

101 : Groupe opérant sur un ensemble.
Exemples et applications.

Cadre : E un ensemble non vide et $\mathfrak{S}(E)$ l'ensemble des bijections de E .

I) Généralités

A) Définitions, exemples

Définition. Caractérisation par le morphisme $\Phi : G \rightarrow \mathfrak{S}(E)$. Exemples classiques d'actions. Définitions d'orbites, d'actions transitive et fidèle. Théorème de CAYLEY.

B) Dénombrer à l'aide des orbites

Définition de stabilisateur. Théorème de bijection. Équation aux classes. **DEV 1** : CARDINAL DE $\mathcal{D}_n(\mathbb{F}_q)$. Cas des classes de conjugaison. Définition de fixateur. Formule de BURNSIDE.

II) Actions sur les groupes finis

G groupe fini d'ordre n .

A) Résultats classiques

Théorème de LAGRANGE. Application aux groupes d'ordre premier. Exemple de $\mathbb{H}$.

B) Les p -groupes

Définition, E^G . Centre d'un p -groupe. Exemple. Applications aux groupes d'ordre p^2 . Exemple. Théorème de CAUCHY. p -sous-groupe de SYLOW. Théorème de SYLOW. Applications.

C) Les groupes $\mathfrak{S}_n$ et $Aut(\mathfrak{S}_n)$

Action sur $\mathfrak{S}_n$, définition d'un r -cycle. Conjugaisons des

cycles dans $\mathfrak{S}_n$ et des 3-cycles dans $\mathfrak{A}_n$. Sous-groupe d'indice n dans $\mathfrak{S}_n$. Définitions des groupes $Aut(\mathfrak{S}_n)$ et $Int(\mathfrak{S}_n)$. **DEV 1** : AUTOMORPHISMES DE $\mathfrak{S}_n$. Cas où $n = 6$.

III) Applications en algèbre linéaire

A) Actions sur des ensembles matriciels

Actions de STEINITZ. Définition de classe d'équivalence. Théorème du rang. Caractérisation des matrices diagonalisables.

B) Actions sur un espace vectoriel

Représentation linéaire. Exemples de représentation (triviale, régulière, groupe diédral). Représentation par permutation. Dénombrement des points fixes d'une permutation.

Références :

- ROMBALDI
- PERRIN
- CALDERO

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

I) Généralités

A) Autour de la fonction exponentielle

Définition des séries entières exponentielle, sinus et cosinus. Propriétés. Formule de MOIVRE et d'EULER. Applications à la linéarisation. Polynomes de CHEBYCHEV. Noyaux de DIRICHLET et FEJÉR.

B) Groupe des nombres complexes de module 1.

Définitions de $\mathbb{U}$, exemples. Argument d'un complexe non nul. Exemples. Propriétés et isomorphismes. Résolution de $z^n = z_0$. Propriétés. Racines primitives de l'unité. Indicatrice d'EULER, application.

II) Angles orientés

Isomorphisme entre $\mathbb{U}$ et $SO(\mathbb{C})$. Définitions d'angle orienté entre deux complexes non nuls puis entre 2 droites. Relation de CHASLES.

III) Polynômes cyclotomiques

Définition, exemples, propriétés des polynômes cyclotomiques. Irréductibilité du polynôme sur $\mathbb{Z}$. Application au degré de l'extensions $\mathbb{Q}(\zeta)$. Théorème de WEDDERBURN.

IV) Applications

A) Représentation linéaire

Définitions, propriétés. Lemme de SCHUR. Théorème de MASCHKE. DEV 1 : MORPHISMES DE $(\mathcal{S}^1, \times)$ DANS $(GL_n(\mathbb{R}), \times)$.

B) Spectres de matrices

Définition d'une valeur propre, exemple. Spectre d'un automorphisme orthogonal dans le cadre euclidien. DEV 2 : DÉTERMINANT CIRCULANT. Application à un calcul de déterminant.

ANNEXES : Racines n -ième de l'unité, angles orientés.

Références :

- RUDIN
- ARNAUDIÈS-FRAYSSE
- PERRIN
- ROMBALDI
- GOURDON

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

Cadre : G un groupe.

I) Généralités

A) Sous-groupe distingué

Définitions, exemples

B) Ensemble quotient

Classe à gauche, partition, LAGRANGE, relation compatible, lien avec un sous-groupe distingué. Théorème de structure de groupe sur un ensemble quotient, théorème d'isomorphisme.

C) Action par conjugaison

Définition d'une action de groupe, bijection avec l'orbite, équation aux classes. Cas d'une opération par conjugaison. Application aux p -groupes.

II) Application à la simplicité des groupes

Définition d'un groupe simple.

A) Groupes symétrique et alterné

Parties génératrices de $\mathfrak{S}_n$, exemples. Signature, groupe alterné $\mathfrak{A}_n$. DEV 1 : SIMPLICITÉ DE $\mathfrak{A}_n$, POUR $n \geq 5$. Le cas $\mathfrak{A}_4$, sous-groupes distingués de $\mathfrak{S}_n$.

B) Groupes matriciels

$(E, \langle \cdot, \cdot \rangle)$ un espace euclidien sur un corps K .

Groupes $GL(E)$ et $SL(E)$, identification aux groupes de

matrices. Réflexion, transvection, conjugaison, exemple. Retournement, exemple, partie génératrice de $O(n)$. DEV 2 : $SO_n(\mathbb{R})$ ENGENDRÉ PAR LES RETOURNEMENTS + $SO_3(\mathbb{R})$ EST SIMPLE.

III) Application au dévissage de groupes

p -groupe de SYLOW, exemple. Théorèmes de SYLOW. Application. Produit semi-direct, caractérisation. Exemples et contre-exemples de produits semi-directs.

ANNEXE : Représentations d'une dilatation, d'une transvection, d'un retournement et renversement orthogonaux.

Références :

- PERRIN
- ROMBALDI
- CALDERO

104 : Groupes finis. Exemples et applications

I) Généralités

- A) Définitions, propriétés
Définitions, exemples, LAGRANGE, sous-groupe engendré, sous-groupe distingué, exemples.
- B) Actions de groupe
Définition, exemple (conjugaison). Orbite, stabilisateur, bijection. Équation aux classes, centre d'un p -groupe. Théorème de CAUCHY, exemple.

II) Groupes abéliens finis

- A) Groupes cycliques
Groupe cyclique, exemple, structure des groupes cycliques (racines de l'unité). Exemple des groupes d'ordre premier, d'ordre pq commutatif, contre-exemple ($\mathfrak{S}_3$). Sous-groupe d'un groupe cyclique.
- B) Automorphismes de $\mathbb{Z}/n\mathbb{Z}$
Caractérisation des générateurs de $\mathbb{Z}/n\mathbb{Z}$. Fonction d'Euler. Structure de $Aut(\mathbb{Z}/n\mathbb{Z})$. Théorème chinois. Cyclicité de $(\mathbb{Z}/n\mathbb{Z})$. Application au groupe $Aut(\mathbb{Z}/n\mathbb{Z})$.

III) Groupes non abéliens finis

- A) Groupes symétrique et alterné
Définition, cardinal de $\mathfrak{S}_n$. r -cycle, transposition. Générateurs de $\mathfrak{S}_n$. Centre de $\mathfrak{S}_n$. Signature, définition de $\mathfrak{A}_n$. Cardinal de $\mathfrak{A}_n$. DEV 1 : SIMPLICITÉ DE $\mathfrak{A}_n$, POUR $n \geq 5$. Automorphisme intérieur, isomorphisme. DEV 2 : AUTOMORPHISMES DE $\mathfrak{S}_n$. Application.

- B) Le groupe diédral
Définition, caractérisation d'un groupe diédral. Produit semi-direct, cas $n = 3$, centre du groupe D_n . Groupe des isométries sur le cube.

ANNEXE : Représentation du groupe diédral.

Références :

- GOURDON
- ROMBALDI
- PERRIN

105 : Groupe des permutations d'un ensemble fini. Applications.

I) Généralités

A) Définitions, propriétés

Définition, exemple de l'ensemble $\{1, \dots, n\}$. r -cycle, transposition, exemples. Centre de $S(E)$. Cas d'ensembles en bijection. Exemple. Cardinal de $S(E)$. Exemple.

