une unique suite finie de polynômes unitaires $P_1, \ldots, P_r$, appelés **invariants de similitude**, et une décomposition $E = \bigoplus_{i=1}^r E_i$ en sous-espaces stables de E telles que :
- $P_{i+1} \mid P_i$ pour tout $1 \leq i \leq r-1$, - $f|_{E_i}$ est cyclique de polynôme minimal P_i pour tout $1 \leq i \leq r$.

Remarque 35

f est quelconque ici (contrairement à la décomposition de Jordan). On a $P_1 = \pi_f$ et $\prod_{i=1}^r P_i = \chi_f$.

Application 36

Deux endomorphismes sont semblables si et seulement si ils ont les mêmes invariants de similitudes.

Exemple 37

Déterminant circulant

Application 38

Suite de polygones.

III. Calculs pratiques avec des polynômes d'endomorphismes

III.A. Calculs d'inverses, de puissances [Mansuy]

Proposition 39

Si f admet un polynôme annulateur $P = \sum_{k=0}^{p} a_k X^k$ tel que $a_0 = P(0) \neq 0$, alors f est inversible et

$$f^{-1} = -\frac{1}{a_0} \sum_{k=0}^{p} a_k f^{k-1} \in \mathbb{K}[f].$$

Corollaire 40

f est inversible si et seulement si 0 n'est pas racine de π_f.

III.B. Exponentielle de matrices [Rombaldi]

On suppose ici que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Définition 41 – Exponentielle de matrice

Proposition 42

$e^A \in GL_n(\mathbb{K})$ avec $(e^A)^{-1} = e^{-A}$

Application 43

Calcul de l'exponentielle matricielle avec décomposition de Dunford.

Application 44

Résolution de $Y' = AY$

Proposition 45

L'exponentielle matricielle complexe est surjective.

Application 46

Calcul d'exponentielle avec la technique du polynôme annulateur

f	π_f	χ_f
nilpotent d'indice k	X^k	X^n
homothétie de rapport λ	$X - \lambda$	$(X-\lambda)^n$
projecteur sur F	$X^2 - X$	$(X-1)^p X^{n-p}$
symétrie par rapport à F	$X^2 - 1$	$(X-1)^p (X+1)^{n-p}$

Références :

— Rombaldi

— Objectif agrégation,

— R. MANSUY et R. MNEIMNÉ : Algèbre linéaire : Réduction des endomorphismes,

— Gourdon

Table des matières

I Polynômes d'endomorphisme **1**
- I.A L'algèbre $\mathbb{K}[f]$ et polynôme minimal [Mansuy] . . . 1
- I.B Polynôme caractéristique [Gourdon, Mansuy, Objectif Agreg] . . . 1
- I.C. Polynômes d'endomorphisme et sous-espaces stables . . . 1
- I.D. Liens entre polynômes et valeurs propres . . . 1

II. Application à la réduction d'endomorphismes **2**
- II.A. Trigonalisation et diagonalisation . . . 2
- II.B. Décomposition de sous-espaces stables . . . 2

III. Calculs pratiques avec des polynômes d'endomorphismes **3**
- III.A Calculs d'inverses, de puissances . . . 3
- III.B. Exponentielle de matrices . . . 3

Leçon n° 151 : SOUS-ESPACES STABLES PAR UN ENDOMORPHISME OU UNE FAMILLE D'ENDOMORPHISMES D'UN ESPACE VECTORIEL DE DIMENSION FINIE. APPLICATIONS. .

Piroutet Alban

28 juillet 2026

Soit $\mathbb{K}$ un corps commutatif, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$. Soit $f \in \mathcal{L}(E)$.

I Sous-espace stables par un endomorphisme

I.A) Définitions et premières propriétés [Mansuy]

Définition 1

Un sous-espace vectoriel F de E est dit *f-stable* si $f(F) \subset F$. On note alors $f_{|F} : F \longrightarrow F,\ x \longmapsto f(x)$, l'endomorphisme induit de f sur F.

Exemple 2

f est une homothétie si et seulement si f laisse stable toute droite.

Proposition 3

Soit $g \in \mathcal{L}(E)$ commutant avec f. Alors $\mathrm{Im}(f)$, $\ker(f)$ et $\ker(P(f))$ pour tout $P \in K[X]$ sont g-stables.

Corollaire 4

En particulier $E_\lambda = \ker(f - \lambda \mathrm{id}_E)$ est f-stable pour tout $\lambda \in K$. E_λ est le sous-espace propre associé à λ. S'il est non réduit à $\{0\}$, on dit que λ est une valeur propre de f.

Proposition 5

Caractérisation matricielle des sous-espaces stables.

Proposition 6

Si F est f-stable, alors $\pi_{f_{|F}} \mid \pi_f$ et $\chi_{f_{|F}} \mid \chi_f$.

Application 7

χ_f est irréductible si et si seulement si f n'admet pas de sous-espace stable non trivial.

Proposition 8

Les sous-espaces propres et caractéristique de f sont stables par f.

I.B. Sous-espaces cycliques [Mansuy]

Soit $x \in E$

Définition 9 – Polynôme minimal local, sous-espace cyclique

L'application $\varphi_{f,x} : \mathbb{K}[X] \longrightarrow E,\ P \longmapsto P(f)(x)$ est un morphisme d'espaces vectoriels. Son noyau est un idéal de $\mathbb{K}[X]$. Il est engendré par un unique polynôme unitaire $\pi_{f,x}$ appelé polynôme minimal local de f en x. On note $E_{f,x}$ son image.

Définition 10

On dit que f est cyclique s'il existe $x \in E$ tel que $E = E_{f,x}$

Exemple 11

Si $n = 2$, tout endomorphisme est soit cyclique, soit une homothétie.

Proposition 12

Supposons f cyclique et soit x tel que $E = E_{f,x}$. Alors

$$M_{B_x}(f) = C(\pi_{f,x}) = \begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & & & \vdots & \vdots \\ 0 & \ddots & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & \ddots & \vdots & \vdots \\ \vdots & & & 1 & 0 & -a_{n-2} \\ 0 & \cdots & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$$ où $\pi_{f,x} = X^n + \sum_{k=0}^{n-1} a_k X^k$. C'est une matrice appelée *matrice compagnon* de $\pi_{f,x}$. On a alors $\chi_f = \pi_f = \pi_{f,x}$.

Proposition 13

Si f est cyclique, l'ensemble des endomorphismes commutant avec f est $\mathbb{K}[f]$

Théorème 14 – Théorème de Cayley-Hamilton

χ_f est un polynôme annulateur de f. Autrement dit, $\pi_f | \chi_f$.

II. Détermination de sous-espaces stables et réduction

II.A. Lemme des noyaux et décomposition de Dunford [Mansuy]

Lemme 15 – Lemme des noyaux

Soit $(P_i)_{1 \le i \le r}$ une famille de polynômes deux à deux premiers entre eux. En posant $P = \prod_{i=1}^r P_i$, on a

$$\ker(P(f)) = \bigoplus_{i=1}^{r} \ker(P_i(f)).$$

De plus, le projecteur de $\ker(P(f))$ sur l'un de ces sous-espaces, parallèlement à la somme des autres, est un polynôme en f.

Application 16

Il existe $x \in E$ tel que $\pi_{f,x} = \pi_f$. Donc si $\deg(\pi_f) = n$, alors f est cyclique.

Théorème 17 – Décompostion de Dunford

Soit $f \in \mathcal{L}(E)$ de polynôme caractéristique scindé. Alors il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que :
- d est diagonalisable, n est nilpotent,
- $f = d + n$ et d commute avec n.

De plus, d et n sont des polynômes en f.

Application 18

Soit $M \in M_n(\mathbb{K})$ de polynôme caractéristique scindé. On note $\mu_1, \dots, \mu_n$ les racines de χ_M (comptées sans leur multiplicité). Soit (D, N) la décomposition de Dunford de M. Soit $P \in GL_n(\mathbb{K})$ telle que

$$P^{-1}DP = \Delta = \mathrm{diag}(\mu_1, \dots, \mu_n).$$

Alors on a

$$\exp(M) = P\ \mathrm{diag}(e^{\mu_1}, \dots, e^{\mu_n})\, P^{-1} \sum_{k=0}^{n-1} \frac{N^k}{k!}.$$

Application 19

Résolution de l'équation $Y' = AY$ pour $A \in \mathcal{M}_n(\mathbb{C})$.

II.B. Utilisation de la dualité dans la recherche de sous-espaces propres [Mansuy, Rombaldi p 672]

Définition 20

Pour $A \subset E$, on définit $A^\perp = \{\varphi \in E^* \mid \forall x \in A,\ \varphi(x) = 0\}$, et pour $B \subset E^*$, on définit $B^\circ = \{x \in E \mid \forall \varphi \in B,\ \varphi(x) = 0\}$.

Définition 21

On définit ${}^\top f : E^* \longrightarrow E^*, \qquad \varphi \longmapsto \varphi \circ f$.

Proposition 22

Si B^* est la base duale de B, on a

$$Mat_{B^*}(t_f) = Mat_B(f)^\top.$$

Proposition 23

F est f-stable si et seulement si $F^\perp$ est ${}^\top f$-stable.

Proposition 24

Soit $x \in E$ tel que $\pi_{f,x} = \pi_f$. Alors $E_{f,x}$ admet un supplémentaire f-stable.

II.C. Sous-espaces stables et trigonalisabilité/diagonalisabilté [Mansuy]

Théorème 25

f est trigonalisable si et seulement si χ_f est scindé, si et seulement si π_f est scindé, si et seulement si f admet un polynôme annulateur scindé.

Théorème 26

f est diagonalisable si et seulement si π_f est scindé à racines simples, si et seulement si f admet un polynôme annulateur scindé à racines simples.

Théorème 27 – Trigonalisation/Diagonalisation simultanée

Si u et v commutent et sont diagonalisables (resp. trigonalisables) alors u et v sont codiagonalisables (resp. cotrigonalisables).

Remarque 28

La réciproque est vraie dans le cas diagonalisable mais faux pour le cas trigonalisable.

II.D. Autour des nilpotents et de la décomposition de Jordan [Mansuy, Rombaldi]

Théorème 29 – Décomposition de Jordan

Supposons f de polynôme caractéristique scindé (trigonalisable). Notons $\lambda_1, \dots, \lambda_r$ ses valeurs propres distinctes. Il existe des entiers $d_{j,1} \geq \cdots \geq d_{j,\ell_j}$ pour $j \in [\![1, r]\!]$ tels que, dans une certaine base B de E, $M_B(f)$ soit diagonale par blocs avec les blocs $(B_{j,k})_{1 \leq j \leq r,\, 1 \leq k \leq \ell_j}$, où

$$B_{j,k} = \lambda_j\, \mathrm{Id}_{d_{j,k}} + J_{d_{j,k}}.$$

Théorème 30

Deux endomorphismes trigonalisables sont semblables si et seulement si ils ont même réduction de JORDAN

II.E.Décomposition de FROBENIUS [Mansuy]

Théorème 31 – Décomposition de FROBENIUS

Il existe une unique suite finie de polynômes unitaires $P_1, \dots, P_s$, appelés *invariants de similitude*, et une décomposition

$$E = \bigoplus_{i=1}^{s} E_i$$

en sous-espaces stables de E telle que :

- $P_{i+1} \mid P_i$ pour tout $1 \leq i \leq s-1$,
- $f_{|E_i}$ est cyclique de polynôme minimal P_i pour tout $1 \leq i \leq s$.

Corollaire 32

f et g sont semblables si et seulement si ils ont les mêmes invariants de similitudes.

Corollaire 33

Dans des bases adéquates, la matrice de f est diagonale par blocs avec, pour blocs, les matrices compagnons $(C(P_i))_{1 \leq i \leq s}$. On dit que c'est la *forme réduite* de f.

Application 34

Application au commutant.

II.F. Réduction des endomorphimes normaux [Rombaldi, Gourdon]

Définition 35

Endomorphismes normaux, symétriques, antisymétriques

Théorème 36 – Réduction des endomorphismes normaux

Réduction des endomorphismes normaux.

Corollaire 37

Cas symétrique, antisymétrique et orthogonal.

Table des matières

I Sous-espace stables par un endomorphisme **1**
I.A Définitions et premières propriétés [Mansuy] . . . 1
I.B. Sous-espaces cycliques . . . 1

II. Détermination de sous-espaces stables et réduction **1**
II.A. Lemme des noyaux et décomposition de Dunford . . . 1
II.B. Utilisation de la dualité dans la recherche de sous-espaces propres . . . 2
II.C. Sous-espaces stables et trigonalisabilité/diagonalisabilté . . . 2
II.D. Autour des nilpotents et de la décomposition de Jordan . . . 2
II.E.Décomposition de FROBENIUS . . . 2
II.F. Réduction des endomorphimes normaux . . . 2

Références :

— Objectif Agreg,

— Gourdon Algèbre

— Rombaldi ,

— R.MANSUY et R.MNEIMNÉ : Algèbre linéaire : Réduction des endomorphismes.

— J.-M. Arnaudies, H. Fraysse ‘ . Cours de mathématiques. 3

u	**diagonalisable**	**trigonalisable**	**quelconque**
décomposition	de E suivant les vecteurs propres	de Dunford	de Frobenius
sous-espace stable F	espace propre	espace caractéristique	engendré par un élément
$u_{\|F}$	homothétie	homothétie + nilpotent	cyclique

Leçon n° 152 : Endomorphismes diagonalisables en dimension finie

Piroutet Alban

28 juillet 2026

Soit $\mathbb{K}$ un corps commutatif, E un $\mathbb{K}$ espace vectoriel de dimension finie n.

I Généralités

I.A) Eléments propres [Mansuy algèbre linéaire chap I/IV]

Définition 1

On dit que $\lambda \in \mathbb{K}$ est une valeur propre de f si $E_\lambda = \ker(f - \lambda \mathrm{Id}_E)$ n'est pas réduit à $\{0\}$. E_λ est appelé **sous-espace propre** de f associé à λ, et ses éléments non nuls sont les **vecteurs propres** associés à λ. On note $\mathrm{Sp}(f)$ l'ensemble des valeurs propres de f.

Proposition 2

Les sous-espaces propres de f sont f-stables et en somme directe.

I.B) Polynômes d'endomorphismes [[Algèbre linéaire Mansuy, Ch I/IV]]

Pour $P = \sum_{k=0}^{n} a_k X^k$, on pose $P(f) = \sum_{k=0}^{n} a_k f^k \in \mathcal{L}(E)$

Définition 3 – Polynômes minimal

L'application $\varphi_f : \mathbb{K}[X] \longrightarrow \mathcal{L}(E),\ P \longmapsto P(f)$ est un morphisme d'algèbres. Son noyau, l'ensemble des polynômes annulateurs de f, est un idéal de $\mathbb{K}[f]$.

Proposition 4

On a $\dim(\mathbb{K}[f]) = \deg(\pi_f)$

Exemple 5

Polynômes minimaux usuels (voir annexe)

Remarque 6

Se donner un endomorphisme $f \in \mathcal{L}(E)$ revient à se donner sa matrice M dans une base de E. On a donc les mêmes résultats pour les matrices.

Proposition 7

Soient $f, g \in \mathcal{L}(E)$ tels que f et g commutent. Alors $\ker(f)$ et $\mathrm{Im}(f)$ sont stables par g. En particulier, $\ker(P(f))$ et $\mathrm{Im}(P(f))$ sont stables par f pour tout $P \in \mathbb{K}[X]$.

Lemme 8 – Lemme des noyaux

Soit $(P_i)_{1 \le i \le r}$ une famille de polynômes deux à deux premiers entre eux. Alors, en posant $P = \prod_{i=1}^{r} P_i$, on a $\ker(P(f)) = \bigoplus_{i=1}^{r} \ker(P_i(f))$. De plus, le projecteur de $\ker(P(f))$ sur l'un de ces sous-espaces, parallèlement à la somme des autres, est un polynôme en f.

Application 9

Soit P un polynôme annulateur de f. Si $P = \prod_{i=1}^{r} P_i^{\alpha_i}$ où les $(P_i)_{1 \le i \le r}$ sont deux à deux premiers entre eux, alors on a la décomposition en sous-espaces f-stables $E = \bigoplus_{i=1}^{r} \ker\left(P_i^{\alpha_i}(f)\right)$.

I.C. Polynôme caractéristique [Mansuy Algèbre linéaire Ch V/VII, Gourdon Chap 4]

Définition 10

On définit le polynôme caractéristique de $M \in \mathcal{M}_n(\mathbb{K})$ par $\chi_M(X) = \det(XI_n - M)$.

Proposition 11

Deux matrices semblables ont même polynôme caractéristique. On peut donc définir le polynôme caractéristique de f.

Exemple 12

En dimension 2, on a $\chi_M = X^2 - \mathrm{Tr}(M)X + \det(M)$ et $\chi_M(M) = 0$.
En dimension quelconque, si $\chi_M = \sum_{k=0}^{n} a_k X^k$, on a $a_n = 1$, $a_{n-1} = -\mathrm{Tr}(M)$ et $a_0 = (-1)^n \det(M)$.
Polynômes caractéristiques usuels (cf annexe)

I.D. Liens entre polynômes et valeurs propres [Mansuy Chap V/VII]

Proposition 13

Soit F un sous-espace f-stable de E. On pose f_F l'endomorphisme induit sur F par f. Alors $\pi_{f_F} \mid \pi_f$ et $\chi_{f_F} \mid \chi_f$.
Si $E = \bigoplus_{i=1}^{r} E_i$ est une décomposition en sous-espaces stables de E, alors $\chi_f = \prod_{i=1}^{r} \chi_{f|E_i}$.

Proposition 14

$\lambda \in \mathbb{K}$ est une valeur propre de f si et seulement si $\chi_f(\lambda) = 0$ si et seulement si $\pi_f(\lambda) = 0$.

Théorème 15 – Cayley-Hamilton

χ_f est un polynôme annulateur de f. Autrement dit, $\pi_f \mid \chi_f$.

Définition 16

Soit $\lambda \in \mathrm{Sp}(f)$ une valeur propre de f. On appelle :
- multiplicité géométrique de λ : la dimension de E_λ, notée $\mathrm{mg}(\lambda)$,
- multiplicité algébrique de λ : la multiplicité de λ en tant que racine de χ_f, notée $\mathrm{ma}(\lambda)$,
- multiplicité minimale de λ : la multiplicité de λ en tant que racine de π_f, notée $\mathrm{mm}(\lambda)$.

On a $\mathrm{mm}(\lambda) \le \mathrm{mg}(\lambda)$ et $\mathrm{ma}(\lambda) \le \mathrm{mg}(\lambda)$.

II. Diagonalisabilité

II.A. Critères de diagonalisabilité [Mansuy, Algèbre linéaire Ch VIII]

Définition 17

f est diagonalisable s'il existe une base de E formée de vecteurs propres de f (c'est-à-dire si la matrice dans une certaine base de E est diagonale).

Application 18

Les valeurs propres de f sont alors les coefficients diagonaux d'une matrice diagonale associée à f.

Théorème 19

On a équivalence :

— f est diagonalisable

$\iff E = \bigoplus_{\lambda \in \mathrm{Sp}(f)} E_\lambda$

$\iff \pi_f$ est scindé à racines simples

$\iff$ il existe un polynôme annulateur de f scindé à racines simples

$\iff \chi_f$ est scindé et pour tout $\lambda \in \mathrm{Sp}(f)$, $\mathrm{mg}(\lambda) = \mathrm{ma}(\lambda)$.

Application 20

- Si f admet n valeurs propres distinctes, f est diagonalisable.

- Si f n'a qu'une valeur propre, f est diagonalisable si et seulement si f est une homothétie.
- Un projecteur et une symétrie sont diagonalisables.
- Un endomorphisme nilpotent et diagonalisable est nul.
- $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ est diagonalisable sur $\mathbb{C}$ mais pas sur $\mathbb{R}$.
- Si $\mathrm{rg}(f) = 1$, alors f est diagonalisable si et seulement si $\mathrm{Tr}(f) \neq 0$.

Corollaire 21

Si F est f-stable et f est diagonalisable, alors $f_{|F}$ est diagonalisable.

II.B. Co-diagonalisabilité [Mansuy, Algèbre linéaire Ch VIII]

Proposition 22

Soient $f, g \in \mathcal{L}(E)$ tels que f et g commutent. Alors $\mathrm{Im}(f)$ et les sous-espaces propres de f sont stables par g.

Proposition 23

Soit $(f_k)_{1 \leq k \leq N}$ une famille d'endomorphismes diagonalisables commutant deux à deux. Alors il existe une base commune de diagonalisation (on dit que les $(f_k)_{1 \leq k \leq N}$ sont **co-diagonalisables**).

Application 24

Soient $A, B \in \mathcal{M}_n(\mathbb{R})$ diagonalisables. Alors $\Theta \in \mathcal{L}(\mathcal{M}_n(\mathbb{R}))$ définie par $\Theta(M) = AMB$ est diagonalisable.

Exemple 25

Soit G un sous-groupe fini abélien de $\mathrm{GL}_n(\mathbb{C})$. Alors les éléments de G sont co-diagonalisables. Donc G est conjugué à un sous-groupe de matrices diagonales.