B) Actions de groupes, décomposition en cycles disjoints

Support d'une permutation, action d'une permutation, orbite, exemple. Décomposition en cycle disjoint (unique), en transpositions (plus unique)

II) Le groupe alterné

Morphisme signature, valeurs, applications à des r -cycles, exemples. Groupe alterné, ordre. **DEV 1** : SIMPLICITÉ DE $\mathfrak{A}_n$. Sous-groupes distingués de $S(E)$. Application : morphisme surjectif de $S(E)$ vers $A(E)$.

III) Applications

A) Polynômes symétriques

Définition, exemples, polynôme élémentaire. Décomposition en polynômes élémentaires, exemples.

B) Matrices de permutation

Théorème de CAYLEY, matrice de permutation, lien entre signature d'une permutation et le déterminant de sa matrice de permutation. Identification d'un groupe fini à un sous-groupe de $GL_n(\mathbb{F}_p)$, SYLOW, exemple.

C) Dérangements d'un ensemble fini

Définition, exemple, formule d'inversion de PASCAL, dénombrements du nombre de dérangements, du nombre de permutations à r points fixes, application.

IV) Automorphismes de $S(E)$

Définition, isomorphisme, cas abélien. **DEV 2** : AUTOMORPHISMES DE $\mathfrak{S}_n$. Cas $n = 6$.

Références :

- ROMBALDI
- PERRIN

106 : Groupe linéaire d'un espace vectoriel de dimension finie E , sous groupe de $GL(E)$.

Applications.

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

I) Généralités

Définitions , exemples. produit semi-direct. Caractérisation des éléments de $GL(E)$.

II) Éléments essentiels de $GL(E)$

A) Les homothéties

Définition, exemple, caractérisation des homothéties.

B) Les dilatations

Caractérisation des dilatations, exemple. Conjugaison.

C) Les transvections

Caractérisation des transvections, exemple. Conjugaison dans $GL(E)$ et $SL(E)$, exemple.

III) Étude de $GL(E)$

A) Générateurs, algorithme du pivot de GAUSS

Engendrement de $GL(E)$ et $SL(E)$. Application aux calculs de $D(GL(E))$ et $D(SL(E))$. Matrice de rang r . Ensemble des matrices échelonnées réduites en lignes. Décomposition de $\mathcal{M}_{m,n}(\mathbb{K})$ sous l'action de $GL_m(\mathbb{K})$.

B) Centres et commutateurs

Centres de $GL(E)$ et $SL(E)$. Cas où $\mathbb{K}$ est algébriquement clos. Opération de $PGL(E)$ sur $\mathbb{P}(E)$.

C) Cas des corps finis

Cardinaux des différents groupes, applications aux isomorphismes exceptionnels. DEV 1 : DÉNOMBREMENT DE $\mathcal{D}_n(\mathbb{F}_q)$.

IV) Le groupe orthogonal euclidien

Définition, groupe $O(q)$ et $O^+(q)$, exemple. Centres des deux groupes, suite exacte scindée. Définitions de réflexion et renversement orthogonale, exemples. Engendrement de $O(q)$ et $O^+(q)$ par ces derniers. Application à la simplicité de $SO_3(\mathbb{R})$. Réduction des isométries.

V) Topologie

$GL(E)$ ouvert et dense dans $\mathcal{L}(E)$, application. $GL_n(\mathbb{C})$ connexe par arcs, composantes connexes de $GL_n(\mathbb{R})$. Compacité de $O(E)$. Décomposition polaire, application. DEV 2 : MORPHISMES CONTINUS DE $\mathcal{S}^1$ DANS $GL_n(\mathbb{R})$.

ANNEXES : Représentations d'une dilatation, d'une transvection, d'une réflexion orthogonale et d'un renversement orthogonale dans le cas où $E = \mathbb{R}^2$ ou $E = \mathbb{R}^3$. Différentes actions de $GL_n(\mathbb{K})$.

Références :

- PERRIN
- ROMBALDI
- CALDERO - TOME 2

108 : Exemples de parties génératrices d'un groupe. Applications.

I) Générateurs d'un groupe

A) Sous-groupes engendrés

G un groupe, $X \subset G$ une partie.

Intersection de sous-groupes, définition d'un groupe engendré par une X , exemple. Définition de "type fini". Cas d'une partie dont les éléments commutent 2 à 2, contre-exemple avec D_n . Groupe dérivé, caractérisation d'un groupe abélien, passage au quotient, exemple de $\mathbb{H}$.

B) Ordre d'un élément

Définition, ordre de l'inverse, ordre de g^k sachant $o(g)$, application à $\mathbb{Z}/n\mathbb{Z}$.

II) Les groupes abéliens

A) Groupes monogènes

Définitions : monogène et cyclique, monogène $\Rightarrow$ abélien. Contre-exemple (groupe de KLEIN). Caractérisation des groupes monogènes. Groupe des unités Cas des groupes d'ordre premier, d'ordre pq . Fonction d'EULER, automorphismes de $\mathbb{Z}/n\mathbb{Z}$. Sous-groupe fini d'un corps commutatif.

B) Groupes abéliens finis

Théorème chinois, théorème de KRONECKER, exemple et application à $\mathbb{Z}/60\mathbb{Z}$.

III) Application à la simplicité des groupes

Définition d'un groupe simple.

A) Groupes symétrique et alterné

Parties génératrices de $\mathfrak{S}_n$, exemples. Signature, groupe alterné $\mathfrak{A}_n$. **DEV 1** : SIMPLICITÉ DE $\mathfrak{A}_n$, POUR $n \geq 5$. Le cas $\mathfrak{A}_4$, sous-groupes distingués de $\mathfrak{S}_n$.

B) Groupes matriciels

$(E, \langle \cdot, \cdot \rangle)$ un espace euclidien sur un corps K .

Groupes $GL(E)$ et $SL(E)$, identification aux groupes de matrices. Réflexion, transvection, exemple. Parties génératrices de $GL(E)$ et $SL(E)$. **Retournement, exemple, partie génératrice de $O(n)$** . **DEV 2** : $SO_n(\mathbb{R})$ ENGENDRÉ PAR LES RETOURNEMENTS + $SO_3(\mathbb{R})$ EST SIMPLE.

IV) Groupes de morphismes

Ordre d'un élément par un morphisme, isomorphisme. Ensemble $Hom(G, G')$, applications aux groupes cycliques, à $\mathfrak{S}_n$, à V_4 .

Références :

- ROMBALDI
- PERRIN
- CALDERO - TOME 2

120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

Cadre : $n \in \mathbb{N}^*$.

I) Généralités

- A) Le groupe $\mathbb{Z}/n\mathbb{Z}$
Sous-groupe $n\mathbb{Z}$, caractérisation des sous-groupes de $\mathbb{Z}$. Relation de congruence. Sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$. Isomorphisme avec les groupes cycliques d'ordre n .
- B) Automorphismes de $\mathbb{Z}/n\mathbb{Z}$
Fonction d'EULER, exemples. Isomorphisme avec les automorphismes de $\mathbb{Z}/n\mathbb{Z}$. **DEV 1** : ÉTUDE DE $(\mathbb{Z}/n\mathbb{Z})^*$.
- C) L'anneau $\mathbb{Z}/n\mathbb{Z}$
Structure d'anneau. Théorème chinois, contre-exemple dans le cas où les entiers sont seulement "premiers dans leur ensemble". passage à l'isomorphisme des inversibles.

II) Application à l'arithmétique de $\mathbb{Z}$

Théorème d'EULER puis de FERMAT. Somme des $\varphi(d)$, où d divise n . Théorème de WILSON, théorème de LIOUVILLE.

III) Application à la résolution d'équations diophantiennes

Résolution de $ax \equiv b \pmod{n}$ dans le cas particulier où $a \wedge n = 1$. Résolution dans le cas général. Utilisation du théorème chinois pour un système d'équations diophantiennes : $k \equiv a_j \pmod{n_j}$ ($1 \leq j \leq r$). **DEV 2** : SYSTÈME DE CONGRUENCES. Exemple.

IV) Application aux corps finis

- A) Les carrés de $\mathbb{F}_q$
Carrés de $(\mathbb{F}_q)^*$ et de $\mathbb{F}$. Existence d'une solution à $ax^2 +$

$by^2 = 1$. Étude du groupe $SO(\mathbb{F}_q)$. Cas de la caractéristique 2.

- B) Vers la loi de réciprocité quadratique
Symbole de LEGENDRE, loi de réciprocité quadratique. Cas de 2. Exemple.

V) Cyclotomie

Sous-groupes de l'unité, définition du n -ième polynôme cyclotomique $\Phi_{n,k}$, exemples. Degré de $\Phi_{n,k}$, relations avec $X^n - 1$, irréductibilité de $\Phi_{n,k} \in \mathbb{Z}[X]$, application au degré de l'extension de $\mathbb{Q} \subset \mathbb{Q}(\xi)$.