II.C. Propriétés topologiques sur $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ [Objectif Agreg p 179/ 217]

Proposition 26

Pour $\lambda \in \mathrm{Sp}(f)$, $|\lambda| \leq \|f\|$, où $\|\,.\,\|$ est la norme subordonnée à n'importe quelle norme sur E.

Proposition 27

Pour $A, B \in \mathcal{M}_n(\mathbb{C})$, on a $\chi_{AB} = \chi_{BA}$.

Proposition 28

$M \mapsto \chi_M$ est continue.

Application 29

L'ensemble des matrices nilpotentes est fermé.

Proposition 30

$\overline{\mathcal{D}_n(\mathbb{K})} = \mathcal{T}_n(\mathbb{K})$. En particulier, $\mathcal{D}_n(\mathbb{C})$ est dense dans $\mathcal{M}_n(\mathbb{C})$.

Théorème 31

L'exponentielle induit un homéomorphisme entre $S_n(\mathbb{R})$ et $S_n^{++}(\mathbb{R})$

II.D Décomposition de Dunford [Gourdon, Mansuy]

Théorème 32

Soit $f \in \mathcal{L}(E)$ de polynôme caractéristique scindé. Alors il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que d est diagonalisable, n est nilpotent, $f = d + n$ et d commute avec n. De plus, d et n sont des polynômes en f.

Application 33

Soit $M \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique scindé. On note $\mu_1, \ldots, \mu_n$ les n racines de χ_M (comptées sans leur multiplicité). Soit (D, N) la décomposition de Dunford de M. Soit $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $P^{-1}DP = \Delta = \mathrm{diag}(\mu_1, \ldots, \mu_n)$ soit diagonale.
Alors on a :

$$\exp(M) = P\ \mathrm{diag}(e^{\mu_1}, \ldots, e^{\mu_n})\, P^{-1} \sum_{k=0}^{n-1} \frac{N^k}{k!}.$$

Exemple 34

Un endomorphisme nilpotent et diagonalisable est nul.

II.E. Application aux portraits de phase [Berthelin]

On se place dans le cas où $A \in \mathcal{M}_2(\mathbb{R})$

Application 35

Classification des portraits de phase du système différentiel $Y' = AY$ où $Y = \begin{pmatrix} x \\ y \end{pmatrix}$

III. Théorèmes spectraux [Rombaldi Ch 22, p 697, Donato]

On se place sur $\mathbb{K} = \mathbb{R}$ (resp. $\mathbb{C}$) et on considère E euclidien (resp. hermitien) de dimension finie. On note $M^* = \overline{M}^T$ la transconjuguée de M. On note f^* l'adjoint de $f \in \mathcal{L}(E)$.

Définition 36

On dit que f est une **isométrie** (resp. un endomorphisme unitaire) si f préserve la norme, c'est-à-dire $\forall x \in E$, $\|f(x)\| = \|x\|$.

Définition 37

On dit que f est **auto-adjoint** si $f^* = f$. On dit que f est **normal** si $f^* f = f f^*$.

Exemple 38

On a les mêmes définitions pour les matrices. Une matrice symétrique ou orthogonale (resp. hermitienne ou unitaire) est normale.

Lemme 39

Si F est f-stable et f est normal alors $F^\perp$ est f-stable et f^*-stable.

Application 40

Les sous-espaces propres de f normal ont un orthogonal f-stable

Théorème 41 – Théorème des endomorphismes normaux, cas complexe

Si E est hermitien, tout endomorphisme normal est diagonalisable dans une base orthonormée.

Lemme 42

Toute matrice symétrique réelle admet une valeur propre réelle. De plus les sous-espaces propres associés sont deux à deux orthogonaux.

Théorème 43 – Réduction des endomorphismes auto-adjoints

Tout endomorphisme auto-adjoint admet une base orthonormale de diagonalisation

Application 44

Recherche d'extrama avec la matrice Hessienne

Annexe

Soit F un sous-espace vectoriel de dimension $1 \leq p \leq n-1$

Type de f	π_f	χ_f
Nilpotent d'indice k	X^k	X^n
Homothétie de rapport λ	$X-\lambda$	$(X-\lambda)^n$
Projecteur sur F	X^2-X	$(X-1)^p X^{n-p}$
Symétrie par rapport à F	X^2-1	$(X-1)^p(X+1)^{n-p}$

Classification des portraits de phase en fonction des valeurs propres :

Références :

— Mansuy Algèbre linéaire

— Gourdon Algèbre

— Objectif Agreg

— Berhuy Le grand combat

— Berthelin Equa diff

— Paul Donato Calcul Diff pour la license

— Rombaldi

Table des matières

I Généralités **1**

I.A Eléments propres [Mansuy algèbre linéaire chap I/IV] . . . 1

I.B Polynômes d'endomorphismes [[Algèbre linéaire Mansuy, Ch I/IV]] . . . 1

I.C. Polynôme caractéristique . . . 1

I.D. Liens entre polynômes et valeurs propres . . . 1

II. Diagonalisabilité **1**

II.A. Critères de diagonalisabilité . . . 1

II.B. Co-diagonalisabilité . . . 2

II.C. Propriétés topologiques sur $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ . . . 2

II.D. Décomposition de Dunford . . . 2

II.E. Application aux portraits de phase . . . 2

III. Théorèmes spectraux **2**

Leçon n° 153 : Valeurs propres, vecteurs propres. Calculs exacts ou approchés d'éléments propres. Application

Piroutet Alban

28 juillet 2026

Soit $\mathbb{K}$ un corps, $A \in \mathcal{M}_n(\mathbb{K})$ et $n \geq 1$.

I Elements propres d'une matrice

I.A) Définitions et calculs exacts [Gourdon, X-ens algèbre 2]

Définition 1
Valeur propre, vecteur propre et spectre

Définition 2
Sous-espaces propres

Théorème 3
Somme directe des sous-espaces propres

Définition 4
Polynôme caractéristique

Proposition 5
Valeur propre $\iff$ racine du polynôme caractéristique

Exemple 6
Cas n=2 : expression du polynôme caractéristique donc expression des valeurs propres

Remarque 7
Calculer les valeurs propres demande de trouver les racines d'un polynôme, ce qui est difficile en pratique.

I.B) Cas particuliers de calculs d'éléments propres [Gourdon]

Proposition 8
Déterminant circulant

Application 9
Suite de polygones

Proposition 10
Matrice compagnons et polynôme caractéristique

Proposition 11
Matrices nilpotentes

Proposition 12
Les valeurs propres des matrices symétriques réelles sont réelles.

Proposition 13
Cas des matrices stochastiques

I.C Application à la réduction [Gourdon, Rombaldi]

Théorème 14
Théorème spectral + réduction des endomorphismes normaux

Proposition 15
A est diagonalisable $\iff$ les sous-espaces propres sont en somme directe et engendrent l'espace.

Application 16
Calcul d'une puissance de matrice (diagonalisabilité ou via polynôme annulateur)

Application 17
Etude de la convergence des suites définies par $U_{n+1} = AU_n$ car $U_n = A^n U_0$ et si $(A^n)_{n\in\mathbb{N}}$ converge alors $(U_n)_n$ converge aussi

Application 18
Calul de l'exponentielle de matrice

II. Recherche approchée d'éléments propres

II.A. Normes matricielles et conditionnement [Allaire, Analyse Numérique]

Définition 19
Norme matricielle

Définition 20
Rayon spectral

Proposition 21
$\rho(A) \leq \|A\|$ et on a $\rho(A) = \inf_{norme}(\|A\|)$

Proposition 22
$A^n \to 0 \iff \rho(A) < 1$

Définition 23
Conditionnement

Remarque 24
Permet d'avoir une mesure de l'erreur lors de méthode itérative

Proposition 25
Inégalité avec conditionnement

II.B. Localisation de valeurs propres [Mansuy Réduction des endomorphismes]

Théorème 26
Disques de Gershgörin

Application 27
Application avec le déterminant d'une matrice

Proposition 28
Si un disque est isolé, alors il y a une unique valeur propre dans ce disque.

Remarque 29
En utilisant les disques de Gershgörien sur une matrice compagnon on peut donc localiser les racines d'un polynôme

II.C. Méthodes itératives [Allaire + Ciarlet]

Proposition 30
Méthode de la puissance

Proposition 31
Méthode de la puissance inverse

Proposition 32
Méthode QR

Références :

— Gourdon,

— Rombaldi,

— Francinou Algèbre 2,

— Allaire analyse numérique,

— Ciarlet Introduction à l'analyse numérique matricielle,

— Mansuy Réduction des endomorphismes

Table des matières

I Elements propres d'une matrice **1**
I.A Définitions et calculs exacts [Gourdon, X-ens algèbre 2] . . . 1
I.B Cas particuliers de calculs d'éléments propres [Gourdon] . . . 1
I.C Application à la réduction . . . 1

II.Recherche approchée d'éléments propres **1**
II.A. Normes matricielles et conditionnement . . . 1
II.B. Localisation de valeurs propres . . . 2
II.C. Méthodes itératives [Allaire analyse numérique, Ciarlet introduction à l'analyse numétrique matricielle] . . . 2

Leçon n° 155 : Exponentielle de matrices. Applications

Piroutet Alban

28 juillet 2026

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On munit $\mathcal{M}_n(\mathbb{K})$ d'une norme d'algèbre.

I Convergence et propriétés algébriques de l'exponentielle de matrices [Rombaldi, Ch 23]

Théorème 1

Soit $\sum a_k z^k$ une série entière à coefficients réels ou complexes de rayon de convergence $R > 0$. Si $A \in \mathcal{M}_n(\mathbb{K})$ est telle que $\rho(A) < R$, alors la série de terme général $a_k A^k$ est normalement convergente, et si $\rho(A) > R$, elle est divergente.

Définition 2

On définit $\exp(A) = e^A = \sum_{k=0}^{+\infty} \frac{A^n}{n!}$ c'est une série absolument convergente donc convergente.

Exemple 3

$e^0 = I_n, e^{I_n} = eI_n$

Proposition 4

Soient $A, B \in \mathcal{M}_n(\mathbb{C})$ telles que $AB = BA$, alors $e^{A+B} = e^A e^B = e^B e^A$.

Exemple 5

La réciproque est fausse par exemple en considérant :

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 2i\pi \end{pmatrix}$$

alors $BA = 0_{\mathcal{M}_2(R)} \neq AB$ bien que $e^A e^B = e^B e^A$.

Proposition 6

On en déduit que $\forall A \in \mathcal{M}_n(\mathbb{C}), e^A \in \mathcal{GL}_n(\mathbb{C})$ et $(e^A)^{-1} = e^{-A}$.

Proposition 7

Soient $A \in \mathcal{M}_n(\mathbb{C}), P \in \mathcal{GL}_n(\mathbb{C})$ alors $\exp(P^{-1}AP) = P^{-1}\exp(A)P$.

Proposition 8

Soit $A \in \mathcal{M}_n(\mathbb{C}), (\exp(A))^T = \exp(A^T)$. De même, on a $\overline{\exp(A)} = \exp(\overline{A})$

Corollaire 9

Si $A \in \mathcal{S}_n(\mathbb{R})$ alors $e^A \in \mathcal{S}_n^{++}(\mathbb{R})$

Proposition 10

Soit $A \in \mathcal{M}_n(\mathbb{C}), \det(\exp(A)) = e^{Tr(A)}$

Application 11

L'espace tangent à $SL_n(\mathbb{R})$ est $\ker(Tr)$

Proposition 12

$\exp(A) \in \mathbb{K}[A]$ et commute avec A.

II.Calcul pratique de l'exponentielle

Proposition 13

Soit $A \in \mathcal{GL}_n(\mathbb{C})$ nilpotente alors $e^A = \sum_{k=0}^{n-1} \frac{A^k}{k!}$.
Si $A = diag(\lambda_1, \dots, \lambda_n) \in \mathcal{M}_n(\mathbb{C})$ alors $e^A = diag(e^{\lambda_1}, \dots, e^{\lambda_n})$

Exemple 14

Soit $a \in \mathbb{C}$ et $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, alors :

$$e^A = \begin{pmatrix} e & ae \\ 0 & e \end{pmatrix}$$

Théorème 15 – Décomposition de Dunford

Soit $f \in \mathcal{L}(E)$ de polynôme caractéristique scindé. Alors il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que d est diagonalisable, n est nilpotent, $f = d + n$ et d commute avec n. De plus, d et n sont des polynômes en f.

Application 16

Soit $M \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique scindé. On note $\lambda_1, \dots, \lambda_r$ de multiplicités $\alpha_1, \dots, \alpha_r$, ou encore $\mu_1, \dots, \mu_n$ les racines de χ_M. Soit (D, N) la décomposition de Dunford de M. Soit $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $P^{-1}DP = \Delta = \mathrm{diag}(\mu_1, \dots, \mu_n)$ soit diagonale.
Soit p_i le projecteur sur $\ker(f - \lambda_i \mathrm{Id})^{\alpha_i}$ parallèlement à $\bigoplus_{j \neq i} \ker(f - \lambda_j \mathrm{Id})^{\alpha_j}$.
Alors on a :

$$\exp(M) = P\ \mathrm{diag}(e^{\mu_1}, \dots, e^{\mu_n})\, P^{-1} \sum_{k=0}^{n-1} \frac{N^k}{k!} = \sum_{i=1}^{r} e^{\lambda_i} \left(\sum_{p=0}^{\alpha_i - 1} \frac{(A - \lambda_i \mathrm{Id})^p}{p!} \right) P_i.$$

Proposition 17

Si χ_A est scindé, on a l'équivalence : A est diagonalisable $\iff$ e^A est diagonalisable.
De plus, si χ_A est scindé, la décomposition de Dunford de e^A est $(e^D, e^D(e^N - I_n))$.

III.Propriétés analytiques de l'exponentielle

III.A. Différentiabilité

Théorème 18

L'application exp est de classe $\mathcal{C}^\infty$, de plus :

$$\forall A \in \mathcal{M}_n(\mathbb{C}), \forall H \in \mathcal{M}_n(\mathbb{C}), d\exp(A).H = \sum_{k=1}^{+\infty} \frac{1}{k!} \left(\sum_{0 \leq i,j \leq k-1, i+j=k-1} A^i H A^j \right)$$

Théorème 19

exp est un $\mathcal{C}^1$-difféomorphisme local de 0 sur I_n

III.B. Injectivité et surjectivité

Définition 20

Soit $A \in \mathcal{M}_n(\mathbb{C})$ telle que $\rho(A) < 1$, on pose $\ln(I_n + A) = \sum_{k=1}^{+\infty} \frac{(-1)^{k+1}}{k} A^k \in \mathbb{K}[A]$

Proposition 21

Pour $A \in \mathcal{M}_n(\mathbb{C})$ telle que $\rho(A) < 1$, on a $e^{\ln(I_n+A)} = I_n + A$.

Lemme 22

Pour toute matrice $A \in \mathcal{M}_n(\mathbb{C})$, on a $e^A \in \mathrm{GL}_n(\mathbb{C})$ et $\ln(e^{tA}) = tA$ pour tout réel t.

Théorème 23

L'exponentielle matricielle réalise une bijection de $\mathcal{N}_n(\mathbb{C})$ sur $\mathcal{L}_n(\mathbb{C})$ d'inverse le logarithme matriciel où $\mathcal{N}_n$ désigne l'ensemble des matrices nilpotentes et $\mathcal{L}_n$ l'ensemble des matrices idempotentes.

Lemme 24

Soit $A \in \mathrm{GL}_n(\mathbb{C})$ une matrice diagonalisable. Il existe un polynôme $Q \in \mathbb{C}_{n-1}[X]$ tel que $Q(A)$ soit diagonalisable et $e^{Q(A)} = A$.

Théorème 25

Pour toute matrice $A \in \mathrm{GL}_n(\mathbb{C})$, il existe un polynôme $Q \in \mathbb{C}[X]$ tel que $e^{Q(A)} = A$ (l'exponentielle matricielle réalise une surjection de $\mathcal{M}_n(\mathbb{C})$ sur $\mathrm{GL}_n(\mathbb{C})$).

Théorème 26

L'ensemble $\mathcal{GL}_n(\mathbb{C})$ est connexe par arcs.

Proposition 27

L'application exp est non injective, de noyau les matrices diagonalisables de spectre inclus dans $2i\pi\mathbb{Z}$

Proposition 28

Sur $\mathbb{R}$, exp n'est pas surjective : $\exp(\mathcal{M}_n(\mathbb{R})) = \{M^2, M \in \mathcal{GL}_n(\mathbb{R})\}$

Théorème 29

On a : $\exp : \mathcal{S}_n(\mathbb{R}) \longrightarrow \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme.

Proposition 30

On a : $\mathcal{H}_n(\mathbb{C}) \longrightarrow \mathcal{H}_n^{++}(\mathbb{C})$ est un homéomorphisme.

Corollaire 31

L'application

$$\begin{array}{ccc} \mathcal{S}_n^{++}(\mathbb{R}) & \mapsto & \mathcal{S}_n^{++}(\mathbb{R}) \\ S & \mapsto & \sqrt{S} \end{array}$$

est un homéomorphisme

Application 32 – Décomposition polaire

Les applications :

$$\varphi : (O, S) \in \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) \mapsto OS \in GL_n(\mathbb{R})$$

et

$$\psi : M \in GL_n(\mathbb{R}) \mapsto (M(M^TM)^{-1/2}, (M^TM)^{1/2}) \in \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R})$$

sont des homéomorphismes inverses l'un de l'autre.

IV. Application aux équations différentielles linéaires

IV. A. Théorie des équations différentielles ordinaires

Proposition 33

La fonction $t \mapsto e^{tA}$ est $\mathcal{C}^\infty$ sur $\mathbb{R}$ et sa dérivée est $t \mapsto A\,e^{tA} = e^{tA}A$.

Remarque 34

L'étude de l'équation différentielle :

$$y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1(t)y' + a_0(t)y = b(t)$$

peut se ramener à l'étude d'une équation différentielle d'ordre 1, en posant,

$$Y = \begin{pmatrix} y \\ y' \\ \vdots \\ y^{(n-1)} \end{pmatrix} \quad , \quad B(t) = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ b(t) \end{pmatrix}$$

et

$$A(t) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \\ -a_0(t) & -a_1(t) & \dots & -a_{n-2}(t) & -a_{n-1}(t) \end{pmatrix}$$

Alors, l'équation différentielle s'écrit $Y' = A(t)Y + B(t)$.

Exemple 35

l'équation $y'' - 2y' + y = 0$ se réécrit :

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

Théorème 36 – Formule de Duhamel

L'unique solution de problème de Cauchy :

$$\begin{cases} y' = Ay + B(t) \\ y(t_0) = y_0 \end{cases}$$

est la fonction :

$$y(t) = e^{(t-t_0)A}y_0 + \int_{t_0}^{t} e^{(t-s)A}B(s)\mathrm{d}s$$

Exemple 37

Les solutions de :

$$\begin{cases} x' = 2x + y \\ y' = 2y \end{cases}$$

sont $x(t) = \alpha e^{2t} + \beta t e^{2t}$, $y(t) = \beta e^{2t}$ avec α, β des constantes quelconques.

Théorème 38 – Equation de Sylvester

Soient A, B et $C \in \mathcal{M}_n(\mathbb{C})$, si les valeurs propres de A et de B ont toutes une partie réelle strictement négative l'équation matricielle $AX + XB = C$ admet une unique solution.

IV. B. Stabilité des solutions

Définition 39

On considère l'équation différentielle :

$$y' = f(t, y)$$

pour $t \in I, y \in \Omega$, où f est continue et localement lipschitzienne par rapport à y. On considère son unique solution (par le théorème de Cauchy-Lipschitz), noté y_{t_0,y_0} telle que $y(t_0) = y_0$.
On dit que y_{t_0,y_0} est stable si :

- $\exists \alpha > 0, \forall y_1 \in \Omega$ tel que $\|y_1 - y_0\| \leq \alpha$, y_{t_0,y_1} est définie
- $\forall \varepsilon > 0, \exists \eta \in]0, \alpha]$ tel que si $\|y_1 - y_0\| \leq \eta$, alors $\|y_{t_0,y_1} - y_{t_0,y_0}\| \leq \varepsilon$

On dit que y_{t_0,y_0} est asymptotiquement stable si elle est stable et : $\exists \delta > 0$ tel que $y_{t_0,y_0}(t) - y_{t_0,y_1}(t) \to_{t\to+\infty} 0$ pour tout $y_1 \in \Omega$ tel que $\|y_1 - y_0\| \leq \delta$.

Théorème 40 – stabilité pour un système linéaire

Soit $A \in \mathcal{M}_n(\mathbb{C})$ et notons ses valeurs propres λ_j. Les solutions de $y' = Ay$ sont :

- stable si et seulement si, pour tout j $\Re(\lambda_j) < 0$ ou ($\Re(\lambda_j) = 0$ et le bloc de Jordan de A correspondant est diagonalisable).
- asymptotiquement stables si et seulement si $\Re(\lambda_j) < 0$ pour tout j.

Théorème 41 – Stabilité par linéarisation

Soit $f : \mathbb{R}^N \mapsto \mathbb{R}^N$ de classe C^1 telle que $f(0) = 0$. On pose $A = df(0) \in \mathcal{M}_n(\mathbb{R})$. On suppose que toutes les valeurs propres de A sont strictement négatives. Alors, il existe $\alpha > 0$ tel que, pour tout $y_0 \in \mathbb{R}^N$ vérifiant $\|y_0\| \leq \alpha$, la solution partant de y_0 en $t = 0$ de $y' = f(y)$ existe pour tout $t \geq 0$ et soit asymptotiquement stable.

Exemple 42

Les solutions du système d'équations différentielles réelles, partant de $t = 0$:

$$\begin{cases} x' = x(y^2 - 1) \\ y' = y(x^2 - 1) \end{cases}$$

sont asymptotiquement stables.

Références :

- Berthelin Equa diff,
- Rombaldi,
- Gourdon Algèbre et analyse
- Nouvelle histoire hedeniste tome 1,
- Francinou algèbre 2

Table des matières

I Convergence et propriétés algébriques de l'exponentielle de matrices [Rombaldi, Ch 23] **1**

II.Calcul pratique de l'exponentielle [Rombaldi, Gourdon] **1**

III.Propriétés analytiques de l'exponentielle **1**
III.A. Différentiabilité [Rombaldi, Gourdon] . . . 1
III.B. Injectivité et surjectivité [Rombaldi, Nouvelles histoires Tome 1] . . . 2

IV. Application aux équations différentielles linéaires [Berthelin, Equations différentielles] **2**
IV.A. Théorie des équations différentielles ordinaires . . . 2
IV.B. Stabilité des solutions . . . 3

Leçon n° 156 : Endomorphismes trigonalisables. Endomorphismes nilpotents.

Piroutet Alban

28 juillet 2026

Soit $\mathbb{K}$ un corps commutatif, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$.

I Généralités

I.A) Rappels sur l'étude d'endomorphismes [Mansuy]

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

Définition 1 – Polynôme minimal

$\varphi_f : \mathbb{K}[X] \longrightarrow \mathbb{K}[f],\ P \mapsto P(f)$ est un morphisme d'algèbres. Son noyau est un idéal de $\mathbb{K}[f]$ engendré par un unique polynôme unitaire π_f, appelé **polynôme minimal** de f.

Proposition 2

On a $\dim(\mathbb{K}[f]) = \deg(\pi_f)$

Exemple 3

Polynômes minimaux usuels (cf annexe)

Proposition 4

Soient $f, g \in \mathcal{L}(E)$ tels que f et g commutent. Alors $\ker(f)$ et $\mathrm{Im}(f)$ sont stables par g. En particulier, $\ker(P(f))$ et $\mathrm{Im}(P(f))$ sont stables par f pour tout $P \in \mathbb{K}[X]$.

Lemme 5 – Lemme des noyaux

Soit $(P_i)_{1\leq i\leq r}$ une famille de polynômes deux à deux premiers entre eux et $f \in \mathcal{L}(E)$. Alors, en posant $P = \prod_{i=1}^{r} P_i$, on a

$$\ker(P(f)) = \bigoplus_{i=1}^{r} \ker(P_i(f)).$$

De plus, le projecteur de $\ker(P(f))$ sur l'un de ces sous-espaces, parallèlement à la somme des autres, est un polynôme en f.

Application 6

Soit P un polynôme annulateur de f. Si $P = \prod_{i=1}^{r} P_i^{\alpha_i}$ où les $(P_i)_{1\leq i\leq r}$ sont deux à deux premiers entre eux, alors on a la décomposition en sous-espaces f-stables :

$$E = \bigoplus_{i=1}^{r} \ker\left(P_i^{\alpha_i}(f)\right).$$

Définition 7

On définit le polynôme caractéristique de $M \in \mathcal{M}_n(\mathbb{K})$ par $\chi_M(X) = \det(XI_n - M)$.
Deux matrices semblables ayant le même polynôme caractéristique, on peut définir le polynôme caractéristique de f.

Exemple 8

Polynôme caractéristique usuel

Proposition 9

$\lambda \in \mathbb{K}$ est une valeur propre de f si et seulement si $\chi_f(\lambda) = 0$, si et seulement si $\pi_f(\lambda) = 0$.

Théorème 10 – Théorème de Cayley-Hamilton

χ_f est un polynôme annulateur de f. Autrement dit, $\pi_f \mid \chi_f$.

I.B.Noyaux itérés

Proposition 11

La suite $(\ker(f^k))_{k\in\mathbb{N}}$ est croissante et stationnaire, et on a :

$$\forall k \in \mathbb{N},\quad \dim(\ker(f^{k+1})) = \dim(\ker(f^k)) + \dim\left(\ker(f) \cap \mathrm{Im}(f^k)\right).$$

Corollaire 12

La suite $\left(\dim(\ker(f^{k+1})) - \dim(\ker(f^k))\right)_{k\in\mathbb{N}}$ est décroissante.

Définition 13

$p = \min\{q \in \mathbb{N} \mid \forall k \in \mathbb{N},\ \ker(f^{q+k}) = \ker(f^q)\}$ est appelé **indice** de f.

Proposition 14

$p \leq n$ et on a

$$E = \ker(f^p) \oplus \mathrm{Im}(f^p).$$

II.Endomorphismes nilpotents

Définition 15

$f \in \mathcal{L}(E)$ est **nilpotent** si $f^p = 0$, où p est l'indice (de nilpotence) de f.

Soit f nilpotent d'indice r.

Application 16

On a alors $\pi_f = X^p$ et $\chi_f = X^n$.

Proposition 17

On a $p \leq n$, avec égalité si, et seulement si $\dim(\ker(f)) = 1$.

Application 18

Si f est nilpotent d'indice n, il existe une base B de E telle que :

$$M_B(f) = J_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & \\ 1 & 0 & \cdots & 0 & \\ 0 & 1 & \cdots & 0 & \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

En particulier, f est trigonalisable

Proposition 19

Si f est nilpotente, f est trigonalisable, avec une diagonale de 0.

Proposition 20

Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $g \in \mathcal{L}(E)$ est nilpotent si et seulement si $\forall k \in \mathbb{N}^*, tr(g^k) = 0$.

Exemple 21

Si $\mathbb{K} = \mathbb{F}_p$, le résultat est faux, prenant $g = Id_{(\mathbb{F}_p)^p}$

III. Trigonalisation [Mansuy, Ch IX]

III.A. Caractérisation

Définition 22

$f \in \mathcal{L}(E)$ est trigonalisable s'il existe une base de E dans laquelle la matrice de f soit triangulaire

Proposition 23

Si f est trigonalisable, les coefficients diagonaux de sa matrice dans une base adaptée sont les valeurs propres de f. Notons $(\lambda_i)_{1\leq i\leq r}$ ses valeurs propres, chacune de multiplicité algébrique $\mathrm{ma}(\lambda_i)$. On a alors :

$$\mathrm{Tr}(f) = \sum_{i=1}^{r} \mathrm{ma}(\lambda_i)\lambda_i \quad \text{et} \quad \det(f) = \prod_{i=1}^{r} \lambda_i^{\mathrm{ma}(\lambda_i)}.$$

Théorème 24

f est trigonalisable si et seulement si χ_f est scindé, si et seulement si π_f est scindé, si et seulement si f admet un polynôme annulateur scindé.

Corollaire 25

Si $\mathbb{K} = \mathbb{C}$ ou est algébriquement clos, tout endomorphisme de $\mathcal{L}(E)$ est trigonalisable.

Exemple 26

La matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est trigonalisable sur $\mathbb{C}$ mais pas sur $\mathbb{R}$.

Application 27

Pour $A \in \mathcal{M}_n(\mathbb{C})$, on a $\det(\exp(A)) = \exp(\mathrm{Tr}(A))$.

Corollaire 28

Si f est trigonalisable et si F est un sous-espace f-stable de E, alors f_F est trigonalisable.

III.B. Co-trigonalisation [Mansuy, Rombaldi]

Lemme 29

Soient $f, g \in \mathcal{L}(E)$ tels que f et g commutent. Alors les sous-espaces propres de f sont g-stables.

Proposition 30

Soit $(f_k)_{1\leq k\leq N}$ une famille d'endomorphismes trigonalisables commutant deux à deux. Alors il existe une base commune de trigonalisation (on dit que les $(f_k)_{1\leq k\leq N}$ sont **co-trigonalisables**).

Exemple 31

Soient $(f_k)_{1\leq k\leq n}$ des endomorphismes nilpotents qui commutent deux à deux. Alors $f_1 \cdots f_n = 0$.

Proposition 32

Soit $\mathbb{K} = \mathbb{C}$. Soient $f, g \in \mathcal{L}(E)$ trigonalisables tels que $fg = 0$. Alors f et g sont co-trigonalisables.

Proposition 33

Soit $\mathbb{K} = \mathbb{C}$. Soient $f, g \in \mathcal{L}(E)$ trigonalisables tels que $fg - gf = \alpha f + \beta g$ pour un couple $(\alpha, \beta) \in \mathbb{K}^2$. Alors f et g sont co-trigonalisables.

IV. Utilisations d'endomorphismes nilpotents/trigonalisables

IV.A. Décomposition de Dunford [Mansuy, Gourdon]

Théorème 34

Soit $f \in \mathcal{L}(E)$ de polynôme caractéristique scindé. Alors il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que d est diagonalisable, n est nilpotent, $f = d + n$ et d commute avec n. De plus, d et n sont des polynômes en f.

Application 35

Soit $M \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique scindé. On note $\mu_1, \ldots, \mu_n$ les n racines de χ_M (comptées sans leur multiplicité). Soit (D, N) la décomposition de Dunford de M. Soit $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $P^{-1}DP = \Delta = \mathrm{diag}(\mu_1, \ldots, \mu_n)$ soit diagonale.
Alors on a :

$$\exp(M) = P\ \mathrm{diag}(e^{\mu_1}, \ldots, e^{\mu_n})\, P^{-1} \sum_{k=0}^{n-1} \frac{N^k}{k!}.$$

Exemple 36

Un endomorphisme nilpotent et diagonalisable est nul.

Application 37

Résolution de l'équation $Y' = AY$ avec $A \in \mathcal{M}_n(\mathbb{C})$

IV.B. Réduction de Jordan [Mansuy Algèbre linéaire Ch X, Rombaldi Ch 21]

Lemme 38

Soit f nilpotent d'indice r. Soit $x \notin \ker(f^{r-1})$. Posons $F_x = \mathrm{Vect}\,(x, f(x), \ldots, f^{r-1}(x))$.
- F_x est f-stable et $B_x = (x, f(x), \ldots, f^{r-1}(x))$ en est une base, - F_x admet un supplémentaire f-stable.

Proposition 39

Soit $f \in \mathcal{L}(E)$ nilpotent. Il existe des entiers $d_1 \geq \cdots \geq d_\ell$ tels que, dans une certaine base B de E, $Mat_B(f)$ soit diagonale par blocs avec les blocs $(J_{r_k})_{1\leq k\leq \ell}$.

Théorème 40

Soit $f \in \mathcal{L}(E)$ de polynôme caractéristique scindé. Notons $\lambda_1, \ldots, \lambda_r$ ses valeurs propres.
Il existe des entiers $d_{j,1} \geq \cdots \geq d_{j,\ell_j}$ pour $j \in \{1, \ldots, r\}$ tels que, dans une certaine base B de E, $Mat_B(f)$ soit diagonale par blocs avec les blocs $(B_{j,k})_{1\leq j\leq r, 1\leq k\leq \ell_j}$, où $B_{j,k} = \lambda_j \mathrm{Id}_{d_{j,k}} + J_{d_{j,k}}$ avec $J_d = C(X^d) \in \mathcal{M}_d(\mathbb{K})$.

Théorème 41

Deux endomorphismes trigonalisables sont semblables si et seulement si ils ont même réduction de JORDAN.

IV.C. Autre application [Gourdon, Analyse]

Théorème 42 – Equation de Sylvester

Soient $A, B \in M_n(\mathbb{R})$ telles que

$$\mathrm{Sp}_{\mathbb{C}}(A) \cup \mathrm{Sp}_{\mathbb{C}}(B) = \{\lambda \in \mathbb{C} : \Re(\lambda) < 0\}.$$

Alors, pour tout $C \in M_n(\mathbb{R})$, l'équation

$$AX + XB = C$$

admet une unique solution dans $M_n(\mathbb{R})$.

Annexe

Type de f	π_f	χ_f
Nilpotent d'indice k	X^k	X^n
Homothétie de rapport λ	$X - \lambda$	$(X-\lambda)^n$
Projecteur sur F	$X^2 - X$	$(X-1)^p X^{n-p}$
Symétrie par rapport à F	$X^2 - 1$	$(X-1)^p (X+1)^{n-p}$

Références :

— Gourdon Algèbre et Analyse ,

— Rombaldi,

— Mansuy,

— Objectif Agreg

Table des matières

I Généralités **1**

I.A Rappels sur l'étude d'endomorphismes [Mansuy] . . . 1

I.B.Noyaux itérés [Mansuy] . . . 1

II.Endomorphismes nilpotents [Mansuy] **1**

III. Trigonalisation **2**

III.A. Caractérisation . . . 2

III.B. Co-trigonalisation . . . 2

IV. Utilisations d'endomorphismes nilpotents/trigonalisables **2**

IV.A. Décomposition de Dunford . . . 2

IV.B. Réduction de Jordan . . . 2

IV.C. Autre application . . . 3

Leçon n° 157 : Matrices symétriques réelles, matrices hermitiennes.

Piroutet Alban

28 juillet 2026

Soit $n \in \mathbb{N}^*$. Pour $M \in \mathcal{M}_n(\mathbb{K})$, on note $M^* = \overline{M}^T$.

I Généralités

I.A) Définitions et premières propriétés [Gourdon, Rombaldi]

Définition 1

Soit $M \in M_n(\mathbb{R})$. On dit que M est **symétrique** si $M = M^\top$ et **antisymétrique** si $M = -M^\top$. On note $S_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) \mid M = M^\top\}$ et $A_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) \mid M = -M^\top\}$.
Soit $M \in M_n(\mathbb{C})$. On dit que M est **hermitienne** si $M = \overline{M}^\top$. On note $H_n(\mathbb{C}) = \{M \in M_n(\mathbb{C}) \mid M = \overline{M}^\top\}$.

Exemple 2

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix} \in S_n(\mathbb{R}) \quad \text{et} \quad \begin{pmatrix} 1 & -i & 3+2i \\ i & 1 & 1+i \\ 3-2i & 1-i & 6 \end{pmatrix} \in H_n(\mathbb{C})$$

Remarque 3

$\mathcal{H}_n(\mathbb{C})$ est un $\mathbb{R}$-espace vectoriel mais pas un $\mathbb{C}$-espace vectoriel.

Proposition 4

$$\dim(S_n(\mathbb{R})) = \frac{n(n+1)}{2}, \quad \dim(A_n(\mathbb{R})) = \frac{n(n-1)}{2}, \quad \text{et} \quad \dim_{\mathbb{R}}(H_n(\mathbb{C})) = n^2.$$

Proposition 5

$$M_n(\mathbb{R}) = S_n(\mathbb{R}) \oplus A_n(\mathbb{R}) \quad \text{et} \quad H_n(\mathbb{C}) = S_n(\mathbb{R}) \oplus iA_n(\mathbb{R})$$

Proposition 6

Pour $A \in S_n(\mathbb{R})$ ou $H_n(\mathbb{C})$, on a $\mathrm{Sp}(A) \subset \mathbb{R}$.

Définition 7

On définit : - $S_n^+(\mathbb{R}) = \{S \in S_n(\mathbb{R}) \mid X^\top SX \geq 0 \text{ pour tout } X \in \mathbb{R}^n\}$, - $S_n^{++}(\mathbb{R}) = \{S \in S_n^+(\mathbb{R}) \mid X^\top SX = 0 \implies X = 0\}$, - $H_n^+(\mathbb{C}) = \{H \in H_n(\mathbb{C}) \mid X^*HX \geq 0 \text{ pour tout } X \in \mathbb{C}^n\}$, - $H_n^{++}(\mathbb{C}) = \{H \in H_n^+(\mathbb{C}) \mid X^*HX = 0 \implies X = 0\}$.

I.B) Liens avec les formes bilinéaires symétriques / hermitiennes [Gourdon]

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n, avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ selon le contexte.

Définition 8

Soit $\mathbb{K} = \mathbb{R}$. Soit $\varphi : E \times E \to \mathbb{R}$ une forme bilinéaire. - φ est dite **symétrique** si $\varphi(x,y) = \varphi(y,x)$ pour tout $x, y \in E$. - Si φ est symétrique, l'application $\Phi : E \to \mathbb{R}$, $x \mapsto \varphi(x,x)$ est appelée **forme quadratique associée** à φ. - φ est appelée **forme polaire** associée à Φ (elle est unique).

Définition 9

Soit $\mathbb{K} = \mathbb{C}$. Soit $\varphi : E \times E \to \mathbb{C}$ une forme sesquilinéaire (pour tout $x \in E$, $\varphi(x,\cdot)$ est linéaire et $\varphi(\cdot,x)$ est anti-linéaire). - φ est dite **hermitienne** si $\varphi(x,y) = \overline{\varphi(y,x)}$ pour tout $x, y \in E$. - Si φ est hermitienne, l'application $\Phi : E \to \mathbb{R}$, $x \mapsto \varphi(x,x)$ est appelée **forme hermitienne associée** à φ. - φ est appelée **forme polaire** associée à Φ (elle est unique).

Exemple 10

Dans $C([0,1],\mathbb{C})$, l'application $\varphi : (f,g) \mapsto \int_0^1 f\overline{g}$ est hermitienne, et induit sur $C([0,1],\mathbb{R})$ une forme bilinéaire symétrique.
Sur $\mathbb{K}^n$, $(X,Y) \mapsto X^\top Y$ est bilinéaire symétrique si $\mathbb{K} = \mathbb{R}$, ou sesquilinéaire hermitienne si $\mathbb{K} = \mathbb{C}$.

Proposition 11

Soit $B_E = (e_1, \ldots, e_n)$ une base de E et $\varphi : E \times E \to \mathbb{K}$ une forme bilinéaire ou sesquilinéaire.
- Si $\mathbb{K} = \mathbb{R}$, φ est symétrique si et seulement si $A = M_{B_E}(\varphi) = (\varphi(e_i,e_j))_{1 \leq i,j \leq n} \in S_n(\mathbb{R})$. - Si $\mathbb{K} = \mathbb{C}$, φ est hermitienne si et seulement si $A \in H_n(\mathbb{C})$.
Pour $x, y \in E$, on note X et Y leurs coordonnées dans B_E. Dans les deux cas, on a alors : $\forall x, y \in E, \quad \varphi(x,y) = X^\top AY$.

Proposition 12

Si B'_E est une autre base de E, et P est la matrice de passage de B_E vers B'_E, alors $M_{B'_E}(\varphi) = P^\top AP$.

II. Réduction et applications

II.A. Orthogonalité et théorème spectral [Gourdon, Rombaldi]

Soit Φ une forme quadratique (resp. hermitienne) de forme polaire φ.

Définition 13

Une base B de E est dite Φ-orthogonale si $\varphi(e,e') = 0$ pour $e \neq e' \in B$.

Proposition 14

Il existe une base Φ-orthogonale de E.

Théorème 15

Soit $M \in S_n(\mathbb{R})$ (resp. $M \in H_n(\mathbb{C})$). Alors il existe une matrice P orthogonale (resp. unitaire) telle que $P^{-1}MP = P^*MP$ est diagonale réelle.

Application 16

Soit $S \in S_n(\mathbb{R})$. Alors $S \in S_n^+(\mathbb{R})$ (resp. $S \in S_n^{++}(\mathbb{R})$) si et seulement si $\mathrm{Sp}(S) \subset \mathbb{R}^+$ (resp. $\mathrm{Sp}(S) \subset \mathbb{R}^{*+}$).

Proposition 17

Soit $A \in S_n^{++}(\mathbb{R})$ et $B \in S_n(\mathbb{R})$, alors il existe $P \in GL_n(\mathbb{R})$ telle que $P^\top AP$ et $P^\top BP$ soient diagonales.

II.B. Signature d'une forme quadratique/hermitienne et réduction de Gauss [Gourdon, Rombaldi]

Théorème 18 – Réduction de Gauss

Pour toute forme quadratique (resp. hermitienne) Φ sur E, il existe $r \in \mathbb{N}$, $(\lambda_i)_{1 \leq i \leq r} \in (\mathbb{R}^*)^r$ et $(\ell_i)_{1 \leq i \leq r} \in (E^*)^r$ indépendantes telles que $\Phi = \sum_{i=1}^r \lambda_i \ell_i^2$ (resp. $\Phi = \sum_{i=1}^r \lambda_i |\ell_i|^2$).