Références :

- ROMBALDI
- PERRIN
- GOURDON
- CALDERO

121 : Nombres premiers. Applications.

I) Généralités

A) Définitions, propriétés

Définition, exemples. Nombre infini de nombres premiers. Théorème fondamental de l'arithmétique, exemple. PGCD, PPCM, nombres premiers dans leur ensemble, deux à deux. Lien entre les deux. Théorème de BEZOUT, de GAUSS, exemples.

B) Tests de primalité

Caractérisation d'un premier avec l'anneau $\mathbb{Z}/n\mathbb{Z}$. Théorème de FERMAT, de WILSON, applications. Nombres de MERSENNE, de FERMAT.

II) Application aux polynômes

Critère d'EISENSTEIN, applications. Théorème de réduction modulo p . Faux dans $A[X]$, réciproque fausse. Polynôme cyclotomique, irréductibilité, exemples.

III) Application aux groupes

A) Les p -SYLOW

Définitions : p -groupe, p -SYLOW. Exemple de $GL_n(\mathbb{F}_p)$. Les théorèmes de SYLOW. Application aux groupes d'ordre pq . Exemples.

B) Automorphismes de $\mathbb{Z}/n\mathbb{Z}$

Caractérisation des générateurs de $\mathbb{Z}/n\mathbb{Z}$. Structure de $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$. Inversibles de $\mathbb{Z}/p\mathbb{Z}$. DEV 2 : CYCLICITÉ DE $(\mathbb{Z}/n\mathbb{Z})^*$. Application.

IV) Application aux corps finis

Caractéristique d'un corps, structure des corps finis. $(\mathbb{F}_q)^*$ cyclique. Carrés de $(\mathbb{F}_q)^*$, application. Construction d'un corps fini, exemples. Symbole de LEGENDRE DEV 2 : LOI DE RÉCIPROCITÉ QUADRATIQUE. Application.

Références :

- GOURDON
- PERRIN
- CALDERO

122 : Anneaux principaux. Exemples et applications.

Cadre : $(A, +, \cdot)$ un anneau commutatif unitaire, $\mathbb{K}$ un corps.

I) Principalité

Définition d'un idéal, exemples. Intersection d'idéaux. Morphisme d'anneaux et idéaux. Définition de A/I et ses idéaux. Idéaux maximal et premier, caractérisation. Idéal principal, anneau principal, Théorème chinois et applications.

II) Divisibilité

A) Inversibilité

Élément inversible, lien avec les idéaux, cas d'un corps.

B) Divisibilité

Définition, irréductibilité, exemples, éléments premiers entre eux, équivalence dans un anneau principal.

C) Anneaux factoriels

Éléments associés, exemples. Anneau factoriel, principal $\Rightarrow$ factoriel. Lemmes d'EUCLIDE et de GAUSS.

D) Anneaux à PGCD

PGCD, exemple, anneau à PGCD, PPCM

III) Exemples d'anneaux principaux

A) Anneaux euclidiens

Définition, exemples. Euclidien $\Rightarrow$ principal. Théorème de BEZOUT.

B) L'anneau $\mathbb{Z}[i]$

Définition, propriétés, théorème de FERMAT.

IV) Applications

A) Algèbre linéaire

Polynôme minimal, lemme des noyaux, caractérisation des endomorphismes diagonalisable, trigonalisables. Endomorphisme semi-simple, exemple. **DEV 1** : CARACTÉRISATION DES ENDOMORPHISMES SEMI-SIMPLES. Dunford adapté.

B) Facteurs invariants d'une matrice

Matrices équivalentes. **DEV 2** : FORME NORMALE DE SMITH. Cas d'un corps, exemples.

ANNEXE : Algorithme d'EUCLIDE, algorithme de la forme normale de SMITH.

Références :

- ROMBALDI
- PERRIN
- BECK-MALICK-PEYRÉ

123 : Corps finis. Applications.

Cadre $\mathbb{K}$ un corps, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, p premier

I) Construction des corps finis

- A) Extension de corps, caractéristique
Définitions d'une extension, de degré, exemples. Théorème de la base télescopique. Application. Sous-corps premier, exemple, caractéristique d'un corps, homomorphisme de FROBENIUS, exemple.
- B) Existence et unicité
Corps de décomposition, exemple, unicité et existence. Théorème de WEDDERBURN. Caractérisation des sous-corps, exemple.

II) Le corps $\mathbb{F}_q$

- A) Le groupe $(\mathbb{F}_q)^*$
Définition, cyclicité, application aux automorphismes de $\mathbb{F}_q$.
- B) Carrés de $\mathbb{F}_q$
Nombre de carrés dans $(\mathbb{F}_q)^*$ et $\mathbb{F}_q$, caractérisation d'un carré. Application à -1 et aux nombres premiers.
- C) Vers la loi de réciprocité quadratique
Symbole de LEGENDRE, exemple. DEV 1 : LOI DE RÉCIPROCITÉ QUADRATIQUE. Application. Racines d'un polynôme de degré 2 dans $\mathbb{F}_p$, racines.

III) Quelques applications des corps finis

- A) Polynômes irréductibles sur $\mathbb{F}_q$
Réduction modulo p , exemples. Polynômes unitaires irré-

ductibles de degré i $\mathcal{P}_p(i)$ sur $\mathbb{F}_p$, $I_p(i) = \text{Card}(\mathcal{P}_p(i))$ DEV 2 : POLYNÔMES IRRÉDUCTIBLES SUR $\mathbb{F}_p$.

- B) Groupes linéaires sur $\mathbb{F}_q$
Définitions de $GL(E)$, identification au groupe de matrices. Définition de $SL(E)$. Centre des 2 groupes. Groupes $PGL(E)$ et $PSL(E)$. Cardinaux des différents groupes. exemples. Isomorphismes exceptionnels. $SO_2(\mathbb{F}_q)$, nombre de matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$.

Références :

- TAUVEL
- PERRIN
- CALDERO

125 : Extensions de corps. Exemples et applications.

Cadre : $\mathbb{K}$ un corps.

I) Généralités sur les extensions de corps

Définition d'une extension, du degré, exemples. Théorème de la base télescopique. Application, exemple. Éléments algébrique et transcendant. Polynôme minimal, caractérisation. Sous-corps des éléments algébriques. Extension algébrique, exemple des extensions finie, réciproque fausse.

II) Extension de corps, polynôme

A) Corps de rupture

Définition, exemple, théorème d'existence et d'unicité. Corps isomorphes n'impliquent pas corps égaux.

B) Corps de décomposition

Définition, exemple. Théorème d'existence et d'unicité.

C) Clôture algébrique

Définition d'un corps algébriquement clos, exemple de $\mathbb{C}$ et de $\overline{\mathbb{Q}}$. Théorème de STEINITZ.

III) Application à l'irréductibilité des polynômes

A) Critère d'irréductibilité

Irréductibilité dans les extensions, applications.

B) Polynômes irréductibles sur $\mathbb{F}_p$.

Définitions de $\mathcal{P}_p(i)$ et $I_p(i)$. Corps finis via les polynômes irréductibles. **DEV 1** : POLYNÔMES IRRÉDUCTIBLES SUR $\mathbb{F}_p$.

IV) Cyclotomie

Sous-groupes des racines n -ièmes de l'unité et primitives. n -ième polynôme cyclotomique, exemple. Degré de ce polynôme et égalité. Irréductibilité de $\Phi_{n,k} \in \mathbb{Z}[X]$. Application au degré de l'extension $\mathbb{Q}(\xi)$.

V) Groupe de GALOIS

k -automorphisme, groupe de GALOIS, exemples. Lemme de DEDEKIND. Action de $Gal(D/k)$ sur l'ensemble des racines. Parties génératrice de $\mathfrak{S}_p$. Critère d'EISENSTEIN. **DEV 2** : GALOIS INVERSE.

Références :

- TAUVEL
- PERRIN

126 : Exemples d'équations en arithmétique.

Cadre : $n \in \mathbb{N}^*$.

I) Équation diophantiennes linéaires

A) À deux variables

Équation $ax = b$, théorème de BACHET-BEZOUT, algorithme d'EUCLIDE, exemple. Équation de la forme $ax + ny = c$, théorème de résolution. Exemples.

B) Généralisation à n variables

Résolution de $AX = B$ dans le cas où A est diagonale. **Forme normale de SMITH** Application à la résolution générale de $AX = B$.

II) Système de congruences

Théorème chinois, exemple et contre-exemple. Application à la résolution d'un système, exemple. Généralisation au cas où il n'y a plus de coprimauté. **DEV 1 : SYSTÈME DE CONGRUENCES.**

III) Application des nombres premiers

A) Réduction modulo un nombre premier

Critère d'EISENSTEIN, (soluce modulo p) $\Rightarrow$ (soluce sur Z). Exemple. Caractérisation des carrés de F_p , exemple.

B) Vers la loi de réciprocité quadratique

Symbole de LEGENDRE, exemple. **DEV 2 : LOI DE RÉCIPROCITÉ QUADRATIQUE.** Cas où p est pair. Exemples.

IV) Équations diophantiennes non linéaires

A) Exemples de résolution

Théorème de SOPHIE GERMAIN. Théorème de FERMAT.

B) L'anneau des entiers de GAUSS

L'anneau $Z[i]$, propriétés, l'ensemble Σ . Inversibles de $Z[i]$.

Théorème des deux carrés de FERMAT. Application.

Références :

- GOURDON
- ROMBALDI
- BECK-MALICK-PEYRÉ
- PERRIN
- CALDERO

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

Cadre : A un anneau commutatif unitaire, $Fr(A)$ son corps de fractions, K un corps, $A^\times$ les inversibles de A .

I) L'anneau $K[X]$

Définition d'un irréductible, inversibles de $A[X]$, exemple. Contenu d'un polynôme, polynôme primitif. Caractérisation des irréductibles sur $A[X]$. Exemple. Irréductibles de $K[X]$, caractérisation de la primalité de $A[X]$. Contre-exemple de $\mathbb{Z}[X]$. Caractérisation d'un quotient par un polynôme irréductible.

II) Critères d'irréductibilité

Critère EISENSTEIN, exemples. Théorème de réduction. Contre-exemple dans A . Applications.

III) Extension de corps, polynôme

A) Définitions, propriétés

Définition d'une extension, de degré, exemples. Théorème de la base télescopique, application. Définition d'un élément algébrique, transcendant, exemple. Polynôme minimal, caractérisation. Exemple du sous-corps des algébriques sur un corps.

B) Corps de rupture

Définition, exemple. Théorème d'existence et d'unicité, application à l'irréductibilité (critères dans les extensions), exemples.

C) Corps de décomposition

Définition, théorème d'existence et d'unicité, exemples.
DEV 1 : GALOIS INVERSE. Exemples.

IV) Polynômes irréductibles sur les corps finis

$q = p^n$, p premier, $n \in \mathbb{N}^*$.

A) L'ensemble des polynômes irréductibles sur $\mathbb{F}_p$

Définitions de $\mathcal{P}_p(i)$ et $I_p(i)$. **DEV 2 : POLYNÔMES IRREDUCTIBLES SUR $\mathbb{F}_p$. Exemples.**

B) Factorisation de polynômes

Théorème de BERLEKAMP, applications.

V) Polynômes cyclotomiques

Sous-groupes de l'unité, définition du n -ième polynôme cyclotomique $\Phi_{n,k}$, exemples. Degré de $\Phi_{n,k}$, relations avec $X^n - 1$, irréductibilité de $\Phi_{n,k} \in \mathbb{Z}[X]$, application au degré de l'extension de $\mathbb{Q} \subset \mathbb{Q}(\xi)$.

ANNEXE : Algorithme de BERLEKAMP.

Références :

- PERRIN
- TAUVEL
- BECK-MALICK-PEYRÉ

142 : PGCD et PPCM, algorithmes de calcul. Applications.

Cadre : $(A, +, \cdot)$ un anneau unitaire commutatif intègre, $\mathbb{K}$ un corps.

I) **Propriétés arithmétiques**

Définitions de la divisibilité, d'éléments associés, d'irréductibles. PGCD et PPCM de deux éléments. Exemples. Cas d'un anneau factoriel.

II) **Cas d'un anneau principal**

Définition d'un anneau principal, exemples et contre-exemple. Théorème de BACHET-BEZOUT. Cas où $d = \text{pgcd}(a, b)$. Exemples

III) **Cas d'un anneau euclidien**

Définition d'un anneau euclidien, stathme, exemple de $\mathbb{K}[X]$. Implication successives des différents anneaux usuels. Algorithme d'EUCLIDE. Exemples. Algorithme d'EUCLIDE étendu : obtention d'une relation de BEZOUT, exemples.

IV) **Application en arithmétique**

A) Équations diophantiennes linéaires

Définition, résolution de $ax = b$. Cas de $b = 1$ et $\text{pgcd}(a, b) = 1$, puis de b quelconque. Théorème résumant l'ensemble des solutions dans le cas général. Exemple. Généralisation à n variables. Résolution de $AX = B$ lorsque A est diagonale. **DEV 1** : FORME NORMALE DE SMITH.

B) Système de congruences

Théorème chinois, exemple et contre-exemple. Isomor-

phisme réciproque. Application. Cas général. **DEV 2** : SYSTÈME DE CONGRUENCES.

Références :

- [PERRIN](#)
- [ROMBALDI](#)
- [BECK-MALICK-PEYRÉ](#)

144 : Racines d'un polynôme.
Fonctions symétriques élémentaires.
Exemples et applications.

Cadre : $\mathbb{K}$ est un corps commutatif, $P \in \mathbb{K}[X]$

I) Racines d'un polynôme

Définition d'une racine, caractérisation. Multiplicité d'une racine. Application. Morphisme d'algèbres (fonctions polynomiale. Cas des corps finis. Polynôme dérivé. Polynôme scindé. Lien entre les racines et les polynômes symétriques élémentaires. Applications.

II) Polynômes symétriques élémentaires

Définition d'un polynôme à n indéterminée symétrique. Exemple. Polynôme symétrique élémentaire, exemples. Théorème fondamental des polynômes symétriques. Exemples. Identités de NEWTON. DEV 1 : FORMES DE HANKEL.

III) Extension de corps

A) Extension algébrique

Définition d'une extension de corps, exemples, théorème de la base télescopique, morphisme évaluation en élément du surcops, élément algébrique et transcendant. Caractérisation des éléments algébriques. Sous-corps des éléments algébriques sur $\mathbb{K}$.

B) Adjonction de racines

Corps de rupture, exemple et théorème d'existence. Corps de décomposition, exemple et théorème d'existence. DEV 2 : GALOIS INVERSE.

IV) Applications

A) Localisation des valeurs propres

Théorème de GERSCHGÖRIN-HADAMARD. Matrice à diagonale strictement dominante. Continuité des valeurs propres, déterminant circulant.

B) Réduction des endomorphismes

Polynôme caractéristique, critère de diagonalisabilité / trigonalisabilité, caractérisation des endomorphismes semi-simple.

Références :

- ROMBALDI
- GOURDON
- PERRIN

148 : Décomposition de matrices.

Exemples et applications.

Cadre : $M \in \mathcal{M}_n(\mathbb{K})$ $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, χ_M son polynôme caractéristique, π_M son polynôme minimal.

I) Invariants de similitude

L'espace $E_{M,x}$, invariants de similitude, réduction de FROBENIUS. Exemples et applications.

II) Décomposition de DUNFORD

A) Résultats généraux

Théorème de CAYLEY-HAMILTON, lemme des noyaux, application et exemple. **DEV 1** : DÉCOMPOSITION DE DUNFORD. Exemple.

B) Cas particulier

Matrice semi-simple. Cas où $\mathbb{K} = \mathbb{C}$. Exemple. Caractérisation des matrices semi-simples. Exemple. DUNFORD généralisé.

C) Application à l'exponentielle matricielle

Définition de l'exponentielle matricielle, continuité. Application de la décomposition de DUNFORD à l'exponentielle, exemple. Décomposition de DUNFORD de e^M . **DEV 1 (BIS)** : CARACTÉRISATION D'UNE MATRICE DIAGONALISABLE.

III) Réduction de JORDAN

A) Résultats généraux

Bloc de JORDAN. **DEV 2** : RÉDUCTION DE JORDAN. Exemple.

B) Lien avec la décomposition de DUNFORD

Matrice de passage de la réduction de JORDAN. $JORDAN \longrightarrow DUNFORD$. Exemple.

C) Application à la résolution d'équations différentielles

Définition de $\mathcal{L}_H$. Structure de ses solutions. La matrice fondamentale e^{tA} . Cas diagonalisable. Exemples.