Exemple 19

$\Phi((x,y,z,t)) = xy+yz+zt+tx = \frac{1}{4}\left[(x+z+y+t)^2-(x+z-y-t)^2\right]$

Théorème 20

Il existe un unique couple (s,t) d'entiers naturels tel que pour toute base $B=(e_i)_{1\leq i\leq n}$ Φ-orthogonale, il y a exactement s vecteurs de B pour lesquels $\Phi>0$, t vecteurs de B pour lesquels $\Phi<0$, et $n-s-t$ vecteurs de B pour lesquels $\Phi=0$. On a $s+t=\mathrm{rg}(\Phi)$.

Définition 21

Le couple (s,t) est appelé signature de Φ.

Exemple 22

$\Phi((x,y,z,t)) = xy+yz+zt+tx$ a pour signature $(1,1)$ et pour rang 2.

Corollaire 23

Si $A\in S_n(\mathbb{R})$ (resp. $A\in H_n(\mathbb{C})$) est de rang r, il existe $s,t\in\mathbb{N}$ tels que $s+t=r$ et $P\in GL_n(\mathbb{R})$ (resp. $P\in GL_n(\mathbb{C})$) telle que $P^\top AP$ (resp. P^*AP) est diagonale par blocs avec pour blocs I_s, $-I_t$ et 0_{n-r}.

III. Propriétés topologiques en lien avec les matrices symétriques réelles [Gourdon, Rombaldi]

Proposition 24

$S_n^{++}(\mathbb{R}) = S_n^+(\mathbb{R}) \subset GL_n(\mathbb{R})$ est un ouvert de $M_n(\mathbb{R})$.

Lemme 25

Soit $A\in S_n^+(\mathbb{R})$. Alors il existe $S\in S_n^+(\mathbb{R})$ unique telle que $A=S^2$.

Théorème 26

L'application $O_n(\mathbb{R})\times S_n^{++}(\mathbb{R})\to GL_n(\mathbb{R})$, $(O,S)\mapsto OS$, est un homéomorphisme.

Application 27

$O_n(\mathbb{R})$ est le seul sous-groupe compact de $GL_n(\mathbb{R})$ contenant $O_n(\mathbb{R})$.

Application 28

Pour $A\in M_n(\mathbb{R})$, on a $\|A\|_2=\sqrt{\rho(A^\top A)}$.

Définition 29

Pour $A\in M_n(\mathbb{R})$, on pose $\exp(A)=\sum_{n\geq 0}\frac{A^n}{n!}$.

Exemple 30

On a $\exp(\mathrm{diag}(\lambda_1,\dots,\lambda_n)) = \mathrm{diag}(e^{\lambda_1},\dots,e^{\lambda_n})$.

Théorème 31

$\exp : S_n(\mathbb{R})\to S_n^{++}(\mathbb{R})$ est un homéomorphisme.

Corollaire 32

$GL_n(\mathbb{R})$ est homéomorphe à $O_n(\mathbb{R})\times\mathbb{R}^{n(n+1)/2}$.

IV. Applications

IV.A. Différentielle seconde d'une fonction de classe $\mathcal{C}^2$ [PGCD]

Théorème 33

Soit f une fonction de classe C^2 définie sur un ouvert U de $\mathbb{R}^n$. Alors $D^2f\in M_n(\mathbb{R})$ est une matrice symétrique.

Lemme 34

Soit $A_0\in S_n(\mathbb{R})\cap GL_n(\mathbb{R})$. Alors il existe $V\in\mathcal{V}(A_0)$ et $g\in C^1(V,GL_n(\mathbb{R}))$ telle que $\forall A\in V,\quad A=g(A)^\top A_0 g(A)$.

Théorème 35 – Lemme de Morse

Soit $f:U\to\mathbb{R}$ une fonction de classe C^3 définie sur un ouvert U de $\mathbb{R}^n$ contenant 0. On suppose que $df(0)=0$ et que $d^2f(0)$ est non dégénérée, de signature $(p,n-p)$.
Alors il existe un C^1-difféomorphisme φ entre deux voisinages de l'origine de $\mathbb{R}^n$ tel que $\varphi(0)=0$ et $f(x)-f(0)=\varphi_1(x)^2+\cdots+\varphi_p(x)^2-\varphi_{p+1}(x)^2-\cdots-\varphi_n(x)^2$ au voisinage de 0.

Application 36

Soit x_0 un point critique de f tel que la Hessienne de f est non dégénérée. Alors x_0 est un minimum (resp. maximum) local si et seulement si la Hessienne est de signature $(n,0)$ (resp. $(0,n)$). De plus, si la Hessienne est de signature $(p,n-p)$ pour $1\leq p\leq n-1$, alors il existe des directions v pour lesquelles x_0 sera minimum local de $h\mapsto f(x_0+hv)$ et d'autres pour lesquelles x_0 sera maximum local.

Exemple 37

Soit x_0 un point critique de f tel que $D^2f(x_0)=\begin{pmatrix} r & s\\ s & t\end{pmatrix}$. Alors :

- si $rt-s^2>0$ et $r+t>0$, x_0 est un minimum local,
- si $rt-s^2>0$ et $r+t<0$, x_0 est un maximum local,
- si $rt-s^2<0$, x_0 n'est pas un extremum,
- si $rt-s^2=0$, on ne peut pas conclure.

IV.B. Analyse matricielle numérique [Allaire, Bernis, Ciaerlet]

Théorème 38 – Factorisation LU

Soit $A\in GL_n(\mathbb{R})$ une matrice dont tous les mineurs principaux sont non nuls. Alors il existe un unique couple (L,U) de matrices tel que L est triangulaire inférieure avec diagonale de 1, U est triangulaire supérieure et $A=LU$.

Corollaire 39

Si de plus $A\in S_n(\mathbb{R})$, il existe L triangulaire inférieure à diagonale de 1 et D diagonale telle que $A=LDL^\top$.

Théorème 40 – Factorisation de Cholesky

Soit $A\in S_n^{++}(\mathbb{R})$. Alors il existe une unique matrice B triangulaire inférieure telle que tous ses éléments diagonaux soient positifs et $A=BB^\top$.

Application 41

Soient $n,p\in\mathbb{N}$, $A\in M_{n,p}(\mathbb{R})$ et $b\in\mathbb{R}^n$. On cherche un vecteur $x\in\mathbb{R}^p$ tel que $\|b-Ax\|_2=\inf_{y\in\mathbb{R}^p}\|b-Ay\|_2$.

1. Il existe toujours une solution au problème,
2. x est solution si et seulement si $A^\top Ax=A^\top b$.
3. Si $n\geq p$ et $\mathrm{rg}(A)=p$, $A^\top A$ est inversible et il existe une unique matrice réelle B triangulaire inférieure, à diagonale positive, telle que $A^\top A=BB^\top$, et alors $x=(BB^\top)^{-1}A^\top b$ est une solution.

Contexte : Soit $n \in \mathbb{N}^*$. Soit $A \in S_n^{++}(\mathbb{R})$ et $b \in \mathbb{R}^n$ non nul. On s'intéresse à la résolution approchée du système d'inconnue x,

$$Ax = b \tag{1}$$

La matrice A étant inversible (1) admet une unique solution noté $\overline{x}$.
On associe à A son produit scalaire associé : $< x, y >_A =< x, Ay >= {}^t xAy$, et noterons $||.||_A$ la norme associée.
Considérons l'application

$$\begin{cases} \Phi : \mathbb{R}^n \longrightarrow \mathbb{R}^n \\ \qquad x \longmapsto \dfrac{1}{2}||x||_A^2 - {}^t xb \end{cases}$$

Théorème 42 – Méthode du gradient à pas optimal

— L'application Φ atteint son minimum en $\overline{x}$ et seulement en ce point.
— Soit $a \in \mathbb{R}^n$ distinct de $\overline{x}$ et $(x_k)_k$ la suite de $\mathbb{R}^n$ définie par :

$x_0 = a$,

$\alpha_k = \frac{||\nabla\Phi(x_k)||^2}{||\nabla\Phi(x_k)||_A^2}$ si $x_k \neq \overline{x}$ et 0 sinon

et $x_{k+1} = x_k - \alpha_k \nabla\Phi(x_k)$ La suite $(x_k)_k$ converge vers $\overline{x}$. De plus $\forall k \geq 0$,

$$||x_{k+1} - \overline{x}|| \leq \sqrt{\frac{\lambda_{max}}{\lambda_{min}}} \left(\frac{\lambda_{max} - \lambda_{min}}{\lambda_{max} + \lambda_{min}}\right)^{k+1} ||x_0 - \overline{x}||$$

Définition 43 – Solution des moindres carrés

Soient $A \in \mathcal{M}_{n,p}(\mathbb{R})$ et $b \in \mathbb{R}^n$, on appelle solution des moindres carrés tout vecteur $x \in \mathbb{R}^p$ tel que $||b - Ax||_2 = \min_{y \in \mathbb{R}^p} ||b - Ay||$

Lemme 44

Il existe une solution au problème des moindres carrés si et seulement si, elle satisfait l'équation normale,

$$A^*Ax = A^*b$$

Théorème 45

Pour toute matrice $A \in \mathcal{M}_{n,p}(\mathbb{R})$, il existe toujours au moins une solution de l'équation normale $A^*Ax = A^*b$.
De plus cette solution est unique si et seulement si $\ker A = \{0\}$ et on a alors $x = A^\dagger b$ où $A^\dagger = (A^*A)^{-1}A$

Définition 46

Valeurs singulières d'une matrice

Théorème 47 – Décomposition en valeurs singulières

Définition 48 – Notion de pseudo-inverse

On généralise la notion d'inverse à une matrice non-inversible ou non carrée.

Références :

— Gourdon Algèbre et analyse,
— Rombaldi,
— PGCD,
— Histoire Hédoniste tome 1,
— Ciarlet Introduction à l'analyse numérique matricielle
— Allaire Algèbre linéaire numérique

Table des matières

I Généralités **1**
I.A Définitions et premières propriétés [Gourdon, Rombaldi] . . . 1
I.B Liens avec les formes bilinéaires symétriques / hermitiennes [Gourdon] . . . 1

II.Réduction et applications **1**
II.A. Orthogonalité et théorème spectral . . . 1
II.B. Signature d'une forme quadratique/hermitienne et réduction de Gauss . . . 1

III. Propriétés topologiques en lien avec les matrices symétriques réelles **2**

IV. Applications **2**
IV.A. Différentielle seconde d'une fonction de classe $\mathcal{C}^2$ . . . 2
IV.B. Analyse matricielle numérique . . . 2

Leçon n° 158 : Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).

Piroutet Alban

28 juillet 2026

Soit $(E, \langle\cdot,\cdot\rangle)$ un espace euclidien de dimension finie $n \in \mathbb{N}^*$. On note $\|\cdot\|$ la norme issue du produit scalaire. Soit $u \in L(E)$.

I Endomorphismes d'un espace euclidien

I.A) Adjoint d'un endomorphisme [Rombaldi]

Il existe un unique endomorphisme $u^* \in L(E)$ tel que : $\forall x, y \in E,\ \langle u(x), y\rangle = \langle x, u^*(y)\rangle$. u^* est appelé adjoint de u.

Proposition 1

Soit $B = (e_i)_{1\leq i\leq n}$ une base de E et $S = (\langle e_i, e_j\rangle)_{1\leq i,j\leq n}$ la matrice du produit scalaire dans la base B. Si $A = M_B(u)$, alors $M_B(u^*) = S^{-1}A^\top S$. En particulier, si B est orthonormée, $M_B(u^*) = A^\top$.

Proposition 2

Pour $v, w \in L(E)$ et $\lambda \in \mathbb{R}$, on a :

1. $(v^*)^* = v$,
2. $(v \circ w)^* = w^* \circ v^*$,
3. $\ker(v^*) = \mathrm{Im}(v)^\perp$ et $\mathrm{Im}(v^*) = \ker(v)^\perp$,
4. $\mathrm{rg}(v) = \mathrm{rg}(v^*)$,
5. si F est un sous-espace vectoriel stable par v, alors $F^\perp$ est stable par v^*,
6. $\|u^*\| = \|u\|$.

I.B) Exemples d'endomorphismes remarquables [Rombaldi]

Définition 3

u est un endomorphisme orthogonal (ou isométrie) de E si $u^* = u^{-1}$, autrement dit si u conserve le produit scalaire : $\forall x, y \in E,\ \langle u(x), u(y)\rangle = \langle x, y\rangle$. On note $O(E)$ l'ensemble des isométries de E.

Proposition 4

$v : E \to E$ est orthogonale si et seulement si v est linéaire et conserve la norme.

Exemple 5

- Id_E et $-\mathrm{Id}_E$ sont des endomorphismes orthogonaux. Ce sont les seuls en dimension 1,
- les rotations et les symétries orthogonales sont des isométries,
- les valeurs propres d'une isométrie ne peuvent être que ± 1.

Proposition 6

u est une isométrie de E si et seulement si u est inversible et $u^* = u^{-1}$. Dans une base B orthonormée de E, si $A = M_B(u)$, on a $A^\top = A^{-1}$.

Définition 7

- On dit que u est symétrique (ou auto-adjoint) si $u^* = u$, ou encore si $\forall x, y \in E,\ \langle u(x), y\rangle = \langle x, u(y)\rangle$. On note $S(E)$ l'ensemble des endomorphismes symétriques de E.
- On dit que u est anti-symétrique si $u^* = -u$. On note $A(E)$ l'ensemble des endomorphismes anti-symétriques de E.

Exemple 8

$\frac{u+u^*}{2} \in S(E)$. Un projecteur orthogonal est symétrique.

Définition 9

u est dit normal si $uu^* = u^*u$

Exemple 10

Un endomorphisme auto-adjoint, antisymétrique ou orthogonal est normal.

Proposition 11

Soit B une base orthonormée de E et $A = M_B(u)$. On a les caractérisations matricielles des endomorphismes remarquables vus précédemment :

u	définition	$M_B(u)$
symétrique	$u^* = u$	$A^\top = A$
anti-symétrique	$u^* = -u$	$A^\top = -A$
orthogonal	$u^* = u^{-1}$	$A^\top A = I$
normal	$u^*u = uu^*$	$A^\top A = AA^\top$

II. Endomorphismes normaux [Rombaldi, Gourdon]

Dans cette partie u désigne un endomorphisme normal.

Lemme 12

Si F est un sous-espace vectoriel stable par u, alors $F^\perp$ est stable par u.

Lemme 13

Il existe un sous-espace vectoriel stable par u de dimension 1 ou 2.

Proposition 14

Supposons $n = \dim(E) = 2$. Alors :

- soit u a une valeur propre réelle, et alors u est diagonalisable dans une base orthonormée,
- soit la matrice de u dans une base orthonormée est de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

Théorème 15 – Réduction des endomorphismes normaux

Il existe une base orthonormée B de E telle que

$$M_B(u) = \begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & & \\ & & \lambda_p & & & & \\ & & & R_1 & & & \\ & & & & \ddots & & \\ & & & & & R_r \end{pmatrix},$$

où $p + 2r = n$, $(\lambda_i)_{1 \leq i \leq p} \in \mathbb{R}^p$ et pour $1 \leq k \leq r$, $R_k = \begin{pmatrix} a_k & -b_k \\ b_k & a_k \end{pmatrix}$ avec $b_k \neq 0$.

Application 16

Supposons u antisymétrique. Alors il existe une base orthonormée B de E telle que

$$M_B(u) = \begin{pmatrix} 0 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & & & \\ & & & R_1 & & & \\ & & & & \ddots & & \\ & & & & & R_r \end{pmatrix},$$

où $2r \leq n$ et $R_k = \begin{pmatrix} 0 & -b_k \\ b_k & 0 \end{pmatrix}$.

III. Endomorphismes auto-adjoints

III.A. Premières propriétés [Rombaldi, Allaire]

Proposition 17

$S(E)$ est un sous-espace vectoriel de dimension $\frac{n(n+1)}{2}$.

Définition 18

u est dit symétrique positif (resp. défini positif) s'il est symétrique avec $hx|u(x)i \geq 0$ pour tout $x \in E$ (resp. $hx|u(x)i > 0$ pour $x \in E \setminus \{0\}$). On note $S^+(E)$ (resp. $S^{++}(E)$) l'ensemble des endomorphismes symétriques positifs (resp. définis positifs).

Proposition 19

On a $\mathrm{Sp}(u) \subset \mathbb{R}$ pour $u \in S(E)$, $\mathrm{Sp}(u) \subset \mathbb{R}_+$ pour $u \in S^+(E)$ et $\mathrm{Sp}(u) \subset \mathbb{R}_+^*$ pour $u \in S^{++}(E)$.

Lemme 20

Si $\lambda \neq \mu$, les sous-espaces propres associés $E_\lambda = \ker(u - \lambda \mathrm{id}_E)$ et $E_\mu = \ker(u - \mu \mathrm{id}_E)$ sont orthogonaux.

Proposition 21

Soit $A \in \mathcal{M}_{n,p}(\mathbb{R})$ avec $n \geq p$ telle que $\mathrm{rg}(A) = p$ (ou encore $\ker(A) = \{0\}$). Alors $A^\top A \in S_p^{++}(\mathbb{R})$.

Application 22

Soient $n, p \in \mathbb{N}$ et $A \in \mathcal{M}_{n,p}(\mathbb{R})$ et $b \in \mathbb{R}^n$. On cherche un vecteur $x \in \mathbb{R}^p$ tel que

$$\|b - Ax\|_2^2 = \inf_{y \in \mathbb{R}^p} \|b - Ay\|_2^2.$$

1. Existence d'une solution des moindres carrés + application à la décomposition en valeur singulière ! On a généralisé l'inverse pour une matrice qui n'est pas carré ou inversible !

III.B. Autour du théorème spectral [Rombaldi, H2G2]

Théorème 23 – Théorème spectral

Tout endomorphisme de $S(E)$ est diagonalisable dans une base orthonormée.

Corollaire 24

Soit $A \in S_n(\mathbb{R})$. Alors il existe $P \in O_n(\mathbb{R})$ telle que $P^\top AP$ soit diagonale.

Corollaire 25

Soit $u \in S(E)$. Alors $u \in S^+(E)$ si et seulement si $\mathrm{Sp}(u) \subset \mathbb{R}^+$, et $u \in S^{++}(E)$ si et seulement si $\mathrm{Sp}(u) \subset \mathbb{R}_+^*$.

Application 26

Pour $A \in S_n(\mathbb{R})$, on a $|||A|||_2 = \rho(A)$.

Application 27

Pour $A \in S_n^+(\mathbb{R})$, il existe une unique matrice $B \in S_n^+(\mathbb{R})$ telle que $A = B^2$.

Théorème 28

$\exp : S_n(\mathbb{R}) \longrightarrow S_n^{++}(\mathbb{R})$ est un homéomorphisme.

IV. Endomorphismes orthogonaux

IV.A. Propriétés et réductions [Rombaldi]

Proposition 29

Soit $u \in O(E)$,
- $\mathrm{Sp}(u) \subset U = \{z \in \mathbb{C} \mid |z| = 1\}$,
- $\det(u) = \pm 1$. En particulier, u est inversible.

Proposition 30

Soit $u \in L(E)$.

1. Si $u \in O(E)$, u transforme toute b.o.n. en une b.o.n.,
2. $u \in O(E)$ si et seulement si u transforme une b.o.n. en une b.o.n.

Théorème 31

Soit $u \in O(E)$. Il existe une base orthonormée B telle que

$$M_B(u) = \begin{pmatrix} I_{p_1} & & & & \\ & -I_{p_2} & & & \\ & & R_1 & & \\ & & & \ddots & \\ & & & & R_r \end{pmatrix},$$

où $p_1 + p_2 + 2r = n$ et pour $1 \leq k \leq r$,

$$R_k = \begin{pmatrix} \cos(\theta_k) & -\sin(\theta_k) \\ \sin(\theta_k) & \cos(\theta_k) \end{pmatrix} \quad \text{avec } \theta_k \notin \pi\mathbb{Z}.$$

IV.B. Structure de groupe de $\mathcal{O}_n(\mathbb{R})$

Proposition 32

$O_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$ et

$$O_n^+(\mathbb{R}) = \{A \in O_n(\mathbb{R}) \mid \det(A) = 1\}$$

est un sous-groupe distingué de $O_n(\mathbb{R})$.

Définition 33

Soit u une symétrie orthogonale. On note

$$E^+ = \ker(u - \mathrm{Id}_E) \quad \text{et} \quad E^- = \ker(u + \mathrm{Id}_E)$$

qui vérifient $E = E^+ \oplus E^-$.
- Si $\dim E^- = 1$, on dit que u est une réflexion. - Si $\dim E^- = 2$, on dit que u est un renversement.

Théorème 34

— $\mathrm{O}(R)$ est engendré par les réflexions orthogonales. Plus précisément, si $A \in \mathrm{O}(R)$, A est produit d'au plus n réflexions.
— Pour $n \geq 3$, $\mathrm{O}_n^+(R)$ est engendré par les réflexions orthogonales. Plus précisément, si $A \in \mathrm{O}_n^+(R)$, A est produit d'au plus n renversements.