ANNEXES : Tableau comparatif des différentes décompositions proposées (hypothèse de χ_M scindé, calcul exponentiel, détermination du polynôme caractéristique, du polynôme minimal)

Références :

- GOURDON
- ROMBALDI
- BERTHELIN

149 : Valeurs propres, vecteurs propres.
Calculs exacts ou approchés d'éléments propres
Applications.

Cadre : K un corps, E un K -espace vectoriel de dimension n .

I) Généralités

- A) Valeur propre, vecteur propre, espace propre
Définitions , exemples. Liens avec les matrices, exemples de spectre. **DEV 1 : SUITE DE POLYGONES.**
- B) Polynôme caractéristique, polynôme minimal
Définition, propriétés, exemples. Indépendance de la base. Caractérisation des valeurs propres. Définition du polynôme minimal, caractérisation des valeurs propres. Exemples. Application à la réduction d'endomorphismes. **DEV 2 : DÉCOMPOSITION DE DUNFORD.**

II) Norme matricielle, rayon spectral

- A) Définitions, propriétés
Norme induite, exemples classiques. Définition du rayon spectral, exemple. Cas particulier de la norme induite à la norme euclidienne, exemple.
- B) Théorèmes de HOUSEHOLDER et de GELFAND
Théorèmes d'HOUSEHOLDER et de GELFAND. Application à la série de terme général d'une matrice, contre-exemple pour une norme non-induite.

III) Matrice positive

- A) Définitions, propriétés
Définition, propriétés , exemples.

- B) Le théorème de PERRON-FROBENIUS
Théorème de PERRON-FROBENIUS. Exemple. Théorème de GERSCHÖRIN-HADAMARD, application et exemple.

IV) Calcul approché de valeurs propres

- A) Méthode de la puissance
Objectif, théorème, application à une matrice strictement positive, contre-exemple.
- B) Méthode QR
Objectif, décomposition QR , construction de la méthode, théorèmes de convergence.

Références :

- GOURDON
- ROMBALDI
- SERRE

151 : Dimension d'un espace vectoriel. Rang. Exemples et applications.

Cadre : $\mathbb{K}$ un corps, E un $\mathbb{K}$ -espace vectoriel.

I) Généralités sur la dimension finie

- A) Base d'un espace vectoriel
Définitions d'une famille génératrice, libre, d'une base. Exemples. Théorème d'existence d'une base, d'extraction et de la base incomplète.
- B) Théorèmes fondamentaux sur la dimension
Définition de la dimension de E , corollaires. Dimension d'un sous-espace vectoriel.
- C) Somme directe, sous-espaces supplémentaires
Définition, caractérisation, dimension d'une somme directe, exemples.

II) Application linéaire, dualité

Définition d'une application linéaire de E dans F , noyau et image, rang d'une application, théorème du rang. Définition de l'espace dual, isomorphisme de E^* et E , base duale, exemples. Annulateur d'un sous-espace.

III) Application aux extensions de corps

Définition d'une extension de corps. Théorème de la base télescopique. Éléments algébrique et transcendant. Caractérisation des éléments algébriques. Exemples.

IV) Application à la réduction d'endomorphismes

- A) Polynôme annulateur
Existence d'un polynôme annulateur, théorème de CAYLEY-

HAMILTON, lemme des noyaux, caractérisation des endomorphismes trigonalisables, diagonalisables **DEV 1** : RÉDUCTION DE JORDAN. Semi-simplicité, caractérisation des endomorphismes semi-simples.

- B) Dans un espace vectoriel euclidien
Procédé de GRAM-SCHMIDT. Définition d'un endomorphisme normal, exemples. **DEV 2** : RÉDUCTION DES ENDOMORPHISMES NORMAUX. Applications.

Références :

- GRIFFONE
- PERRIN
- ROMBALDI

152 : Déterminants. Exemples et applications.

Cadre : $\mathbb{K}$ un corps, E un $\mathbb{K}$ -espace vectoriel de dimension $n \in \mathbb{N}^*$.

I) Généralités

A) Définitions, propriétés

Définition d'une forme multilinéaire alternée sur E^p , caractérisation. L'espace vectoriel $\mathcal{A}_n(E, \mathbb{K})$. Déterminant d'un n -uplet relativement à une base. Relation de CHASLES. Caractérisation des familles liées / libres de E . Déterminant d'un endomorphisme de E . Propriétés classiques du déterminant.

B) Méthodes de calcul d'un déterminant

Propriétés classiques sur le déterminant d'une matrice. Matrice triangulaire, développements selon une ligne et une colonne. Formule de la comatrice.

C) Interprétation géométrique

Lien entre le déterminant de deux vecteurs dans $\mathbb{R}^2$ et l'aire du parallélogramme engendré par ces deux derniers. Généralisation au volume dans $\mathbb{R}^n$.

II) Déterminants classiques

A) Déterminant de VANDERMONDE

Déterminant de Vandermonde, calcul de ce dernier. Applications.

B) Déterminant de GRAM

Définition d'une matrice de GRAM, de son déterminant. Distance à un sous-espace vectoriel de dimension finie, exemple.

C) Déterminant circulant

Matrice circulante. DEV 1 : SUITE DE POLYGONES. Application au calcul de déterminant.

III) Applications

A) Valeurs propres d'un endomorphisme

Valeur propre, caractérisation via le polynôme caractéristique (prendre le soin d'étendre le déterminant à l'anneau $\mathbb{K}[X]$ qui n'est pas un corps). DEV 2 : ÉTUDE DE $GL_n(\mathbb{C})$. Application.

B) Changement de variables

Déterminant jacobien. Théorème de changement de variable. Exemples. Théorème d'inversion local, application.

C) Forme quadratique

Formes quadratiques équivalentes. Discriminant. Étude sur $\mathbb{C}$, $\mathbb{R}$ ou $\mathbb{Q}$. Cas des corps finis. Exemples.

ANNEXES : Distance à un sous espace de dimension finie. Suite de polygones. Inversion locale.

Références :

- ROMBALDI
- GRIFFONE
- GOURDON
- GARET-KURTZMANN
- ROUVIÈRE

153 : Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie.

Applications.

Cadre : $\mathbb{K}$ un corps, E un $\mathbb{K}$ -espace vectoriel de dimension $n \in \mathbb{N}^*$.

I) L'algèbre $K[u]$

A) Définitions, propriétés

Définition de $P(u)$. L'algèbre $\mathbb{K}[u]$, définition analogue pour une matrice. Spectre de $P(u)$ en fonction de u dans le cas algébriquement clos, contre-exemple.

B) Polynôme caractéristique

Morphisme d'algèbres $\mathbb{K}[X] \longrightarrow \mathbb{K}[u]$, existence d'un polynôme minimal. Dimension de $\mathbb{K}[u]$, caractérisation du corps $\mathbb{K}[u]$, exemple d'un projecteur. Théorème de CAYLEY-HAMILTON, applications.

C) Sous-espaces stables

Stabilité des noyaux et images de deux endomorphismes commutant, application. Lemme des noyaux, application et exemple.

II) Application à la réduction

A) Décomposition de DUNFORD

DEV 1 : DÉCOMPOSITION DE DUNFORD. Exemple et contre-exemple.

B) Semi-simplicité

Définition, exemple, cas de $\mathbb{K}$ algébriquement clos. **DEV 2 :**

ENDOMORPHISME SEMI-SIMPLE. Application à DUNFORD généralisé.

C) Endomorphisme normal

E euclidien.

Définition, exemples. Cas matriciel, réduction des endomorphismes normaux. Applications.

III) Application au calcul matriciel

A) Calculs d'inverses et de puissances

Polynôme annulateur de coefficient constant non nul, application à l'inversibilité et le spectre d'un tel endomorphisme. Calcul de puissance d'un endomorphisme.

B) Exponentielle matricielle

Définition, propriété polynomiale de $e^u, u \in \mathcal{L}(E)$. Décomposition de DUNFORD de e^u , application à la diagonalisabilité de u . Équation différentielle homogène, polynôme caractéristique et résolution d'une telle équation. Exemple.

C) Géométrie

Déterminant circulant. Application à la suite de polygones.

ANNEXES : Polynômes minimal et caractéristique d'une symétrie, projection sur un sous-espace F , d'un nilpotent, d'une homothétie. Exemples de polygones.

Références :

- ROMBALDI
- BERTHELIN

154 : Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.

Cadre : E est un K -espace vectoriel de dimension n .