IV.C. Etude en dimensions 2 et 3

Proposition 35

Soit $u \in O(\mathbb{R}^2)$ et A la matrice de u dans la base canonique de $\mathbb{R}^2$. On a deux cas :

— soit $u \in O^+(\mathbb{R}^2)$ et alors il existe $\theta \in [0, 2\pi[$ tel que $A = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$. u est alors la rotation d'angle θ centrée en l'origine,

— soit $u \notin O^+(\mathbb{R}^2)$ et alors il existe $\theta \in [0, 2\pi[$ tel que $A = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$. u est alors la symétrie par rapport à la droite d'angle polaire $\theta/2$.

Proposition 36

Soit $u \in O(\mathbb{R}^3)$. Il existe une base B de $\mathbb{R}^3$ telle que la matrice de u dans la base B soit :

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}$$

pour un $\theta \in [0, 2\pi[$ et où $\varepsilon = \pm 1$ vaut :
— 1 si $u \in O^+(\mathbb{R}^3)$ (alors u est une rotation d'angle θ autour d'une droite),
— -1 si $u \notin O^+(\mathbb{R}^3)$ (alors u est la composée d'une rotation d'angle θ autour d'une droite D puis d'une symétrie orthogonale par rapport à $D^\perp$).

IV.D. Topologie du groupe orthogonal [Rombaldi, H2G2]

Proposition 37

$O(E)$ est une partie compacte de $L(E)$.

Proposition 38

Les composantes connexes de $O(E)$ sont les fermés $O^+(E)$ et $O^-(E)$.

Théorème 39 – Décomposition polaire

L'application $O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$, $(O, S) \mapsto OS$, est un homéomorphisme.

Application 40

$O_n(\mathbb{R})$ est le seul sous-groupe compact de $GL_n(\mathbb{R})$ contenant $O_n(\mathbb{R})$.

Application 41

Pour $A \in M_n(\mathbb{R})$, $\quad |||A|||_2 = \sqrt{\rho(A^T A)}$.

Références :

— Allaire Analyse numérique,

— H2G2 Tome premier

— Gourdon Algèbre,

— Perrin

— Rombaldi

Table des matières

I Endomorphismes d'un espace euclidien **1**
I.A Adjoint d'un endomorphisme [Rombaldi] . . . 1
I.B Exemples d'endomorphismes remarquables [Rombaldi] . . . 1

II. Endomorphismes normaux **1**

III. Endomorphismes auto-adjoints **2**
III.A. Premières propriétés . . . 2
III.B. Autour du théorème spectral . . . 2

IV. Endomorphismes orthogonaux **2**
IV.A. Propriétés et réductions . . . 2
IV.B. Structure de groupe de $\mathcal{O}_n(\mathbb{R})$ . . . 3
IV.C. Etude en dimensions 2 et 3 . . . 3
IV.D. Topologie du groupe orthogonal . . . 3

Leçon n° 159 : FORMES LINÉAIRES ET DUALITÉ EN DIMENSION FINIE. EXEMPLES ET APPLICATIONS.

Piroutet Alban

28 juillet 2026

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n.

I Formes linéaires et espace dual

I.A) Généralités sur les formes linéaires [Gourdon et Rombaldi]

Définition 1 – Forme linéaire, espace dual

Une forme linéaire sur E est une application linéaire de E dans K. On note $E^* = \mathcal{L}(E, K)$ l'ensemble des formes linéaires, appelé espace dual de E.

Exemple 2

- Dans K^n, l'application $(x_1, \dots, x_n) \mapsto x_k$ pour un $k \in [\![1, n]\!]$ est une forme linéaire.
- Soit $A \in M_n(K)$. L'application $f_A : M \mapsto \mathrm{Tr}(AM)$ est une forme linéaire sur $M_n(K)$.
- Si $K = \mathbb{R}$ et $f : E \to \mathbb{R}$ est différentiable en un point a, alors $d_a f$ est une forme linéaire.
- Le morphisme d'évaluation $ev_a : P \mapsto P(a)$ en un point $a \in K$ est une forme linéaire sur $K_n[X]$.

Proposition 3

Le noyau d'une forme linéaire non nulle est un hyperplan de E, c'est-à-dire un sous-espace vectoriel de E de dimension $n-1$. Dans ce cas, elle est surjective.
Réciproquement, tout hyperplan de E est le noyau d'une forme linéaire non nulle.

Exemple 4

Si A est non nul, $\{M \in M_n(K) \mid \mathrm{Tr}(AM) = 0\}$ est un hyperplan de $M_n(K)$.

Proposition 5

Soit φ une forme linéaire non-nulle, $\exists x_0 \in E$ tel que $E = \ker(\varphi) \oplus \mathbb{K}x_0$

Proposition 6

Si φ_1 et φ_2 sont deux formes linéaires telles que $\ker(\varphi_1) \subset \varphi_2$. Alors elles sont proportionnelles.

I.B) Espace dual et base duale [Gourdon, Francinou Algèbre 1, Brezis Analyse fonctionnelle]

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E.

Définition 7

On appelle base duale de B la base $B^* = (e_1^*, \dots, e_n^*)$ où chaque e_i^*, défini par $e_i^*(e_j) = \delta_{i,j}$ pour tout j, est l'application donnant la i-ième coordonnée dans la base B.

Exemple 8

- $B = ((1,0),(0,1))$ est une base de K^2. Sa base duale est composée des applications $(x, y) \mapsto x$ et $(x, y) \mapsto y$.
- Soit $B = (E_{ij})_{1 \le i,j \le n}$. La base duale de B est $B^* = (f_{E_{ij}})_{1 \le i,j \le n}$.

Proposition 9

Toute base duale est une base de E^*. En particulier, $\dim(E) = \dim(E^*)$ et pour tout $\varphi \in E^*$, on a $\varphi = \sum_{i=1}^n \varphi(e_i) e_i^*$.

Corollaire 10

$x = \sum_i x_i e_i \longmapsto \varphi = \sum_i x_i e_i^*$ est un isomorphisme de E dans E^*. Il n'est cependant pas canonique car il dépend de la base B choisie.

Théorème 11 – Théorème de Riesz-Fréchet

Soit H un espace de Hilbert. Alors pour toute application $\varphi \in H_0 = H^*$, il existe un unique $f \in H$ tel que

$$\forall v \in H, \quad \varphi(v) = \langle f \mid v \rangle.$$

De plus, l'application $\varphi \mapsto f$ est une isométrie :

$$\|f\|_H = \|\varphi\|_{H_0}.$$

Application 12

Si E est l'espace euclidien (resp. hermitien) $\mathbb{R}^n$ (resp. $\mathbb{C}^n$) muni de son produit scalaire usuel, on a l'isomorphisme canonique de E dans E^* :

$$x \longmapsto \langle x \mid \cdot \rangle.$$

Proposition 13

L'application $f : A \mapsto f_A = \mathrm{Tr}(A.)$ est un isomorphisme de $M_n(K)$ dans son dual. De plus, toute forme linéaire f sur $M_n(K)$ vérifiant $f(XY) = f(YX)$ est colinéaire à la trace.

Application 14

Si $n \ge 2$, tout hyperplan de $M_n(K)$ coupe $GL_n(K)$.

I.B. Espace bidual et base antéduale

Définition 15

$E^{**} = (E^*)^*$ est appelé espace bidual de E^*.

Proposition 16

On a un isomorphisme de E dans E^{**} donné par

$$\Theta : E \longrightarrow E^{**}, \quad x \longmapsto (f \mapsto f(x)).$$

Proposition 17

Soit $B^* = (f_1, \dots, f_n)$ une base de E^*. Alors il existe une unique base $B = (e_1, \dots, e_n)$ de E dont B^* est la base duale. B est alors appelée *base antéduale*.

Exemple 18

Soient $(a_i)_{0\leq i\leq n}$ une famille de points de K deux à deux distincts. Notons

$$\ell_i = \prod_{j\neq i} \frac{X - x_j}{x_i - x_j} \in K_n[X]$$

et $B^* = (\ell_0, \dots, \ell_n)$ la base (de $\mathbb{K}_n[X]^*$) des polynômes de Lagrange.
Alors la base antéduale de B est $(\mathrm{ev}_{a_0}, \dots, \mathrm{ev}_{a_n})$.

II.Autour de l'orthogonalité

II.A. Notion d'orthogonalité

Définition 19

- On dit que $\varphi \in E^*$ et $x \in E$ sont orthogonaux si $\varphi(x) = 0$.
- Pour $A \subset E$, on définit
$$A^\perp = \{\varphi \in E^* \mid \forall x \in A,\ \varphi(x) = 0\},$$
l'orthogonal de A.
- Pour $B \subset E^*$, on définit l'orthogonal de B par
$$B^\circ = \{x \in E \mid \forall \varphi \in B,\ \varphi(x) = 0\}.$$

Proposition 20

- Si $A_1 \subset A_2 \subset E$, on a $A_2^\perp \subset A_1^\perp$.
- Si $B_1 \subset B_2 \subset E^*$, on a $B_2^\circ \subset B_1^\circ$.
- Si $A \subset E$, on a $A^\perp = \mathrm{Vect}(A)^\perp$ et si $B \subset E^*$, on a $B^\circ = \mathrm{Vect}(B)^\perp$.

Théorème 21

Soit F (resp. G) un sous-espace vectoriel de E (resp. E^*).
- On a $\dim(F) + \dim(F^\perp) = \dim(E)$ et $(F^\perp)^\circ = F$.
- On a $\dim(G) + \dim(G^\circ) = \dim(E)$ et $(G^\circ)^\perp = G$.

Application 22

- Soient $(f_i)_{1\leq i\leq k} \in (E^*)^k$ de rang r. Alors $F = \bigcap_{i=1}^k \ker(f_i)$ est de dimension $n - r$.
- Réciproquement, si G est un sous-espace vectoriel de dimension $n - r$, il existe r formes linéaires indépendantes dont G est l'intersection des noyaux.

Exemple 23

L'ensemble des applications linéaires qui s'annulent sur un hyperplan de E forme une droite de E^*.

Exemple 24

Soit $E = \mathbb{R}^4$ et $(e_i)_{1\leq i\leq 4}$ les vecteurs de la base canonique. Soit $F = \mathrm{Vect}(e_1 + e_2 + e_3,\ e_2 - e_4)$. Alors $F = \ker(\varphi_1) \cap \ker(\varphi_2)$, où $\varphi_1(a, b, c, d) = a - c$ et $\varphi_2(a, b, c, d) = b + d - a$.

II.B. Transposée d'une application linéaire [Rombaldi]

Soit F un autre $\mathbb{K}$-espace vectoriel de dimension finie p et $u \in \mathcal{L}(E, F)$.

Définition 25

On définit l'application transposée de u par

$${}^t u : F^* \longrightarrow E^*, \quad f \longmapsto f \circ u.$$

Proposition 26

- $u \mapsto {}^t u$ est linéaire et injective de $\mathcal{L}(E, F)$ dans $\mathcal{L}(F^*, E^*)$,
- $\mathrm{Im}({}^t u) = \ker(u)^\perp$,
- $\mathrm{Im}(u^\perp) = \ker({}^t u)$,
- Si $v \in \mathcal{L}(F, G)$ où G est un K-espace vectoriel, alors ${}^t(v \circ u) = {}^t u \circ {}^t v$.

Proposition 27

Soient B et B_0 deux bases de E et F, de bases duales B^* et B_0^*. Alors

$$M_{B_0^*, B^*}(u) = \left(M_{B, B_0}({}^t u)\right)^\mathsf{T}.$$

En particulier, $\mathrm{rg}({}^t u) = \mathrm{rg}(u)$.

Proposition 28

Si P est la matrice de passage d'une base B de E vers une base B_0, alors la matrice de passage de B^* vers B_0^* est $(P^{-1})^\mathsf{T}$.

III. Applications

III.A. Utilisation de la dualité dans la recherche de sous-espaces propres [Rombaldi, Mansuy]

Soit $f \in \mathcal{L}(E)$. On suppose connues les notions de polynôme minimal (noté π_f) et de polynôme minimal local (noté $\pi_{f,x}$ en un point x).

Proposition 29

F est f-stable si et seulement si $F^\perp$ est ${}^t f$-stable.

Proposition 30

Soit $x \in E$ tel que $\pi_{f,x} = \pi_f$. Alors $E_{f,x} = \mathbb{K}[f](x)$ admet un supplémentaire f-stable.

Théorème 31 – Décomposition de Frobenius

Il existe une unique suite finie de polynômes unitaires $P_1, \dots, P_s$, appelés **invariants de similitude**, et une décomposition $E = \bigoplus_{i=1}^s E_i$ en sous-espaces stables de E tels que :
- $P_{i+1} \mid P_i$ pour tout $1 \leq i \leq s - 1$,
- $f_{|E_i}$ est cyclique de polynôme minimal P_i pour tout $1 \leq i \leq s$.

Corollaire 32

Dans des bases adéquates, la matrice de f est diagonale par blocs avec, pour blocs, les matrices compagnons $(C(P_i))_{1\leq i\leq s}$. On dit que c'est la **forme réduite** de f.

Théorème 33 – Décomposition de Jordan

III.B.Calcul différentiel [Objectif Agreg, Gourdon, PGCD]

On se place sur $\mathbb{K} = \mathbb{R}$ et on considère $(E, \langle ., . \rangle)$ un espace euclidien.

Proposition 34

Si $f : E \to \mathbb{R}$ est différentiable en $a \in E$, alors il existe un unique vecteur, appelé *gradient* de f en a et noté $\nabla f(a)$, tel que :

$$\forall h \in E, \quad d_a f(h) = \langle \nabla f(a) \mid h \rangle.$$

Application 35

Géométriquement, le gradient s'interprète comme la direction de plus grande pente de f autour de a. C'est l'idée utilisée dans de nombreux algorithmes d'optimisation.

Théorème 36 – Méthode du gradient à pas optimal

— L'application Φ atteint son minimum en $\overline{x}$ et seulement en ce point.
— Soit $a \in \mathbb{R}^n$ distinct de $\overline{x}$ et $(x_k)_k$ la suite de $\mathbb{R}^n$ définie par :

$x_0 = a$,

$\alpha_k = \frac{||\nabla\Phi(x_k)||^2}{||\nabla\Phi(x_k)||_A^2}$ si $x_k \neq \overline{x}$ et 0 sinon

et $x_{k+1} = x_k - \alpha_k \nabla\Phi(x_k)$ La suite $(x_k)_k$ converge vers $\overline{x}$. De plus $\forall k \geq 0$,

$$||x_{k+1} - \overline{x}|| \leq \sqrt{\frac{\lambda_{max}}{\lambda_{min}}} \left(\frac{\lambda_{max} - \lambda_{min}}{\lambda_{max} + \lambda_{min}}\right)^{k+1} ||x_0 - \overline{x}||$$

Théorème 37 – Théorème des extrema liés

Soit $f, g_1, \ldots, g_r : U \subset \mathbb{R}^n \to \mathbb{R}$ des fonctions de classe C^1 définies sur U ouvert. Notons

$$\Gamma = \{x \in U \mid g_1(x) = \cdots = g_r(x) = 0\}.$$

Si $f|_\Gamma$ admet un extremum local en $a \in \Gamma$ et si les formes linéaires $(dg_1(a), \ldots, dg_r(a))$ sont libres, alors il existe des réels (uniques) $\lambda_1, \ldots, \lambda_r$, appelés *multiplicateurs de Lagrange*, tels que

$$df(a) = \sum_{i=1}^{r} \lambda_i \, dg_i(a).$$

Application 38

Tout endomorphisme symétrique de E admet une valeur propre réelle. En effet soit f un endomorphisme symétrique réelle, on cherche à maximiser sur la sphère unité la fonction $x \mapsto < f(x), x >$

Application 39

1. Soient $x_1, \ldots, x_n$ des vecteurs de $(E, \langle \cdot \mid \cdot \rangle)$ un espace préhilbertien (réel ou complexe). Alors

$$|\det((\langle x_i \mid x_j \rangle)_{1 \leq i,j \leq n})| \leq \prod_{i=1}^{n} \|x_i\|^2.$$

2. Soient $x_1, \ldots, x_n$ des vecteurs de $\mathbb{C}^n$. Alors

$$|\det(x_1, \ldots, x_n)| \leq \prod_{i=1}^{n} \|x_i\|_2,$$

où $\| \cdot \|_2$ désigne la norme hermitienne standard sur $\mathbb{C}^n$.

Dans les deux cas, on a égalité si et seulement si la famille $\{x_i\}_{1 \leq i \leq n}$ est orthogonale ou si l'un des vecteurs est nul.

Références :

— Gourdon Algèbre et analyse
— Rombaldi
— Bernis 40 devs pour l'agreg analyse
— Mansuy
— Brézis Analyse fonctionnelle

Table des matières

I Formes linéaires et espace dual **1**
I.A Généralités sur les formes linéaires [Gourdon et Rombaldi] . . . 1
I.B Espace dual et base duale [Gourdon, Francinou Algèbre 1, Brezis Analyse fonctionnelle] . . . 1
I.B. Espace bidual et base antéduale . . . 1

II.Autour de l'orthogonalité [Gourdon p 126, Rombaldi Chap 14] **2**
II.A. Notion d'orthogonalité . . . 2
II.B. Transposée d'une application linéaire . . . 2

III. Applications **2**
III.A. Utilisation de la dualité dans la recherche de sous-espaces propres . . . 2
III.B.Calcul différentiel . . . 2

Leçon n° 161 : Espaces vectoriels et espaces affines euclidiens : distances, isométries.

Piroutet Alban

28 juillet 2026

Soit $\mathcal{E}$ et $\mathcal{F}$ deux espaces affines et $\vec{E}$, $\vec{F}$ leurs sev associés

I Espaces affines, euclidiens. Notion de distance

I.A) Applications affines [Audin, Rombaldi]

Définition 1 – Application affine

Soit $f : \mathcal{E} \to \mathcal{F}$ est dite affine s'ils existent $\vec{f} \in L(E, F)$ et $O \in \mathcal{E}$ tels que $\forall B \in \mathcal{E}$, $\overrightarrow{f(O)f(B)} = \vec{f}(\overrightarrow{OB})$

Remarque 2

L'application affine ne dépend pas du point de départ mais seulement de la partie linéaire.

Exemple 3

Les constantes, les applications linéaires, homothéties.

Proposition 4

Une composée d'applications affines est encore affine avec : $\overrightarrow{f \circ g} = \vec{f} \circ \vec{g}$.

Corollaire 5

On peut définir alors le groupe affine $\mathcal{GA}(\mathcal{E})$ le groupe des applications affines de $\mathcal{E}$.

Proposition 6

L'application : $GA(\mathcal{E}) \to GL(E), f \mapsto \vec{f}$ est un morphisme de groupe surjectif de noyau le groupe des translations de $\mathcal{E}$, isomorphe lui même au groupe $(E, +)$.

Lemme 7

Soit O un point de $\mathcal{E}$. Soit f un isomorphisme linéaire de E. Il existe une unique application affine $\vec{f}$ dont f est l'application linéaire associée et qui fixe O.

Lemme 8

Soit E un espace affine de direction $\vec{E}$ et soit $O \in E$. Soit $f : \vec{E} \to \vec{E}$ un isomorphisme linéaire. Il existe une unique application affine

$$\varphi : E \to E$$

telle que

$$\vec{\varphi} = f \quad \text{et} \quad \varphi(O) = O.$$

Théorème 9 – Théorème de structure des applications affines

Étant donné un point $O \in E$, toute application affine φ de E dans lui-même s'écrit de façon unique sous la forme

$$\varphi = t_{\vec{u}} \circ \psi,$$

où $t_{\vec{u}}$ est une translation de vecteur $\vec{u} \in \vec{E}$ et où ψ est une application affine de E dans lui-même qui fixe O, c'est-à-dire $\psi(O) = O$.

I.B. Isométries affines [Audin]

Définition 10

Un espace affine est dit euclidien si son espace vectoriel associé est euclidien. On définit alors $d(A, B) = \left\|\overrightarrow{AB}\right\|$

Définition 11

Une isométrie vectorielle est une application linéaire qui conserve la norme (ou encore le produit scalaire via l'identité du parallélogramme).

Une isométrie affine si f préserve les distances ie $\forall A, B \in \mathcal{E}, d(f(A), f(B)) = d(A, B)$.

Proposition 12

Les ensembles $O(E)$, $Isom(\mathcal{E})$, munis de la composition des applications, sont des groupes.

Exemple 13

Les translations, symétries orthogonales et réflexion.

I.C. Distance et matrices de Gram [Gourdon]

Définition 14

Matrice de Gram

Proposition 15

Matrice de Gram $\iff$ matrice hermitienne positive.

Théorème 16 – Déterminant de Gram, distance à un sous-espace vectoriel

II. Etude du groupe orthogonale

II.A. Générateurs et réduction [Perrin + Audin]

Remarque 17

Le théorème de structure justifie cette étude.

Définition 18

$O_n(\mathbb{R})$

Proposition 19
$O(\mathbb{R}^n) \simeq O_n(\mathbb{R})$ isomorphes

Proposition 20
$O(E)$ agit transitivement sur les bases orthonormées.