I) Généralités

- A) Définitions, premières propriétés
Définition d'un sous-espace stable, endomorphisme induit. Matrice triangulaire par blocs. Lien avec le polynôme caractéristique.
- B) Sous-espaces cycliques
Définitions d'un sous-espace cyclique, d'une matrice compagnon, lien avec les endomorphismes cycliques. Théorème de CAYLEY-HAMILTON. Réduction de FROBENIUS. Applications.
- C) Dualité
Définition du dual, bidual, propriétés, caractérisation des sous-espaces stables via la dualité.

II) Application à la réduction

- A) Diagonalisation, trigonalisation
Lemme des noyaux, application à la caractérisation des endomorphismes diagonalisables et trigonalisables. Codiagonalisabilité/trigonalisabilité. Cas des corps finis : Cardinal de $\mathcal{D}_n(\mathbb{F}_q)$.
- B) Réductions de Dunford et Jordan
Décomposition de DUNFORD, application à l'exponentielle.

Définition d'un endomorphisme semi-simple, exemple. Caractérisation dans un corps algébriquement clos **DEV 1** : CARACTÉRISATION DES ENDOMORPHISMES SEMI-SIMPLES. Application. Réduction de Jordan. Exemple.

- C) Endomorphismes normaux
Définition, exemples. **DEV 2** : RÉDUCTION DES ENDOMORPHISMES NORMAUX. Applications.

III) Application aux représentations des groupes finis

- A) Définitions et propriétés
Représentation, exemples. Morphismes de représentation.
- B) Décomposition en somme directe
Théorème de MASCHKE. Lemme de SCHUR.

Références :

- BECK-MALICK-PEYRÉ
- GOURDON
- ROMBALDI

155 : Endomorphismes diagonalisables en dimension finie.

Cadre : E est un $\mathbb{K}$ -espace vectoriel de dimension n .

I) Généralités

- A) Définitions, premières propriétés
Définition d'un endomorphisme diagonalisable, d'une matrice diagonalisable. Exemple. Polynôme caractéristique d'un endomorphisme, lien avec ses valeurs propres, exemple. Dimension d'un espace propre.
- B) Caractérisation
 $(\chi_f \text{ scindé à racines simples sur } \mathbb{K}) \Rightarrow (f \text{ diagonalisable})$. Caractérisation, exemple. Codiagonalisation, diagonalisation de la somme. Polynôme minimal, théorème de CAYLEY-HAMILTON, lemme des noyaux et application à la caractérisation de la diagonalisabilité, exemple. Stabilité par restriction à un sev stable.
- C) Cas des corps finis
DEV 1 : CARDINAL DE $\mathcal{D}_n(\mathbb{F}_q)$. Équivalent.

II) Décomposition de matrices

- A) Décomposition de DUNFORD
Décomposition de DUNFORD, exemple. Application à l'exponentielle. DEV 2 : MORPHISMES CONTINUS DE $\mathcal{S}^1$ VERS $GL_n(\mathbb{R})$.
- B) Semi-simplicité
Définition, exemple. Caractérisation, cas d'un corps algébriquement clos. DUNFORD généralisé.

III) Cas d'un espace euclidien

Endomorphisme normal, exemples. Matrice normale. Théorème de réduction des endomorphismes normaux. Application au théorème spectral, calcul de $\rho(A)$ pour $A \in \mathcal{S}_n(\mathbb{R})$.

IV) Applications

- A) En géométrie
Matrice circulante, suite de polygones.
- B) Facteurs invariants
Forme normale se SMITH, applications.
- C) Résolution d'équations différentielles
Définition de $(\mathcal{L}_H)$, existence d'une solution globale. Le sous-espace vectoriel $(\mathcal{S}_H)$. Résolution dans le cas d'une matrice diagonalisable, exemples.

ANNEXES : Tableau récapitulatif de diagonalisabilité selon les racines des polynômes, exemple d'un polygone, schéma des solutions de $\mathcal{L}_H$ dans le cas diagonalisable.

Références :

- GOURDON
- ROMBALDI
- BECK-MALICK-PEYRÉ
- BERTHELIN

156 : Exponentielle de matrices.

Applications.

Cadre : $\mathbb{K}$ un corps ($\mathbb{R}$ ou $\mathbb{C}$), $||| \cdot |||$ une norme d'algèbre sur $\mathcal{M}_n(\mathcal{K})$

I) Généralités

Définition, exemple d'une matrice diagonale, continuité, cas de matrices semblables. L'application $t \mapsto e^{tA}$, inversibilité.

II) Méthodes de calcul de l'exponentielle matricielle

Décomposition des noyaux, théorème de CAYLEY-HAMILTON, application. DEV 1 : DUNFORD + APPLICATION. Exemple.

III) Injectivité et surjectivité

Matrices nilpotentes et unipotentes, logarithme matriciel, bijection. $exp : \mathcal{M}_n(\mathbb{C}) \longrightarrow GL_n(\mathbb{C})$ est surjective non injective, exemple. Connexité par arcs de $GL_n(\mathbb{C})$, composantes connexes de $GL_n(\mathbb{R})$. Restrictions de l'exponentielle à $\mathcal{S}_n(\mathbb{R})$, applications.

IV) Propriétés topologiques

L'espace vectoriel $\mathbb{K}[A]$, différentiabilité de l'exponentielle. Morphisme continue de $(\mathbb{S}, \times)$ dans $GL_n(\mathbb{C})$. DEV 2 : MORPHISME CONTINU DE $(\mathbb{S}, \times)$ DANS $GL_n(\mathbb{R})$.

V) Applications aux équations différentielles

Définition de $(\mathcal{L}_H)$, exemple, matrice fondamentale, forme de ses solutions dans le cas constant.. Applications et exmples.

ANNEXES : Solutions des équations différentielles selon la nature des valeurs propres.

Références :

- ROMBALDI
- GOURDON
- CALDEROI
- BERTHELIN

157 : Endomorphismes trigonalisables, endomorphismes nilpotents

Cadre : $\mathbb{K}$ un corps ($\mathbb{R}$ ou $\mathbb{C}$), E un $\mathbb{K}$ espace vectoriel de dimension finie.

I) Trigonalisation

A) Définitions, caractérisation

Définition, caractérisation des endomorphismes diagonalisables, exemple et contre-exemple. Endomorphisme induit. Spectre d'un endomorphisme.

B) Dualité, trigonalisation simultanée

Définition, propriétés, caractérisation des sous-espaces stables via la dualité. Stabilité des sous-espaces pour deux endomorphismes qui commutent. Application à la cotrigonalisation. Exemple.

II) Endomorphismes nilpotents

A) Le cône $\mathcal{N}$

Définition de $\mathcal{N}$, exemples. Nature de $\mathcal{N}$. Cas de la dimension 2. Commutativité des éléments nilpotents. L'espace $Vect(\mathcal{N})$.

B) Caractérisation des endomorphismes nilpotents

Indice de nilpotence, caractérisation des endomorphismes nilpotents

C) Application à la réduction d'endomorphismes

Lemme des noyaux. DEV 1 : DÉCOMPOSITION DE DUNFORD. Endomorphisme semi-simple, DUNFORD généralisé.

III) Sous-espaces cycliques

Endomorphisme cyclique. Matrice compagnon. Invariants de similitude, réduction de FROBENIUS. Applications.

IV) Vers la réduction de JORDAN

Matrice de JORDAN. DEV 2 : RÉDUCTION DE JORDAN. Exemples et applications.

ANNEXES : Cône $\mathcal{N}$, matrice de JORDAN.

Références :

- GOURDON
- BECK-MALICK-PEYRÉ
- ROMBALDI

158 : Matrices symétriques réelles, matrices hermitiennes.

I) Généralités

A) Définitions, propriétés

Définitions, matrice positive, valeurs propres d'une telle matrice.

B) Endomorphisme adjoint

Endomorphisme adjoint, matrice relativement à une base orthonormée, exemple. Propriétés de l'adjoint. Endomorphisme symétrique, exemples.

II) Réduction

A) Théorème spectral

Théorème spectral, caractérisation des produits scalaires via les formes hermitiennes.

B) Endomorphisme normal

Définition, matrice normale, exemples. **DEV 1** : RÉDUCTION DES ENDOMORPHISMES NORMAUX. Applications.

C) Classification des formes hermitiennes

Forme hermitienne non dégénérée, exemple. Orthogonalité relativement à une forme hermitienne. Base orthogonale, théorème d'existence. Théorème de SYLVESTER. Signature. Réduction simultanée.