Définition 21
$SO(E)$

Proposition 22
Centre de $O(E)$ et $SO(E)$

Définition 23
Renversements et réflexions

Théorème 24
$O(E)$ est engendré par les réflexions et $SO(E)$ par les renversements

Théorème 25
Réduction des éléments de $O_n(\mathbb{R})$.

II.B. Topologie et structure [Perrin, Objectif Agreg, Carnet de voyage en Algébrie]

Proposition 26
$O_n(\mathbb{R})$ est compact

Proposition 27
$O_n(\mathbb{R})$ possède deux composantes connexes : $O_n^+(\mathbb{R})$ et $O_n^-(\mathbb{R})$

Théorème 28
$SO_3(\mathbb{R})$ est simple.

II.C. Conséquences sur le cas affine

Définition 29
Isométries positives, déplacements.

Proposition 30
Les éléments de $I_S(\mathcal{E})$ sont engendrés par au plus $n+1$ réflexion.

III. Classification

III.A. Isométries du plan [Audin, H2G2 tome premier]

Théorème 31
Classification des éléments de $O_2(\mathbb{R})$

Théorème 32
Classification des isométries affines en dimension 2.

Proposition 33
Groupe diédral

III.B. Isométries de l'espace

Théorème 34
Classification des éléments de $O_3(\mathbb{R})$

Théorème 35
Classification des isométries affines en dimension 3.

Théorème 36
Isométrie du cube + coloration du cube

Références :

— Audin Géométrie,

— H2G2 tome premier,

— Perrin,

— Gourdon,

— Carnet de voyage en Algébrie,

— Objectif Agreg

Table des matières

I Espaces affines, euclidiens. Notion de distance **1**
I.A Applications affines [Audin, Rombaldi] . . . 1
I.B. Isométries affines . . . 1
I.C. Distance et matrices de Gram . . . 1

II. Etude du groupe orthogonale **1**
II.A. Générateurs et réduction . . . 1
II.B. Topologie et structure . . . 2
II.C. Conséquences sur le cas affine . . . 2

III. Classification **2**
III.A. Isométries du plan . . . 2
III.B. Isométries de l'espace . . . 2

Leçon n° 162 : Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.

Piroutet Alban

28 juillet 2026

Soit $\mathbb{K}$ un corps, $n, p \in \mathbb{N}^*$.

I De l'intersection d'hyperplans aux systèmes linéaires

I.A) Rencontre naturelle de systèmes linéaires [Rombaldi]

Théorème 1
F est de dimension $r \iff$ c'est l'intersection de $n-r$ hyperplans.

Remarque 2
Un hyperplan= une équation à n inconnnues, on a donc pour F un espace de dimension r, $n-r$ équations.

I.B) Conditions d'existence et unicité des solutions [Griffone]

Définition 3
Système compatible et homogène.

Remarque 4
On peut se ramener au cas $AX = B$ et on parle de rang du système par $rg(A)$.

Exemple 5
Exemple de système compatible et pas compatible.

Théorème 6
Le système $AX = B$ est compatible si et seulement si $B \in Im(A)$ et S l'ensemble des solutions est un sous-espace affine dirigé par $\ker(A)$ et de dimension $p - rg(A)$.

Application 7
Si $A \in M_n(\mathbb{K})$ alors $\dim(\mathcal{C}(A)) \geq n$.

Définition 8
Système de Cramer

Proposition 9
Une et une seule solution donnée par calcul de déterminant.

I.C. Cas des matrices triangulaires [Ciarlet introduction à l'analyse numérique matricielle]

Proposition 10
Méthode de remontée en $O(n^2)$ opérations élémentaires dans le corps de base.

Remarque 11
On cherche donc après des opérations dites élémentaires sur la matrice à se ramener à une matrice triangulaire et utiliser la méthode de la remontée.

II. Résolution pratique d'un système linéaire

II.A. Algorithme du pivot de Gauss [Objectif Agreg, Griffone Algèbre linéaire, Nouveaux H2G2 Caldéro, Fleury Calcul formel]

Proposition 12
L'ensemble des solutions ne change pas après opérations élémentaires sur A.

Définition 13
Matrice de transvection, dilatation, transposition.

Proposition 14
Multplication à gauche = agir sur les lignes, multiplication à droite = agir sur les colonnes.

Définition 15
Matrice échelonnée en ligne

Exemple 16
Exemple de telle matrice

Définition 17
Action par translation à gauche $(P, A) \mapsto PA$

Théorème 18
Action sur les lignes et on a toujours une forme échelonnée réduite dans une orbite.

Application 19
Algo de pivot de Gauss $\implies$ se ramener à échelonnée réduite par opérations élémentaires.

Exemple 20
Exemple de passage de matrice à échelonnée réduite.

Remarque 21
$rg(A)$ pivvots donc le reste donne les conditions de comptatibilité

Application 22
Calcul en $O(n^3)$ opérations élémentaires de $rg(A)$, $\ker(A)$, $Im(A)$, $\det(A)$ et A^{-1}

II.B. Applications du pivot de Gauss [Rombaldi, Griffone, Francinou 2 Algèbre]

Théorème 23
Ici, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, générateurs de $SL_n(\mathbb{K})$ et $GL_n(\mathbb{K})$

Application 24
$GL_n(\mathbb{R})$ a deux composantes connexes $GL_n^+(\mathbb{R})$ et $GL_n^-(\mathbb{R})$. De plus $SL_n(\mathbb{K})$ est connexe par arcs.

Application 25

Déterminer si une famille est libre.

Application 26

Déterminer les équations vérifiant un sev

Application 27

Vérifier si un vecteur $v \in \text{Vect}(v_1, \dots, v_p)$

Application 28

Vérifier si $\{v_1, \dots, v_p\}$ est génératrice

Théorème 29 – Factorisation LU

Soit $A \in \mathcal{M}_n(\mathbb{K})$ une matrice dont tous les mineurs principaux sont non nuls. Alors il existe un unique couple (L, U) de matrices tel que L est triangulaire inférieure avec diagonale de 1, U est triangulaire supérieure et $A = LU$.

Théorème 30 – Factorisation de Cholesky

Soit A une matrice symétrique réelle définie positive. Alors il existe une unique matrice B triangulaire inférieure telle que tous ses éléments diagonaux soient positifs et $A = BB^*$

Application 31

Si $A \in GL_n(\mathbb{K})$ admet une décomposition $A = LU$, on résout $AX = B$ en résolvant $LY = B$ puis $UX = Y$. Ces deux systèmes étant triangulaires, ils ont un coût moins important. De même dans le cas de la factorisation de CHOLESKY.

II.C. Résolution numérique [Ciarlet, Allaire, Bernis]

On suppose dans cette partie que $n = p$ et $A \in S_n^{++}(\mathbb{R})$ est une matrice symétrique définie positive. On pose $\langle ., . \rangle$ le produit scalaire usuel sur $\mathbb{R}^n$.

Théorème 32 – Méthode du gradient à pas optimal

— L'application Φ atteint son minimum en $\overline{x}$ et seulement en ce point.

— Soit $a \in \mathbb{R}^n$ distinct de $\overline{x}$ et $(x_k)_k$ la suite de $\mathbb{R}^n$ définie par :

$x_0 = a$,

$\alpha_k = \frac{||\nabla\Phi(x_k)||^2}{||\nabla\Phi(x_k)||_A^2}$ si $x_k \neq \overline{x}$ et 0 sinon

et $x_{k+1} = x_k - \alpha_k \nabla\Phi(x_k)$ La suite $(x_k)_k$ converge vers $\overline{x}$. De plus $\forall k \geq 0$,

$$||x_{k+1} - \overline{x}|| \leq \sqrt{\frac{\lambda_{max}}{\lambda_{min}}} \left(\frac{\lambda_{max} - \lambda_{min}}{\lambda_{max} + \lambda_{min}}\right)^{k+1} ||x_0 - \overline{x}||$$

Proposition 33 – Méthode des moindres carrés + décomposition en valeurs singulières

III. Autres applications/ approches avec l'analyse [Gourdon]

Théorème 34 – Equation de Sylvester

Soient $A, B \in \mathcal{M}_n(\mathbb{C})$ deux matrices dont les valeurs propres sont de partie réelle strictement négative. Alors pour tout $C \in \mathcal{M}_n(\mathbb{C})$, l'équation $AX + XB = C$ admet une unique solution $X \in \mathcal{M}_n(\mathbb{C})$.

Références :

— Rombaldi,

— Grifone Algèbre linéaire,

— Ciarlet introduction à l'analyse numérique matricielle,

— Nouvelles H2G2 TOME 1

— Francinou Algèbre 2

— Objectif Agreg

— Allaire Analyse numérique

— Bernis 40 devs pour l'agreg

— Gourdon Algèbre, Analyse

Table des matières

I De l'intersection d'hyperplans aux systèmes linéaires **1**

I.A Rencontre naturelle de systèmes linéaires [Rombaldi] . . . 1

I.B Conditions d'existence et unicité des solutions [Griffone] . . . 1

I.C. Cas des matrices triangulaires . . . 1

II. Résolution pratique d'un système linéaire **1**

II.A. Algorithme du pivot de Gauss . . . 1

II.B. Applications du pivot de Gauss . . . 1

II.C. Résolution numérique . . . 2

III. Autres applications/ approches avec l'analyse (Sylvester) **2**

Leçon n° 170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité. Applications.

Piroutet Alban

Agrégation de Mathématiques — 2025

E est un $\mathbb{K}$-espace vectoriel de dimension finie n, où $\mathbb{K}$ est un corps de caractéristique différente de 2.

I Généralités sur les formes quadratiques

I.A) Formes bilinéaires et formes quadratiques [Rombaldi, Griffone, Gourdon]

Définition 1
Forme bilinéaire symétrique

Définition 2
Matrice d'une forme bilinéaire + expression dans un base

Définition 3
Forme quadratique et forme polaire

Proposition 4
Unicité de la forme polaire et formule de polarisation

Remarque 5
Une forme quadratique est un polynôme homogène de degré 2.

Proposition 6
Isomorphisme entre $Q(E)$ et $S_2(E)$ et donc dimension de $Q(E)$.

Exemple 7
Exemples de formes quadratiques et forme polaire associée.

Remarque 8
Vision matricielle des formes quadratiques : si on note $M = (\varphi(e_i, e_j))$ alors $\varphi(x) = X^T M X$

Proposition 9
Soit q une forme quadratique, l'ensemble des matrices représentant q dans une base de E est exactement l'une des orbites de l'action par congruence sur $\mathcal{S}_n(\mathbb{K})$:

$$\mathcal{GL}_n(\mathbb{K}) \times \mathcal{S}_n(\mathbb{K}) \longrightarrow \mathcal{S}_n(\mathbb{K}), \quad (P, S) \longmapsto P^\top S P$$

Définition 10
On définit le discriminant de $S \in \mathcal{S}_n(\mathbb{K})$ par $\overline{\det(S)} \in \mathbb{K}^*/(\mathbb{K}^*)^2$ si S est inversible et 0 sinon.

Proposition 11
Deux matrices congruentes ont même discriminant, on peut donc définir le discriminant d'une forme quadratique.

I.B. Orthogonalité, rang, isotropie [Rombaldi]

Définition 12
Deux éléments orthogonaux et orthogonal d'une partie.

Théorème 13
Les différentes propriétés sur les orthogonaux.

Définition 14
Définition vecteur isotrope et cône isotrope.

Exemple 15
Cônes isotropes de $q(x, y) = x^2 - y^2$ et $q(x, y, z) = x^2 + y^2 - z^2$ +annexe.

Définition 16
Noyau d'une forme quadratique

Proposition 17
$\mathrm{Rad}(q) \subset \mathcal{C}_q$

Proposition 18
Forme quadratique non-dégénérée + définie

Définition 19
Rang d'une forme quadratique

Théorème 20
$F \oplus F^\perp = E \iff q_F$ est non-dégénérée.

Définition 21
Base q-orthogonale

Théorème 22
Existence d'une base q-orthogonale.

II.Réduction et classification des formes quadratiques

II.A. Réduction de Gauss [Griffone, Rombaldi, Gourdon, Fleury]

Théorème 23 – Réduction de Gauss
Pour toute forme quadratique sur E, il existe un entier r, $\lambda_1, \ldots, \lambda_r \in \mathbb{K}^*$ et $l_1, \ldots, l_r$ des formes linéaires indépendantes tels que $q(x) = \sum_{i=1}^{r} \lambda_i l_i^2$

Corollaire 24
La forme polaire associée à q est alors $\varphi(x, y) = \sum_{i=1}^{r} \lambda_i l_i(x) l_i(y)$

Exemple 25

$q(x,y,z) = -x^2 - y^2 - z^2 + 2(xy + xz + yz) = -(x - y - z)^2 + (y + z)^2 + (y - z)^2$

Corollaire 26

Il existe une base orthogonale pour q. La matrice de q dans cette base est $\text{diag}(\lambda_1, \dots, \lambda_n)$ où $\lambda_i = 0$ pour $i > r$. En particulier $r = \text{rang}(q)$ et $\ker(q) = \bigcap_{i=1}^{r} \ker(l_i)$

Définition 27

On dit que q est définie si $q(x) \neq 0$ pour tout $x \neq 0$. On dit que q est positive (resp négative) si $q(x) \geq 0$ (resp $q(x) \leq 0$) pour tout $x \neq 0$.

Lemme 28 – Cauchy-Schwarz

Si q est positive, alors on a

$$|\varphi(x,y)| \leq \sqrt{q(x)}\sqrt{q(y)}$$

Proposition 29

Si q est positive son radical est égal à son cône isotrope.

Remarque 30

Classifier les formes quadratiques revient à chercher les orbites de l'action par congruence.

Soit E une forme quadratique sur E de rang r.

II.B. Sur $\mathbb{R}$ [Griffone, Gourdon]

Théorème 31 – Loi d'inertie de Sylvester

Il existe un unique couple d'entier $(s,t) \in \mathbb{N}^2$ tel que pour toute base q-orthogonale $(e_i)_{1 \leq i \leq n}$ de E, $s = \text{Card}(\{i \in [\![1,n]\!], q(e_i) > 0\})$ et $t = \text{Card}(\{i \in [\![1,n]\!], q(e_i) < 0\})$ De plus $s + t = \text{rang}(q)$. Un tel couple est appelé signature de la forme quadratique q.
On a alors que la matrice de q dans n'importe quelle base est congruente à $\text{diag}(I_r, -I_t, 0_{n-r})$.

Corollaire 32

Lien positivité et signature

Exemple 33

Donner un exemple de forme quadratique réelle et lien avec sa signature.

Corollaire 34

Deux formes quadratiques réelles sont congruentes si elles ont même signature.

Remarque 35

On a donc $r + 1$ classes d'équivalences pour les formes quadratiques de rang r.

Théorème 36 – Critère de Sylvester

La signature (s,t) de q est entièrement déterminée par :

$$s = \max(\{\dim(F) | F \in \mathcal{P}\}),\ t = \max(\{\dim(F) | F \in \mathcal{N}\})$$

où $\mathcal{P}$ (resp. $\mathcal{N}$) désigne l'ensemble des sous-espaces de $\mathbb{R}^n$ sur lesquels la restriction de q est définie positive (resp. définie négative).

Exemple 37

La signature de $M \mapsto \text{tr}(M^2)$ est $(\frac{n(n+1)}{2}, \frac{n(n-1)}{2})$.

Théorème 38 – Théorème spectral

Soit ϕ une forme quadratique définie positive sur E et ψ forme quadratique quelconque. Alors il existe une base orthonormée pour ϕ et orthonormale pour ψ.

III.C. Sur $\mathbb{C}$ [Griffone]

Théorème 39 – Classification sur $\mathbb{K} = \mathbb{C}$(ou $\mathbb{K}$ algébriquement clos)

La matrice de q dans une certaine base est $J_r = \text{diag}(I_r, 0_{n-r})$ où $r = \text{rang}(q)$. Dans cette base, on a donc $q(x_1, \dots, x_n) = x_1^2 + \dots + x_r^2$.

Corollaire 40

Deux formes quadratiques sur un $\mathbb{C}$ espace-vectoriel sont congruentes si et seulement si elles ont même rang.

Application 41

Il y a donc $n + 1$ classes de congruences de formes quadratiques sur E.

III.C. Sur $\mathbb{F}_q$ [Rombaldi]

On suppose $\mathbb{K} = \mathbb{F}_q$ où $q = p^l$ pour un p premier impair et $l \in \mathbb{N}^*$. On note $\mathbb{F}_q^2 = \{x^2 | x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{2*} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$

Théorème 42 – Classification sur $\mathbb{K} = \mathbb{F}_q$

Soit $\alpha \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{2*}$ la matrice de q dans une certaine base est $\text{diag}(I_{r-1}, \delta, 0_{n-r})$ où $\delta \in \{1, \alpha\}$.

Application 43

Il y a $2n + 1$ classes de congruences de formes quadratiques sur E.

Théorème 44 – Loi de réciprocité quadratique

Soient $p \neq q$ des nombres premiers impairs. Alors :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \text{ où } \left(\frac{x}{q}\right) = \begin{cases} 0 & \text{si } x = 0, \\ 1 & \text{si } x \text{ est un carré dans } \mathbb{F}_p^*, \\ -1 & \text{sinon.} \end{cases}$$

Proposition 45

Soient a, b deux entiers et p un nombre premier, alors $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Théorème 46 – Loi de réciprocité quadratique complémentaires

Soit p un nombre premier impair

— $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

— $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Application 47

$\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = \dots$ Ainsi 26 n'est pas un carré modulo 307

III.Application [PGCD, H2G2]

Théorème 48 – Forme de Hankel

Soit $P \in \mathbb{R}[X]$ de degré n et $x_1, \dots, x_t$ ses racines distinctes, de multiplicité $m_1, \dots, m_t$. On définit $s_k = \sum_{l=1}^{t} m_l x_l^k$ pour $k \in \mathbb{N}$. Puis on pose :

$$\forall (X_0, \dots, X_{n-1}) \in \mathbb{C}^n, s(X_1, \dots, X_n) = \sum_{0 \leq i,j \leq n-1} s_{i+j} X_i X_j$$

Alors $s_{\mathbb{R}}$ la restriction de s à $\mathbb{R}^n$ est une forme quadratique sur $\mathbb{R}^n$, de signature (p, q) où $p+q = t$ et $p-q$ est le nombre de racines réelles de P.
Intérêt calcul de la forme de Gauss sans connaître les racines de P.

Application 49

Application aux polynômes de degré 2 et 3

Proposition 50

La différentielle seconde est une forme quadratique.

Théorème 51 – Lemme de Morse

Soient U un ouvert de $\mathbb{R}^n$ contenant l'origine, et $f : U \to \mathbb{R}$ une fonction de classe C^3 sur U. On suppose que $df_0 = 0$, et que la forme quadratique $d^2 f_0$ est non dégénérée, de signature $(p, n-p)$. Alors il existe un C^1-difféomorphisme φ entre deux voisinages de l'origine dans $\mathbb{R}^n$ tel que $\varphi(0) = 0$ et telle que :

$$f(x) - f(0) = \varphi_1(x)^2 + \dots + \varphi_p(x)^2 - \varphi_{p+1}(x)^2 - \dots - \varphi_n(x)^2$$

où $\varphi(x) = (\varphi_1(x), \dots, \varphi_n(x))$

Références :

— -Rombaldi,

— - Histoires hédonistes de groupes et géométries, Tome 1, Caldero, Germoni

— Gourdon Algèbre

— Grifone Algèbre linéaire

— PGCD

— Fleury Algèbre et calcul formel

Table des matières

I Généralités sur les formes quadratiques **1**

I.A Formes bilinéaires et formes quadratiques [Rombaldi, Griffone, Gourdon] 1

II.Réduction et classification des formes quadratiques **1**

II.A. Réduction de Gauss 1

II.B. Sur $\mathbb{R}$ 2

II.C. Sur $\mathbb{C}$ 2

III.C. Sur $\mathbb{F}_q$ 2

III.Application **3**

Leçon n° 171 : FORMES QUADRATIQUES RÉELLES. CONIQUES. EXEMPLES ET APPLICATIONS.

Piroutet Alban

Agrégation de Mathématiques — 2025

E est un $\mathbb{K}$-espace vectoriel de dimension finie n, où $\mathbb{K}$ est un corps de caractéristique différente de 2.

I Généralités sur les formes quadratiques

I.A) Formes bilinéaires et formes quadratiques [Rombaldi, Griffone, Gourdon]

Définition 1
Forme bilinéaire symétrique

Définition 2
Matrice d'une forme bilinéaire + expression dans un base

Définition 3
Forme quadratique et forme polaire

Proposition 4
Unicité de la forme polaire et formule de polarisation

Remarque 5
Une forme quadratique est un polynôme homogène de degré 2.

Proposition 6
Isomorphisme entre $Q(E)$ et $S_2(E)$ et donc dimension de $Q(E)$.

Exemple 7
Exemples de formes quadratiques et forme polaire associée.