III) Topologie de $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{H}_n(\mathbb{C})$

Propriétés de $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{H}_n(\mathbb{C})$, décomposition polaire, application. Exponentielle d'une matrice, exemple. Homéomorphismes, applications.

IV) Applications

A) Calcul différentiel

Matrice hessienne, extremum local, condition suffisance d'existence. Cas $n = 2$. **DEV 2** : LEMME DE MORSE. Application.

B) Décomposition matricielle

Factorisation LU , décomposition de CHOLESKY. Exemples.

Références :

- GRIFFONE
- ROMBALDI
- ALLAIRE-KABER

159 : Formes linéaires et dualité en dimension finie. Exemples et applications.

Cadre : $\mathbb{K}$ un corps, E un $\mathbb{K}$ -espace vectoriel de dimension $n \in \mathbb{N}^*$.

I) Généralités

A) Définitions, propriétés

Définition, exemple de la différentielle. L'espace vectoriel E^* . Isomorphisme entre E et E^* . Exemple de $M_n(\mathbb{K}) \simeq (M_n(\mathbb{K}))^*$.

B) Espaces dual et bidual

Base duale, exemple. Espace bidual. Isomorphisme entre E et E^{**} . Existence d'une base antéduale, exemple.

II) Orthogonalité

A) Définition, propriétés

Définition et propriétés de l'orthogonal. Propriétés sur les dimensions, équations d'une sous-espace vectoriel.

B) Application transposée

Application transposée, propriétés. Caractérisation de la stabilité d'un e.v. via le dual. Application. Changement de base dans le dual

C) Cas d'un espace euclidien

$(E, \langle \cdot, \cdot \rangle)$ est un espace euclidien.
Orthogonalité via le produit scalaire. Théorème de RIESZ-FRÉCHET. Orthogonalité via le produit scalaire. Lien entre les sous-espace orthogonaux pour le produit scalaire / dualité. Existence et unicité d'un endomorphisme adjoint.

III) Applications aux formes quadratiques

A) Définitions, propriétés

Définition, base orthogonale. Théorème d'existence, exemple.

B) Classification et application

Théorème de SYLVESTER. Application. DEV 2 : FORMES DE HANKEL. Application.

IV) Application à la réduction d'endomorphismes

Matrice de JORDAN, espace stable par un endomorphisme. DEV 1 : RÉDUCTION DE JORDAN. Application à la résolution d'EDLH. Famille libre d'applications.

ANNEXES : Références :

- GOURDON
- GRIFONE
- ROMBALDI

160 : Endomorphismes remarquables d'un espace vectoriel euclidien.

Cadre : $(E, \langle . \rangle)$ un espace euclidien, $\|.\|$ la norme induite par $\langle . \rangle$.

I) Généralités

- A) Résultats essentiels
Définition d'un orthogonal, propriétés , exemples. Dual de E . Base orthonormale. Existence d'une b.o.n.. Orthogonalisation de GRAM-SCHMIDT. Exemple. inégalité de CAUCHY-SCHWARZ, cas d'égalité.
- B) Adjoint d'un endomorphisme
Existence d'un adjoint. Matrice relativement à une b.o.n.. Exemple. Propriétés de l'adjoint.

II) Exemples d'endomorphismes remarquables

- A) Endomorphismes auto-adjoint et antiauto-adjoint
Définition, exemple. Théorème spectral. Application au matrice. Caractérisation d'un produit scalaire. Spectre d'un endomorphisme auto-adjoint.
- B) Endomorphismes orthogonaux
Définition, exemple. Groupe $O(E)$. caractérisations des endomorphismes orthogonaux. Valeurs propres. Groupe $SO(E)$. Réduction des endomorphismes orthogonaux. Application. Renversement et retournement orthogonaux.
DEV 1 : ENGENDREMENT DE $SO(E)$ + APPLICATION.
- C) Endomorphismes normaux
Définition, exemples, matrice relativement à une b.o.n..
DEV 2 : RÉDUCTION DES ENDOMORPHISMES NORMAUX.

III) Applications

- A) Calculs de distances
Existence d'un projecteur orthogonal. Application projection. Exemple. Matrice de GRAM, application à la calcul de distance, exemple.
- B) Méthode des moindres carrés
Définition du problème, théorème d'existence. Applications et exemples.

Références :

- GRIFFONE
- CALDERO
- ROMBALDI
- ALLAIRE-KABER

161 : Distance dans un espace affine euclidien. Isométries.

Cadre : $(E, \mathcal{E})$ un espace affine.

I) Généralités

A) Définitions, propriétés

Définitions d'un espace affine euclidien, distance entre deux points de $\mathcal{E}$. Distance à un sous-espace affine, projeté orthogonal.

B) Matrice et déterminant de GRAM

Matrice et déterminant de GRAM, caractérisation de son inversibilité. Distance à un sous-espace vectoriel. Exemple. Application à l'inégalité d'HADAMARD. Expression du projeté orthogonal sur un sous-espace vectoriel de dimension finie à l'aide de la matrice de GRAM.

II) Isométries d'un espace affine euclidien

A) Forme canonique

Théorème de forme canonique des isométries affines.

B) Isométries affines conservant une partie

Définition d'une isométrie fixant une partie, déplacement et anti-déplacements fixant une partie. Exemple du cube. Théorème liant $Is(\mathcal{P})$ et $\mathfrak{S}(\mathcal{P})$. Exemple du groupe diédral.

III) Structure des isométries

A) Le groupe orthogonal

Définitions de réflexion et retournement orthogonal. Théorème de CARTAN-DIEUDONNÉ. DEV 1 : $SO_n(\mathbb{R})$ ENGENDRÉ PAR LES RENVERSEMENTS + $SO_3(\mathbb{R})$ EST SIMPLE.

Théorème de classifications de $O_2(\mathbb{R})$ et $O_3(\mathbb{R})$, conséquence et exemple. Définition d'un endomorphisme normal, exemples des endomorphismes orthogonaux et des similitudes. DEV 2 : RÉDUCTION DES ENDOMORPHISMES NORMAUX. Application à la réduction des endomorphismes orthogonaux, cas général.

B) Isométries du plan

Décomposition d'une isométrie en produit de réflexions. Application à la classification des isométries du plan affine euclidien.

ANNEXES : Représentations d'une translation, d'une symétrie glissée etc.. Illustrations d'une rotation et symétrie orthogonale dans $\mathbb{R}^2$, puis de $O(\mathbb{R}^3)$. Projection orthogonale sur un sous-espace vectoriel. Tableau récapitulatif des isométries du plan affine euclidien.

Références :

- ROMBALDI
- AUDIN
- CALDERO
- GRIFONE

162 : Systèmes d'équations linéaires, opérations élémentaires, aspects algorithmiques et conséquences théoriques.

Cadre : $\mathbb{K}$ un corps commutatif de caractéristique nulle.

I) Généralités

A) Définitions

Définition d'un système, système compatible, exemples.
Rang d'un système linéaire.

B) Système de CRAMER et cas général

Définition, solution d'un tel système. Déterminant principal, inconnue principale. Théorème de ROUCHÉ-FONTENÉ.
Exemples.

II) Réduction de GAUSS

A) Définition

Matrices élémentaires. Définitions d'un pivot, d'une matrice échelonnée, exemple. Action de groupe sur $\mathcal{M}_{m,n}(\mathbb{K})$. Complexité algorithmique en $\mathcal{O}(n^3)$. Exemple.

B) Applications en algèbre linéaire

Invariance d'un ensemble engendrant un espace vectoriel.
Applications.

III) Formes normales d'HERMITE et de SMITH

Forme d'HERMITE. Application. DEV 1 : FORME NORMALE DE SMITH.

IV) Méthodes de résolution

A) Décomposition LU

Théorème et application, complexité, exemple.

B) Factorisation de CHOLESKY Théorème et application, complexité, exemple.

C) Méthode de gradient

DEV 2 : GRADIENT À PAS OPTIMAL.

Références :

- GOURDON
- CALDERO
- GRIFFONE
- BECK-MALICK-PEYRÉ
- ALLAIRE-KABER

170 : Formes quadratiques sur un espace vectoriel de dimension finie.
Orthogonalité, Isotropie. Applications.

Cadre : K un corps de caractéristique $\neq 2$, E un K -espace vectoriel.

I) Généralités

A) Définitions

Définitions : forme bilinéaire symétrique, exemple, l'ensemble $\mathcal{B}(E \times E, K)$. Forme quadratique, forme polaire associée.

B) Représentation matricielle

Définition, exemple, matrice de passage. Classe congruence dans $S_n(K)$.

C) Représentation polynomiale

Polynôme homogène, polynôme représentant dans une base. Exemples.

II) Orthogonalité, isotropie

q une forme quadratique sur E de forme polaire ϕ .

A) Cône isotrope, noyau de ϕ

Définition, vecteur isotrope, exemple. Noyau de q . définie $\Rightarrow$ non dégénérée. Réciproque fausse. Base q -orthogonale, théorème d'existence. Théorème spectral. Orthogonalité selon q . Exemples. Propriétés.

B) Algorithme de GAUSS

Expression en somme de formes linéaires au carré, algorithme de GAUSS, exemples.

III) Classification des formes quadratiques

Définition de rang, exemples. Formes quadratiques équivalentes. Équivalence $\Rightarrow$ même rang. Réciproque fausse. Équivalence sur un corps algébriquement clos, théorème de SYLVESTER, puis sur $\mathbb{F}_q$. Exemples.

IV) Applications

A) Nombres de racines d'un polynôme réel

Mise en contexte. DEV 1 : FORME DE HANKEL.

B) Carrés de $\mathbb{F}_q$.

Définition d'un carré, exemple, caractérisation d'un carré. Application à -1 et aux nombres premiers. Symbole de LEGENDRE, exemple. DEV 2 : LOI DE RÉCIPROCITÉ QUADRATIQUE.

Références :

- SEGUINS-PAZZIS
- GOURDON
- GRIFONE
- CALDERO
- PERRIN

171 : Formes quadratiques réelles. Coniques.
Exemples et applications.

Cadre : E un $\mathbb{R}$ -espace vectoriel.

I) Généralités

A) Définitions

Définitions : forme bilinéaire symétrique, exemple, l'ensemble $\mathcal{B}(E \times E, K)$. Forme quadratique, forme polaire associée.

B) Représentation matricielle

Définition, exemple, matrice de passage. Classe congruence dans $S_n(K)$.

II) Orthogonalité, isotropie

A) Cône isotrope, noyau de ϕ

Définition, exemple. Vecteurs orthogonaux, exemples. Propriétés de l'orthogonalité. Noyau de q . Exemple. Base q -orthogonale. Théorème d'existence d'une base q -orthogonale.

B) Algorithme de GAUSS

Mise sous somme de formes linéaires au carré. Théorème de GAUSS. Exemples. Range de q . Lien avec les matrices. Définitions de f.q. équivalentes. Théorème de SYLVESTER. Applications.

III) Applications

A) Racines d'un polynôme réel

Mise en contexte. DEV 1 : FORME DE HANKEL.

B) Différentielle seconde.

Théorème de SCHWARZ, matrice hessienne et formule de TAYLOR à l'ordre 2. DEV 2 : LEMME DE MORSE. Application.

C) Coniques

Définitions, exemple. Quadrique affine, forme quadratique homogénéisée. Intersection d'une quadrique et d'une droite. Classification euclidienne des coniques affines.

ANNEXE : Lemme de MORSE, conique.

Références :

- SEGUINS-PAZZIS
- GOURDON
- GRIFONE
- CALDERO

181 : Barycentres dans un espace affine réel de dimension finie, convexité. Applications.

Cadre : $(\mathcal{E}, E)$ un $\mathbb{R}$ -espace affine de dimension finie.

I) Barycentres

A) Définitions, propriétés

Définition d'un barycentre, isobarycentre, exemples. Associativité. DEV 1 : SUITE DE POLYGONES.

B) Sous-espace affine

Sous-espace affine, exemple du parallélogramme de $\mathcal{E}$. Caractérisation d'une application affine par les barycentres. Application à l'image d'un segment par une application affine.

C) Coordonnées barycentriques

Repère affine, coordonnées cartésiennes / coordonnées barycentriques, exemples.

II) Convexité

A) Ensemble et fonction convexes

Définitions, exemple, caractérisation avec l'épigraphe d'une fonction. Combinaison convexe, propriétés par somme de convexes.

B) Enveloppe convexe

Définition, propriétés, théorème de LUCAS. Théorème de CARATHÉODORY. Applications. Stabilité des convexes par les applications affines.

C) Résultats de séparation

Soit E un e.v.n..

Hyperplan affine, caractère fermé d'un hyperplan. Séparation de parties au sens large / strict. Jauge d'un convexe.

DEV 2 : THÉORÈME DE HAHN-BANACH (GÉOMÉTRIQUE).

III) Applications aux points extrémaux

Définition de point extrémal. Théorème de KREIN-MILMAN. Théorème de HELLY. Applications.

ANNEXES : Exemples d'une droite, d'un segment, d'un triangle. Ensembles convexe et non convexe, enveloppe convexe. Illustration d'hyperplans d'appui et de séparation.

Références :

- AUDIN
- TAUVEL
- BECK-MALICK-PEYRÉ
- BREZIS

190 : Méthodes combinatoires, problèmes de dénombrement

Cadre : A et D deux ensembles.

I) Généralités

A) Principes de base du dénombrement

Principes d'indépendance, de partition, lemme des bergers, exemples.

B) Résultats classiques

Nombres d'applications, de permutations et d'injections de D dans A . Coefficient binomial, formule du crible.

II) En analyse :

A) Probabilités sur un ensemble fini

Probabilité uniforme sur un ensemble fini, exemple.

B) Les séries pour dénombrer

Définitions des nombres de CATALAN et de BELL, nombre de CATALAN, formule du nombre de BELL.

III) En algèbre :

A) Utilisations du groupe symétrique

Définitions d'une permutation et d'un dérangement, nombre de r -cycles, applications au nombre de dérangements, au nombre de permutations ayant un certain nombre de points fixes.

B) Actions de groupe

Définition, caractérisation via un morphisme de groupes, orbites, transitivité, fidélité, stabilisateur, exemples. Équation

aux classes. Formule de BURNSIDE. Application (classes de conjugaison de $\mathcal{S}_n$). **DEV 1** : CARDINAL DE $\mathcal{D}_n(\mathbb{F}_q)$.

C) Sur les corps finis

Dénombrement des cardinaux de $GL_n(\mathbb{F}_q)$ de $SL_n(\mathbb{F}_q)$, isomorphismes exceptionnels. Fonction d'EULER. Application à la cyclicité de $(\mathbb{F}_q^*, \times)$ **DEV 2** : POLYNÔMES IRRÉDUCTIBLES SUR $\mathbb{F}_q$.

Références :

- GARET-KURTZMANN
- OUVARD - TOME 1
- FGA - TOME 1
- ROMBALDI
- PERRIN

191 : Exemples d'utilisation de techniques d'algèbre en géométrie

Cadre : E un $\mathbb{K}$ espace vectoriel, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I) Géométrie affine

A) Définitions

Définitions d'un espace affine, de sa direction, d'un sous-espace affine, exemples.

B) Barycentres

Système pondéré, définition d'un barycentre, isobarycentre, exemples. Plan d'ARGAND-CAUCHY. **DEV 1** : SUITE DE POLYGONES.

C) Applications affines

Définition, groupe $GA(\mathcal{E})$. Espace euclidien, isométrie affine. Déplacements de $\mathcal{E}$.

II) Géométrie euclidienne

A) $O_2(\mathbb{R})$ et $O_3(\mathbb{R})$

Caractérisation des matrices de $SO_2(\mathbb{R})$ et de $O_2(\mathbb{R}) \setminus SO_2(\mathbb{R})$; Représentation géométrique. Caractérisation des matrices de $O_3(\mathbb{R})$ et de $SO_3(\mathbb{R})$. Connexité par arcs de $SO_3(\mathbb{R})$. **DEV 2** : SIMPLICITÉ DE $SO_3(\mathbb{R})$.

B) Projection orthogonale

Existence d'un projecteur orthogonal sur un sous-espace vectoriel. Exemple. L'application projection. Matrice de GRAM, application aux calculs de distances.

III) Angle, produit vectoriel

A) Angle

Définition d'un angle (non orienté), existence d'un angle dans un espace orienté. Exemple. Propriétés de la rotation. Cas de la dimension 3.

B) Produit vectoriel

Définition d'un produit vectoriel, propriétés, caractère bilinéaire et alternée du produit vectoriel. Identité de LA-GRANGE.

ANNEXES : Angle orienté, rotation dans $\mathbb{R}^2$ et $\mathbb{R}^3$

Références :

- AUDIN
- ROMBALDI
- GRIFFONE