Remarque 8
Vision matricielle des formes quadratiques : si on note $M = (\varphi(e_i, e_j))$ alors $\varphi(x) = X^T M X$

Proposition 9
Soit q une forme quadratique, l'ensemble des matrices représentant q dans une base de E est exactement l'une des orbites de l'action par congruence sur $\mathcal{S}_n(\mathbb{K})$:

$$\mathcal{GL}_n(\mathbb{K}) \times \mathcal{S}_n(\mathbb{K}) \longrightarrow \mathcal{S}_n(\mathbb{K}), \quad (P, S) \longmapsto P^\top S P$$

Définition 10
On définit le discriminant de $S \in \mathcal{S}_n(\mathbb{K})$ par $\overline{\det(S)} \in \mathbb{K}^*/(\mathbb{K}^*)^2$ si S est inversible et 0 sinon.

Proposition 11
Deux matrices congruentes ont même discriminant, on peut donc définir le discriminant d'une forme quadratique.

I.B. Orthogonalité, rang, isotropie [Rombaldi]

Définition 12
Deux éléments orthogonaux et orthogonal d'une partie.

Théorème 13
Les différentes propriétés sur les orthogonaux.

Définition 14
Définition vecteur isotrope et cône isotrope.

Exemple 15
Cônes isotropes de $q(x, y) = x^2 - y^2$ et $q(x, y, z) = x^2 + y^2 - z^2$ +annexe.

Définition 16
Noyau d'une forme quadratique

Proposition 17
$\mathrm{Rad}(q) \subset \mathcal{C}_q$

Proposition 18
Forme quadratique non-dégénérée + définie

Définition 19
Rang d'une forme quadratique

Théorème 20
$F \oplus F^\perp = E \iff q_F$ est non-dégénérée.

Définition 21
Base q-orthogonale

Théorème 22
Existence d'une base q-orthogonale.

II.Réduction, classification des formes quadratiques réelles

II.A. Réduction de Gauss [Griffone, Rombaldi, Gourdon, Fleury]

Théorème 23 – Réduction de Gauss
Pour toute forme quadratique sur E, il existe un entier r, $\lambda_1, \ldots, \lambda_r \in \mathbb{K}^*$ et $l_1, \ldots, l_r$ des formes linéaires indépendantes tels que $q(x) = \sum_{i=1}^{r} \lambda_i l_i^2$

Corollaire 24
La forme polaire associée à q est alors $\varphi(x, y) = \sum_{i=1}^{r} \lambda_i l_i(x) l_i(y)$

Exemple 25

$q(x,y,z) = -x^2 - y^2 - z^2 + 2(xy + xz + yz) = -(x - y - z)^2 + (y + z)^2 + (y - z)^2$

Corollaire 26

Il existe une base orthogonale pour q. La matrice de q dans cette base est $\text{diag}(\lambda_1, \dots, \lambda_n)$ où $\lambda_i = 0$ pour $i > r$. En particulier $r = \text{rang}(q)$ et $\ker(q) = \bigcap_{i=1}^{r} \ker(l_i)$

Définition 27

On dit que q est définie si $q(x) \neq 0$ pour tout $x \neq 0$. On dit que q est positive (resp négative) si $q(x) \geq 0$ (resp $q(x) \leq 0$) pour tout $x \neq 0$.

Lemme 28 – Cauchy-Schwarz

Si q est positive, alors on a

$$|\varphi(x,y)| \leq \sqrt{q(x)}\sqrt{q(y)}$$

Proposition 29

Si q est positive son radical est égal à son cône isotrope.

Remarque 30

Classifier les formes quadratiques revient à chercher les orbites de l'action par congruence.

Soit E une forme quadratique sur E de rang r.

II.B. Classification des formes quadratiques réelles [Griffone, Gourdon]

Théorème 31 – Loi d'inertie de Sylvester

Il existe un unique couple d'entier $(s,t) \in \mathbb{N}^2$ tel que pour toute base q-orthogonale $(e_i)_{1 \leq i \leq n}$ de E, $s = \text{Card}(\{i \in [\![1,n]\!], q(e_i) > 0\})$ et $t = \text{Card}(\{i \in [\![1,n]\!], q(e_i) < 0\})$ De plus $s + t = \text{rang}(q)$. Un tel couple est appelé signature de la forme quadratique q.
On a alors que la matrice de q dans n'importe quelle base est congruente à $\text{diag}(I_r, -I_t, 0_{n-r})$.

Corollaire 32

Lien positivité et signature

Exemple 33

Donner un exemple de forme quadratique réelle et lien avec sa signature.

Corollaire 34

Deux formes quadratiques réelles sont congruentes si elles ont même signature.

Remarque 35

On a donc $r + 1$ classes d'équivalences pour les formes quadratiques de rang r.

Théorème 36 – Critère de Sylvester

La signature (s,t) de q est entièrement déterminée par :

$$s = \max(\{\dim(F) | F \in \mathcal{P}\}),\ t = \max(\{\dim(F) | F \in \mathcal{N}\})$$

où $\mathcal{P}$ (resp. $\mathcal{N}$) désigne l'ensemble des sous-espaces de $\mathbb{R}^n$ sur lesquels la restriction de q est définie positive (resp. définie négative).

Exemple 37

La signature de $M \mapsto \text{tr}(M^2)$ est $(\frac{n(n+1)}{2}, \frac{n(n-1)}{2})$.

Théorème 38 – Théorème spectral

Soit ϕ une forme quadratique définie positive sur E et ψ forme quadratique quelconque. Alors il existe une base orthonormée pour ϕ et orthonormale pour ψ.

II.C. Application [PGCD, H2G2]

Théorème 39 – Forme de Hankel

Soit $P \in \mathbb{R}[X]$ de degré n et $x_1, \dots, x_t$ ses racines distinctes, de multiplicité $m_1, \dots, m_t$. On définit $s_k = \sum_{l=1}^{t} m_l x_l^k$ pour $k \in \mathbb{N}$. Puis on pose :

$$\forall (X_0, \dots, X_{n-1}) \in \mathbb{C}^n, s(X_1, \dots, X_n) = \sum_{0 \leq i,j \leq n-1} s_{i+j} X_i X_j$$

Alors $s_{\mathbb{R}}$ la restriction de s à $\mathbb{R}^n$ est une forme quadratique sur $\mathbb{R}^n$, de signature (p,q) où $p + q = t$ et $p - q$ est le nombre de racines réelles de P.
Intérêt calcul de la forme de Gauss sans connaître les racines de P.

Application 40

Application aux polynômes de degré 2 et 3

Proposition 41

La différentielle seconde est une forme quadratique.

Théorème 42 – Lemme de Morse

Soient U un ouvert de $\mathbb{R}^n$ contenant l'origine, et $f : U \to \mathbb{R}$ une fonction de classe C^3 sur U. On suppose que $df_0 = 0$, et que la forme quadratique $d^2 f_0$ est non dégénérée, de signature $(p, n-p)$. Alors il existe un C^1-difféomorphisme φ entre deux voisinages de l'origine dans $\mathbb{R}^n$ tel que $\varphi(0) = 0$ et telle que :

$$f(x) - f(0) = \varphi_1(x)^2 + \dots + \varphi_p(x)^2 - \varphi_{p+1}(x)^2 - \dots - \varphi_n(x)^2$$

où $\varphi(x) = (\varphi_1(x), \dots, \varphi_n(x))$

III. Application à l'étude des coniques

III.A. Vocabulaire [Audin]

On se place dans un plan affine euclidien $\mathcal{P}$, muni d'un repère orthonormé.

Définition 43

Une conique $\mathcal{C}$ est l'ensemble des points (x,y) deP satisfaisant l'équation :

$$ax^2 + 2bxy + cy^2 + dx + ey + f = 0 \quad (1)$$

où $a, b, c, d, e, f \in \mathbb{R}$ sont des paramètres, avec $(a,b,c) \neq (0,0,0)$. $q(x,y) = ax^2 + bxy + cy^2$ est la forme quadratique associée à E, supposée non nulle, et $l(x,y) = dx + ey$ est la forme linéaire associée à E.

Remarque 44

q ne dépend pas de l'origine O choisi.

Définition 45

Un point Ω est centre de symétrie de $\mathcal{C}$ si dans le repère $(\Omega, \vec{i}, \vec{j})$, la partie linéaire de l'équation définissant $\mathcal{C}$ est nulle. $\mathcal{C}$ est dite à centre si elle admet un unique centre de symétrie.

Proposition 46

$\mathcal{C}$ est à centre unique $\iff$ q est non-dégénérée.

Exemple 47

— $\Omega = (a, b)$ est l'unique centre de la conique définie par $(x-a)^2 + (y-b)^2 = c$ dans $(O, \vec{i}, \vec{j})$.
— Une conique de type $ax^2 + dx + ey + f = 0$ n'est pas à centre

Proposition 48

Si $\mathcal{C}$ est à centre, il existe un repère orthonormé de $\mathcal{P}$, d'origine Ω, dans lequel l'équation $\mathcal{C}$ est du type $\alpha x^2 + \beta y^2 = \gamma$ avec $(\alpha, \beta) \neq (0, 0)$

Définition 49

On définit $Q(x, y, z) = q(x, y) + l(x, y)z + fz^2$ la forme quadratique sur $\mathbb{R}^3$ appelée forme homogénéisée de q. $\mathcal{C}$ est dite propre si Q est non dégénérée.

Exemple 50

Les coniques propres sont de « vraies » coniques : ce ne sont pas des droites.

Théorème 51 – Classification des coniques propres

$\text{sgn}(Q)$	$\text{sgn}(q)$	Classe	Exemple
$(3,0)/(0,3)$	$(2,0)/(0,2)$	$\varnothing$	$x^2 + y^2 = -1$
$(2,1)/(1,2)$	$(2,0)/(0,2)$	ellipse	$x^2 + y^2 = 1$
$(2,1)/(1,2)$	$(1,1)$	hyperbole	$x^2 - y^2 = 1$
$(2,1)/(1,2)$	$(1,0)/(0,1)$	parabole	$x^2 + y = 0$

Théorème 52 – Classification des coniques impropres

$\text{sgn}(Q)$	$\text{sgn}(q)$	Classe	Exemple
$(2,0)/(0,2)$	$(2,0)/(0,2)$	point	$x^2 + y^2 = 0$
$(2,0)/(0,2)$	$(1,0)/(0,1)$	$\varnothing$	$x^2 = -1$
$(1,1)$	$(1,1)$	droites sécantes	$x^2 - y^2 = 0$
$(1,1)$	$(1,0)/(0,1)$	droites parallèles	$x^2 = 1$
$(1,0)/(0,1)$	$(1,0)/(0,1)$	droite double	$x^2 = 0$

III.B. Point de vue géométrique [Audin, Rombaldi]

Théorème 53 – Caractérisation foyer-directrice

Soit $\mathcal{C}$ une conique propre non vide qui n'est pas un cercle. Alors il existe un point $F \in \mathcal{P}$, appelé foyer, une droite D ne contenant pas F, appelée directrice, et un réel $e > 0$, appelé excentricité, tels que
$\mathcal{C} = \{M \in \mathcal{P} \mid d(M, F) = e\, d(M, D)\}$.
— Si $e < 1$, $\mathcal{C}$ est une ellipse.
— Si $e = 1$, $\mathcal{C}$ est une parabole.
— Si $e > 1$, $\mathcal{C}$ est une hyperbole.

Définition 54

La perpendiculaire à D passant par F est appelée axe focal. C'est un axe de symétrie de la conique.

Théorème 55 – Équation dans le repère focal

Dans le repère $(F, \vec{i}, \vec{j})$, où $\vec{i}$ est unitaire dirigeant l'axe focal et $\vec{j}$ unitaire parallèle à D, l'équation de $\mathcal{C}$ est, en notant p l'abscisse de D :
$(1 - e^2)x^2 + y^2 + 2pe^2x - p^2e^2 = 0$.

Proposition 56

Si $\mathcal{C}$ est à centre ($e \neq 1$), alors le centre a pour coordonnées
$\left(-\frac{pe^2}{1-e^2}, 0\right)$
dans le repère $(F, \vec{i}, \vec{j})$.
Par symétrie, $\mathcal{C}$ est aussi la conique caractérisée par le foyer F' et la directrice D' symétriques de F et D par rapport au centre.

Proposition 57 – Définition bifocale des coniques propres à centre

— Si $\mathcal{C}$ est une ellipse (qui n'est pas un cercle), alors $\mathcal{C} = \{M \in \mathcal{P} \mid MF + MF' = 2a\}$, pour un réel $2a$ appelé grand axe de $\mathcal{C}$.
— Si $\mathcal{C}$ est une hyperbole, alors $\mathcal{C} = \{M \in \mathcal{P} \mid |MF - MF'| = 2a\}$, pour un réel $2a$ appelé grand axe de $\mathcal{C}$.

Références :

— -Rombaldi,
— - Histoires hédonistes de groupes et géométries, Tome 1, Caldero, Germoni
— Gourdon Algèbre
— Grifone Algèbre linéaire
— PGCD
— Fleury Algèbre et calcul formel
— Audin Géométrie

Table des matières

I Généralités sur les formes quadratiques **1**
I.A Formes bilinéaires et formes quadratiques [Rombaldi, Griffone, Gourdon] . . . 1

II.Réduction et classification des formes quadratiques **1**
II.A. Réduction de Gauss . . . 1
II.B. Sur $\mathbb{R}$ . . . 2
II.C. Application . . . 2

III. Application à l'étude des coniques **2**
III.A. Vocabulaire . . . 2
III.B. Point de vue géométrique . . . 3

Leçon n° 181 : Convexité dans $\mathbb{R}^n$. Applications en algèbre et en géométrie.

Piroutet Alban

28 juillet 2026

Soit E un $\mathbb{R}$-espace vectoriel de dimension $n \geq 1$. X un espace affine de direction E.

I Ensembles et fonctions convexes

I.A. Barycentres [Audin, Tauvel]

Définition 1

Soit $\mathcal{E}$ un $\mathbb{K}$-espace affine, on appelle point pondéré de $\mathcal{E}$ tout couple $(A, \lambda) \in \mathcal{E} \times \mathbb{K}$. Soient $(A_i, \lambda_i)_{i\in[\![1,n]\!]}$ une famille de points pondérés, on appelle masse totale de cette famille le scalaire $\sum_{i=1}^n \lambda_i$.

Définition 2

Soit $(A_i, \lambda_i)_{i\in[\![1,n]\!]}$ une famille de points pondérés de E. Si la masse totale de cette famille est non nulle, on définit le barycentre des (A_i, λ_i) comme l'unique point $G \in E$ tel que

$$\sum_{i=1}^n \lambda_i \overrightarrow{GA_i} = 0.$$

Proposition 3

Soient $G \in E$ et $(A_i, \lambda_i)_{i\in[\![1,n]\!]}$ une famille de points pondérés de masse totale non nulle. Les conditions suivantes sont équivalentes :

- G est le barycentre des $(A_i, \lambda_i)_{i\in[\![1,n]\!]}$,
- il existe $O \in E$ tel que :
$$\sum_{i=1}^n \lambda_i \overrightarrow{OA_i} = \left(\sum_{i=1}^n \lambda_i\right) \overrightarrow{OG},$$
- pour tout $O \in E$, on a :
$$\sum_{i=1}^n \lambda_i \overrightarrow{OA_i} = \left(\sum_{i=1}^n \lambda_i\right) \overrightarrow{OG}.$$

Notations :
Soit $(A_i, \lambda_i)_{i\in[\![1,n]\!]}$ une famille de points pondérés de E.
- Si $\sum_{i=1}^n \lambda_i = 0$, l'application (2.1) est constante et on note $\sum_{i=1}^n \lambda_i A_i \in E$ la valeur de cette constante.
- Si $\sum_{i=1}^n \lambda_i = 1$, on note $\sum_{i=1}^n \lambda_i A_i \in E$ le barycentre des (A_i, λ_i).
- D'après la proposition 2.2.6, lorsque $m := \sum_{i=1}^n \lambda_i \neq 0$, le barycentre des (A_i, λ_i) est

$$\sum_{i=1}^n \frac{\lambda_i}{m} A_i \in E,$$

ce que l'on notera aussi

$$\frac{1}{m} \sum_{i=1}^n \lambda_i A_i.$$

Proposition 4 – Homogénéité du barycentre

Soient $(A_i, \lambda_i)_{i\in[\![1,n]\!]}$ tels que $\sum_i \lambda_i \neq 0$ et $\alpha \in \mathbb{K}^*$. Alors le barycentre G des $(A_i, \lambda_i)_{i\in[\![1,n]\!]}$ est aussi le barycentre des $(A_i, \alpha\lambda_i)_{i\in[\![1,n]\!]}$.

Proposition 5 – Associativité du barycentre

Soit $p \in \mathbb{N}^*$, soient $n_1, \ldots, n_p \in \mathbb{N}^*$ et soit $(A_{ij}, \lambda_{ij})_{i\in[\![1,p]\!], j\in[\![1,n_i]\!]}$ une famille de points pondérés de E.
Supposons que :

$$\forall i \in [\![1,p]\!], \quad \sum_{j=1}^{n_i} \lambda_{ij} \neq 0, \qquad \text{et} \qquad \sum_{i=1}^{p}\sum_{j=1}^{n_i} \lambda_{ij} \neq 0.$$

On note G le barycentre des $(A_{ij}, \lambda_{ij})_{i\in[\![1,p]\!], j\in[\![1,n_i]\!]}$, et pour tout $i \in [\![1,p]\!]$ on note G_i le barycentre des $(A_{ij}, \lambda_{ij})_{j\in[\![1,n_i]\!]}$.
Alors G est aussi le barycentre de la famille

$$\left(G_i, \sum_{j=1}^{n_i} \lambda_{ij}\right)_{i\in[\![1,p]\!]}.$$

Application 6

Concours des médianes d'un triangle

Définition 7

Soit $n \in \mathbb{N}^*$ non divisible par la caractéristique $\mathrm{car}(K)$ du corps K, alors l'*isobarycentre* (ou centre de gravité) des points $A_1, \ldots, A_n \in E$ est le barycentre des points pondérés $(A_1, 1), \ldots, (A_n, 1)$.
Lorsque $\mathrm{car}(K) \neq 2$, l'isobarycentre de A et B est appelé le *milieu* de A et B.

Application 8 – Gourdon

Suites de polygone + dessin annexe

I.B. Parties convexes d'un espace affine réel [Tauvel]

Définition 9

Segment fermé et ouvert

Définition 10

C est convexe si et seulement si tout segment reste dans C.

Exemple 11

Les convexes de $\mathbb{R}$ sont les intervalles.

Exemple 12

Les boules sont convexes

Définition 13

Combinaison convexe

Proposition 14

C convexe ssi tte combinaison convexe de points de C reste dans C.

Proposition 15

Un convexe est connexe par arcs.

Proposition 17

L'image directe et réciproque d'un convexe par une application affine est convexe

Application 18

Les demi-espaces sont convexes.

Proposition 19

Une intersection quelconque de convexes reste convexe.

Définition 20

Enveloppe convexe.

I.C. Fonctions convexes [Rombaldi]

Soit C un convexe d'un espace vectoriel normé $(E, \|\|)$.

Définition 21

La fonction $f : C \to \mathbb{R}$ est dite convexe si

$$\forall (x,y) \in C^2, \forall \lambda \in [0,1], f(\lambda x + (1-\lambda)y) \leq \lambda f(x) + (1-\lambda) f(y)$$

Définition 22

On appelle épigraphe de f l'ensemble $\mathcal{E}(f) = \{(x,y) \in C \times \mathbb{R}, y \geq f(x)$.

Proposition 23

f convexe si et seulement si son épigraphe est convexe + annexe.

Proposition 24

Si f est de classe dérivable alors f convexe $\iff$ f' croissante.

Proposition 25

Si f est de classe C^2 alors f convexe $\iff$ $f'' \geq 0$

Application 26

Inégalité de Hölder

Application 27

Inégalité de Jensen.

II. Propriétés topologiques

II.A. Enveloppe convexe [Tauvel + Francinou Algèbre 1 seconde addition]

Définition 28

Enveloppe convexe

Proposition 29

L'enveloppe convexe est l'ensemble des combinaisons convexes d'éléments de la partie.

Théorème 30 – Gauss-Lucas

Soit $P \in \mathbb{C}[X]$ on note $Conv(P)$ l'enveloppe convexe de ses racines. Si P est non-constant : $Conv(P') \subset Conv(P)$

Exemple 16

Les sous-espaces affines / vectoriels sont convexes.

Application 31

Déterminer le plus grand entier $n \geq 2$ tel que les racines non nulles de $(X+1)^n - X^n - 1$ soient de module 1.

Proposition 32

Si A est ouverte alors $Conv(A)$ est ouverte.

II.B. Compacité [Tauvel Géométrie]

Proposition 33

Si A est compact alors $Conv(A)$ est compacte.

Proposition 34

Si A est bornée, $Conv(A)$ l'est aussi et $\delta(A) = \delta(Conv(A))$.

II.C. Intérieur et adhérence [Tauvel Géométrie]

Proposition 35

Si A est convexe alors $\bar{A}$ et $\mathring{A}$ est convexe

Proposition 36

Si A est convexe alors $\mathring{A} \neq \emptyset \iff A$ contient $n+1$ points affinements indépendants $\iff < A >= X$.

II.D. Points extrémaux [Tauvel Géométrie]

Définition 37

Point extrémal

Proposition 38

Propriétés équivalentes

Théorème 39 – Groupe des isométries du cube

On a $Iso^+(C) \simeq \mathfrak{S}_4$ et $Iso(C) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$

Application 40

Il y a 57 manières différentes de colorier un cube avec 3 couleurs.

Références :

— Tauvel Géométrie

— H2G2 Tome premier

— Carnet de voyage en algébrie

— Gourdon Algèbre

— Rombaldi

— Audin Géométrie

Table des matières

I Ensembles et fonctions convexes **1**
I.A. Barycentres 1
I.B. Parties convexes d'un espace affine réel 1
I.C. Fonctions convexes 2

II. Propriétés topologiques **2**
II.A. Enveloppe convexe 2
II.B. Compacité 2
II.C. Intérieur et adhérence 2
II.D. Points extrémaux 2

Leçon n° 190 : Méthodes combinatoires, problèmes de dénombrement.

Piroutet Alban

28 juillet 2026

I Notion de dénombrement et de combinatoire

I.A) Bijections entre cardinaux [Gourdon Algèbre Proba+ Duverney théorie des nombres]

Définition 1

Un ensemble E est fini s'il est vide ou s'il existe $n \in \mathbb{N}^*$ tel qu'il existe une bijection de $[\![1, n]\!]$ dans E. Dans ce cas, l'entier n ne dépend pas de la bijection, on l'appelle cardinal de E

Proposition 2

Soient E et F deux ensembles.

1. Si E est fini et s'il existe une bijection de E vers F, alors F est fini et $|F| = |E|$.
2. Si F est fini et s'il existe une injection de E vers F, alors E est fini et $|E| \leq |F|$, avec égalité $\iff$ f bijective.
3. Si E est fini et s'il existe une surjection de E vers F, alors F est fini et $|F| \leq |E|$, avec égalité $\iff$ f bijective.

Définition 3

Deux ensembles sont dits équipotents s'il existe une bijection de l'un dans l'autre.

Corollaire 4 – Principe des tiroirs

Soient E et F deux ensembles finis avec $|E| > |F|$. Si φ est une application de E vers F, alors il existe $y \in F$ ayant au moins deux antécédents par φ dans E.

Application 5 – Théorème de Dirichlet

Soient $\alpha \in \mathbb{R}$ et $N \in \mathbb{N}^*$, il existe $(p, q) \in \mathbb{Z}^2$ avec $q \in [\![1, N]\!]$ tels que $|\alpha - \frac{p}{q}| < \frac{1}{qN}$. En bonus : la mesure d'irrationalité d'un irrationnel est au moins égale à 2.

I.B) Principe additif [Gourdon, Algèbre Proba ; Foata et Fuchs, Calcul des probabilités]

Proposition 6

Soit B un ensemble fini et A une partie de B. Alors A est fini et $|A| \leq |B|$ avec égalité si et seulement si $A = B$.

Proposition 7

$\text{card}(A \cup B) = \text{card}(A) + \text{card}(B) - \text{card}(A \cap B)$.

Corollaire 8

Si $A_1, \dots, A_n$ sont des ensembles finis deux à deux disjoints alors $|\cup_{i=1}^n A_i| = \sum_{i=1}^n |A_i|$.

Proposition 9

Si $B \subset A$ avec A fini, alors $\text{card}(A \setminus B) = \text{card}(A) - \text{card}(B)$.

Lemme 10 – Lemme des bergers

Lemme des bergers : pour $f : E \to F$ et $y \in F$, $n_y = \text{card}(f^{-1}(\{y\}))$, alors

$$\sum_{y \in F} n_y = \text{card}(E).$$

Proposition 11 – Formule du crible de Poincaré

Soient $A_1, \dots, A_n$ des ensembles finis. Alors on a : $|\bigcup_{i=1}^n A_i| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < \cdots < i_k \leq n} |A_{i_1} \cap \cdots \cap A_{i_k}|$

I.C. Principe multiplicatif

Proposition 12

Soient n ensembles finis $E_1, \dots, E_n$. Le produit cartésien $E_1 \times \cdots \times E_n$ est un ensemble fini et on a $|E_1 \times \cdots \times E_n| = |E_1| \times \cdots \times |E_n|$. En particulier, pour un ensemble E fini, on a $|E^n| = |E|^n$.

Définition 13

k-liste et p-arrangement d'un ensemble à n éléments + cardinal.

Proposition 14

Soient E et F deux ensembles finis.

1. L'ensemble des applications de E dans F noté F^E est fini avec $|F^E| = |F|^{|E|}$.
2. Si $n = |E|$ et $p = |F|$, le nombre d'application de E dans F injective est $A_n^p = \frac{n!}{(n-p)!}$ + interprétation en terme de tirage de boule (tirage sans remise je crois)
3. Si $n = |E|$, l'ensemble des bijections de E dans E est fini et de cardinal égal à $n!$.

Proposition 15

Si E est un ensemble fini, l'ensemble de ces parties $\mathcal{P}(E)$ est fini et de cardinal égale à $2^{|E|}$.

I.D. Coefficients binomiaux et combinatoire [Gourdon, Rombaldi]

Définition 16

Définition, formules classiques (somme des coefficients binomiaux + preuve, formule de PASCAL, de VANDERMOND)

Proposition 17

Soit $n \in \mathbb{N}$, $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

Proposition 18

Formule de binôme de Newton

I.E. Séries génératrices [Gourdon, Algèbre Proba, Algèbre le grand combat]

Définition 19

Série génératrice et série exponentielle

Remarque 20

Une relation de récurrence entre les termes de la suite se traduit par une équation fonctionnelle vérifiée par la série génératrice.

Application 21

Nombre de dérangement, nombres de Bell

II. Formule d'inversion

II.A. Inversion de Pascal [Rombaldi + carnet de voyage en algébrie]

Théorème 22

Formule d'inversion de Pascal

Corollaire 23

Nombre de surjections

II.B. Inversion de Möbius [Rombaldi + carnet de voyage en algébrie]

Définition 24

Fonction de Möbius

Lemme 25

Calcul de $\sum_{d|n} \mu(d)$

Théorème 26

Inversion de Möbius

Théorème 27

$X^{p^n} - X = \prod_{d|n} \prod_{P \in U_n(p)} P$ et dénombrement des polynômes irréductibles de degré donné avec équivalent.

Application 28

Probabilité que deux nombres soient premiers entre eux. (si t'es chaud)

III. Groupes et combinatoire

III.A. Actions de groupes [Rombaldi, Gourdon, H2G2, Carnet de voyage]

Théorème 29 – Théorème de Lagrange

Si G est un groupe fini alors pour tout sous-groupe H de G l'ordre de H divise l'ordre de G. En particulier, l'ordre de tout élément divise le cardinal du groupe.

Proposition 30

Si morphisme de groupe, lien entre les cardinaux de l'image et du noyau

Définition 31

Action de groupe. Et définition équivalente se donner un morphisme.

Définition 32

Orbites et stabilisateur

Proposition 33

Si G est fini, $\forall x \in X, |G| = |w(x)| \times |\mathrm{Stab}(x)|$

Théorème 34

Equations aux classes

Théorème 35

Formule de Burnside.

Application 36

Isométrie du cube + il est possible de colorier de 57 manières les face d'un cube avec au plus 3 couleurs.

IV. Dénombrement en algèbre

IV.A. Dénombrement sur un corps fini [H2G2, Rombaldi]

Soit $p \in \mathcal{P}$ et $q = p^n$ où $n \in \mathbb{N}^*$. On note $\mathbb{F}_q$ le corps à q éléments.

Proposition 37

Cardinaux de $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathrm{SL}_n(\mathbb{F}_q)$

On note $\mathbb{F}_q^2 = \{x^2 \mid x \in \mathbb{F}_q\}$ et $(\mathbb{F}_q^2)^* = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

Proposition 38

Si $p = 2$, alors $\mathbb{F}_q^2 = \mathbb{F}_q$. Sinon, on a

$$\#\mathbb{F}_q^2 = \frac{q+1}{2}$$

Application 39

Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, l'équation

$$ax^2 + by^2 = c$$

admet des solutions dans $\mathbb{F}_p$.

Proposition 40

$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} [p]$

Théorème 41 – Loi de réciprocité quadratique

Soient p, q deux entier impairs premiers, alors $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$

Remarque 42

Le résultat de cette application est fondamentale dans la théorie de la réduction des formes quadratiques sur un corps finis.

Références :

— Rombaldi Algèbre,

— Gourdon Algèbre Proba,

— Duverney théorie des nombres,

— Carnet de voyage en algébrie,

— Algèbre le grand combat,

— Foata et Fuchs, Calcul des probabilités section proba discrète et dénombrement

Table des matières

I Notion de dénombrement et de combinatoire **1**
I.A Bijections entre cardinaux [Gourdon Algèbre Proba+ Duverney théorie des nombres] 1
I.B Principe additif [Gourdon, Algèbre Proba ; Foata et Fuchs, Calcul des probabilités] 1
I.C. Principe multiplicatif [Gourdon, Algèbre Proba] 1
I.D. Coefficients binomiaux et combinatoire [Gourdon, Algèbre Proba] 1
I.E. Séries génératrices 1

II. Formule d'inversion **2**
II.A. Inversion de Pascal 2
II.B. Inversion de Möbius 2

III. Groupes et combinatoire **2**
III.A. Actions de groupes 2

IV. Dénombrement en algèbre **2**
IV.A. Dénombrement sur un corps fini 2

191. Exemples d'utilisation de techniques d'algèbre en géométrie

Alban Piroutet et Lever Hugo

Agrégation de Mathématiques — 2025

I Application de l'algèbre linéaire

I.A) Classification des isométries d'un espace euclidien [Rombaldi + Gourdon]

Définition 1

Soit E un espace euclidien, une isométrie de E une application $u : E \to E$ qui converse le produit scalaire, ie $\langle u(x), u(y)\rangle = \langle x, y\rangle \, \forall x, y \in E$.

Théorème 2

Une application $u : E \to E$ est une isométrie si, et seulement si, elle est linéaire et converse la norme.

Théorème 3 – Classification des isométries d'un espace euclidien

Soit $u \in \mathcal{O}(E)$ avec $\dim(E) = n \geq 2$. Il existe une base orthonormée $\mathcal{B}$ de E dans laquelle la matrice de u s'écrit :

$$\begin{pmatrix} I_p & 0 & 0 & \cdots & 0 \\ 0 & -I_q & 0 & \cdots & 0 \\ 0 & 0 & \begin{matrix}\cos\theta_1 & -\sin\theta_1 \\ \sin\theta_1 & \cos\theta_1\end{matrix} & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & & \begin{matrix}\cos\theta_r & -\sin\theta_r \\ \sin\theta_r & \cos\theta_r\end{matrix} \end{pmatrix},$$

avec $\forall k \in [\![1, r]\!], \theta_k \in]0, 2\pi[\setminus\{\pi\}$ et p, q, r sont des entiers naturels tels $p + q + 2r = n$ (si l'un de ces entiers est nul, les blocs de matrices correspondants n'existent pas).

Corollaire 4

Les composantes connexes de $\mathcal{O}(E)$ sont $\mathcal{O}^+(E)$ et $\mathcal{O}^-(E)$.

I.B) Déterminant de Gram [Gourdon , Rombaldi]

Définition 5

On appelle matrice de Gram, notée $G(x_1, ..., x_n)$, la matrice de coefficients $(\langle x_i, x_j\rangle)_{i,j}$. On note $g(x_1, ..., x_n)$ son déterminant, appelé déterminant de Gram.

Proposition 6

Toute matrice de Gram est symétrique définie positive. Réciproquement, toute matrice symétrique positive est une matrice de Gram.

Proposition 7

On a $g(x_1, ..., x_n) = 0$ si et seulement si la famille $(x_1, ..., x_n)$ est liée.

Théorème 8

Soit F un sous espace vectoriel de E, $(x_1, ..., x_k)$ une base de F et $x \in E$. Alors :

$$\operatorname{dist}(x, F)^2 = \frac{g(x_1, ..., x_k, x)}{g(x_1, ..., x_k)}$$

Corollaire 9

Soit $(X_1, ..., X_n)$ une famille de vecteurs colonnes de $\mathbb{R}^n$, M la matrice formée de ces vecteurs, alors :

$$|\det(M)| \leq \prod_{i=1}^{n} \|X_i\|^2$$

Si les vecteurs sont non nuls, il y a égalité si et seulement si les vecteurs (X_i) sont orthogonaux.

Application 10

Dans le plan euclidien, le parallélogramme est d'aire maximale si et seulement si c'est un rectangle. Dans $\mathbb{R}^3$, le parallélépipède est d'aire maximale si et seulement si il est rectangle.

I.C) Volume et déterminant [Objectif Agreg, Gourdon, Rombaldi, Ulmer]

Théorème 11

Soient $u, v \in \mathbb{R}^2$. l'aire du parallélogramme engendré par u et v est égale à la valeur absolue du déterminant des deux vecteurs.

Théorème 12

On note $\operatorname{Vol}(u_1, ...u_n)$ le volume du polytope engendré par $u_1, ..., u_n$, c'est à dire l'ensemble $\{z \in \mathbb{R}^n, z = \sum \lambda_i u_i, 0 \leq \lambda_i \leq 1\}$, alors :

$$\operatorname{Vol}(u_1, ..., u_n) = |\det(u_1, ..., u_n)|$$

Application 13

L'aire d'un triangle de sommets $A = (x_A, y_A)$, $B = (x_B, y_B)$ et $C = (x_C, y_C)$ est donnée par la formule :

$$S = \frac{1}{2}\begin{vmatrix} x_B - x_A & x_C - x_A \\ y_B - y_A & y_C - y_A \end{vmatrix}$$

Voir Annexe 3

Lemme 14

Soient $(a_i)_{i\in[\![1,n]\!]} \in \mathbb{C}^n$, et

$$C = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}, \quad P(X) = \sum_{k=1}^{n} a_k X^{k-1}, \qquad \omega = e^{2\pi i/n} \text{ alors } \det C = \prod_{k=0}^{n-1} P(\omega^k).$$

Application 15

Soit $Z = (z_1, \dots, z_n) \in \mathbb{C}^n$, $\quad Z^{(0)} = Z$, $\quad Z^{(k+1)} = (z_1^{(k)}, \dots, z_n^{(k)})$.
$z_j^{(k+1)} = \frac{z_j^{(k)} + z_{j+1}^{(k)}}{2} \quad (1 \leq j \leq n)$
Alors la suite $(Z_k)_{k\in\mathbb{N}}$ converge vers l'isobarycentre des affixes $z_1, \dots, z_n$. Voir Annexe 1

Définition 16

Résultant de deux polynômes

Proposition 17

Propriétés du résultant

Proposition 18

Formule de Aaron

II. Application de la théorie des groupes en géométrie

II.A) Action de groupes et géométrie [Perrin , Rombaldi]

Remarque 19

Les actions ont un lien fort avec la géométrie : on peut agir sur une structure géométrique.

Application 20 – Théorème de Cayley

Soit G un sous-groupe fini d'ordre n alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Théorème 21 – Equations aux classes

Si G est fini, choisissons pour chaque orbite O un représentant x_O. Alors :

$$|X| = \sum_{O\in\mathcal{O}} \frac{|G|}{|\mathrm{Stab}(x_O)|}$$

Théorème 22 – Formule de Burnside

Si on considère G un groupe fini agissant sur un ensemble fini X, en notant $\mathcal{O}$ le nombre d'orbites, on a : $|\mathcal{O}| = \frac{1}{|G|}\sum_{g\in G} |\mathrm{Fix}(g)|$.

II.B) Application aux isométries laissant stable des polytopes [H2G2, Carnet de voyage en algébrie, Rombaldi]

Définition 23

Soit $\mathcal{E}$ un espace affine, soit $\mathcal{P}$ une partie de $\mathcal{E}$ ayant au moins deux éléments. On note $I_s(\mathcal{P})$ (resp$(I_s^+(\mathcal{P}), I_s^-(\mathcal{P}))$ l'ensemble des isométries de $\mathcal{E}$ qui conservent $\mathcal{P}$. Si $\varphi \in I_s(\mathcal{P})$ sa restriction à $\mathcal{P}$ est alors une permutation de $\mathcal{P}$.

Proposition 24

Le groupe des isométries du triangle équilatéral est isomorphe à $\mathfrak{S}_3$.

Théorème 25

Le groupe $\mathrm{I_s}(C)$ des isométries qui conservent le cube C est aussi le groupe $\mathrm{I_s}(S)$ des isométries qui conservent l'ensemble S de ses sommets, et c'est un groupe fini isomorphe à un sous-groupe du groupe symétrique S_8. La symétrie de centre 0, $\sigma_0 : x \mapsto -x$, appartient à $\mathrm{I_s}^-(C)$; l'application $\rho \mapsto \rho \circ \sigma_0$ réalise une bijection de $\mathrm{I_s}^+(C)$ sur $\mathrm{I_s}^-(C)$ et $|\mathrm{I_s}(C)| = 2|\mathrm{I_s}^+(C)|$.

Théorème 26

Le groupe $\mathrm{I_s}(S)$ agit de façon transitive sur S et il a 48 éléments. Le groupe $\mathrm{I_s}^+(S)$ est isomorphe à $\mathfrak{S}_4$ et le groupe $\mathrm{I_s}(S)$ est isomorphe à $\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Application 27

Il y a 57 manières de colorier un cube avec au plus trois couleurs.

III. Application de la théorie des corps à la géométrie [Gozard, Carréga]

III.A) Construction à la règle et au compas [Carrega, Gozard]

$\mathcal{P}$ le repère affine euclidien orienté, on identifie un point à ses coordonnées.

Définition 28

Soit X une partie de $\mathcal{P}$ de cardinal au moins 2. On considère les droites affines de $\mathcal{P}$, passant par deux points A et B de X, et le cercle de centre A et passant par B. Un point $M \in \mathcal{P}$ est constructible en un pas à partir de X, si et seulement si, il existe : deux droites ou bien une droite et un cercle, ou bien deux cercles, dont M soit un point d'intersection.

Remarque 29

Chaque point de X est constructible en un pas à partir de X.

Définition 30

On définit par récurrence être constructible en n pas à partir d'une base B. Et on appelle ensemble des points constructibles (à la règle et au compas) l'ensemble de ces points.

On prendra dans la suite $B = \{0, I\}$.

Proposition 31

On peut construire :
- le symétrique d'un point par rapport à un autre
- le milieu de deux points et la médiatrice entre deux points
- la perpendiculaire à une droite passant par un point
- la parallèle à une droite passant par un point

III.B) Nombres constructibles [Carrega, Gozard]

Définition 32

On dit que $x \in \mathbb{R}$ est constructible si $(0, x)$ est constructible (ou de façon équivalente $(x, 0)$).

Proposition 33

Tout rationnel est constructible.

Proposition 34

Le point $M = (x, y)$ est constructible $\iff$ x et y le sont.

Théorème 35

L'ensemble des réels constructibles est un sous-corps de $\mathbb{R}$ stable par racine carré.

Théorème 36 – Wantzel

Un réel t est constructible $\iff$ il existe une suite finie $(L_0, \dots, L_n)$ de sous-corps de $\mathbb{R}$ vérifiant :
- $L_0 = \mathbb{Q}$
- L_{i+1} est une extension quadratique de L_i
- $t \in L_n$

Remarque 37

On appelle tour d'extension quadratique une telle suite.

Corollaire 38

Si x est constructible, il existe $p \in \mathbb{N}$ tel que $[\mathbb{Q}(x) : \mathbb{Q}] = 2^p$.

Remarque 39

La réciproque est fausse. On considère le polynôme $P = X^4 - 4X + 2$, on montre alors que P admet une racine réelle non-constructible alors que l'extension qu'elle engendre sur $\mathbb{Q}$ est de degré 4.

Corollaire 40

Tout nombre constructible est algébrique.

III.C) Réponses à quelques grands problème de géométrie [Carrega, Gozard]

Application 41

La duplication du cube à la règle et au compas est impossible

Application 42

En admettant la transcendance de π, on montre que la quadrature du cercle est impossible à la règle et au compas

Références :

— Perrin,

— Gourdon,

— Carnet de voyage en algébrie,

— H2G2 Tome premier,

— Carréga,

— Gozard,

— Objectif Agreg,

— Ulmer Anneaux et résultant.

Table des matières

I Application de l'algèbre linéaire **1**
- I.A Classification des isométries d'un espace euclidien [Rombaldi + Gourdon] . . . 1
- I.B Déterminant de Gram [Gourdon , Rombaldi] . . . 1
- I.C. Volume et déterminant . . . 1

II. Application de la théorie des groupes en géométrie **2**
- II.A. Action de groupes et géométrie . . . 2
- II.B. Application aux isométries laissant stable des polytopes . . . 2

III. Application de la théorie des corps à la géométrie **2**
- III.A. Construction à la règle et au compas . . . 2
- III.B. Nombres constructibles . . . 2
- III.C.Réponses à quelques grands problème de géométrie . . . 3