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

0.1 Etude d'une action de groupes.

1. Action d'un groupe sur un ensemble.
 - [THG] def : action de groupe - action fidèle, prop : def équivalente d'une action de groupe, def : invariant sous l'action de G , exemples d'actions naturelles : des sous-groupes du groupe symétrique - sur l'ev K^n - sur l'espace vectoriel euclidien $\mathbb{R}^n$, ex : S_n agit sur $K[X_1, \dots, X_n]$.
 - [ULM] ex : action d'un groupe triviale - par translation - par conjugaison, appli : thm de Cayley, ex : $GL(2, 2) \sim S_3$.
2. Orbites et stabilisateurs.
 - [THG] def : orbite et stabilisateur, def : action transitive, ex : action de $GL(E)$ sur $\mathbb{P}(E)$.
 - [ULM] ex : l'action de D_n sur S_n est transitive, ex : cas des actions par translation et par conjugaison.
 - [THG] prop : les orbites forment une partition, ex : action naturelle de S_n sur $\{1, \dots, n\}$ qui donne la décomposition en cycle.
 - [ULM] appli : lien espace affine et action de groupes.
 - [H2G2]  appli : groupe d'isométrie du tétraèdre et du cube.
 - [THG] prop : la bijection $S/S_x \rightarrow O_x$ et l'égalité des cardinaux.
 - [RAU] ex : cardinal de S_n .
3. L'équation aux classes : action d'un groupe sur un ensemble fini.
 - [THG] thm : équation aux classes, corollaire : si $p|Card(G)$ alors il existe un élément de G d'ordre p .
 - [COM] appli (arithmétique) : $n^p = n \bmod(p)$, corollaire : thm de Burnside.
 - [COM] appli (dénombrement) : nombre de colliers possibles en fonction des perles de couleurs.
 - [THG] appli : thm de Sylow, ex : tout groupe d'ordre 40 possède un sous-groupe distingué.
 - [ULM] ex : un groupe d'ordre 200 n'est pas simple.

0.2 Description des orbites sur les espaces de matrices.

1. Un outil de classification.
 - [H2G2] def : invariants - invariant complet, def : système de représentants, def : action par équivalence, ex : thm du rang via l'action de groupes - le rang est un invariant complet - un système de représentant est l'ensemble des matrice $(J_r)_{0 \leq r \leq \min(m,n)}$, appli : le nombre de matrice de rang r dans $M_{n,m}(\mathbb{F}_q)$, def : action par multiplication à gauche, ex : le noyau est un invariant total - les matrices échelonnées en lignes sont un système de représentants, rq : cette matrice échelonnée réduite s'obtient par la méthode du pivot de Gauss en multipliant à gauche par des matrices inversibles correspondant à des opérations élémentaires (dilatation-transvection-permutation), appli : calcul du rang - inverse d'une matrice.
2. Application à la réduction des endomorphismes (et des formes quadratiques [SI POSSIBLE]).
 - [H2G2] def de l'action par conjugaison - $(P, M) \mapsto PMP^{-1}$, prop : deux matrices sont semblables ssi elles sont dans la même orbite, csq : classifier les endomorphismes revient à classifier les orbites pour cette action, ex : le déterminant - le polynôme minimal - le polynôme caractéristique - le spectre sont des invariants, appli : caractérisation de la diagonalisabilité (une matrice est dz ssi elle est dans la même orbite qu'une matrice diagonale), ex : pour l'action restreinte $GL_n(\mathbb{C}) \curvearrowright D_n(\mathbb{C})$, le polynôme caractéristique est un invariant complet et un système de représentants est donné par l'ensemble des matrices diagonales, c-ex : le polynome minimal n'est pas un invariant complet, appli : (réduction de Frobenius) : les invariants de similitude forment un système complet d'invariant - diagonalisation par blocs de matrices compagnons.
 - [FG]  appli : dénombrement des matrices diagonalisables de $M_n(\mathbb{F}_q)$.
 - [H2G2 et GRI] def : action par congruence, rq : deux matrices sont congruentes ssi elles sont les matrices de la même forme quadratique dans des bases différentes, def : signature - discriminant, appli : classification sur $\mathbb{C}$: invariants (le rang) et représentants - classification sur $\mathbb{R}$: invariants (la signature) et représentants

(thm de Sylvester) - classification sur $\mathbb{F}_q$: invariants (avec le discriminant) et représentants.

0.3 Actions sur un espace vectoriel : les représentations linéaires.

- [COL et RAU] def : représentation - dimension d'une représentation, ex : représentation de dimension 2 de S_3 ,
def : caractère d'une représentation, propriétés des caractères, ex : représentations de permutation, def : représentation irréductible, thm de Maschke, thm principal sur les caractères.
- [PEY] 🍷 ex : table de caractère de S_4 , ex : table de caractère de D_n .

Références :

Cortella, Théorie des groupes.
Combes, Algèbre et géométrie.
Ulmer, Théorie des groupes.
Colmez, Eléments d'analyse et d'algèbre.
Rauch, Les groupes finis et leurs représentations.
Peyré, L'algèbre discrète et la transformée de Fourier.
Histoire hédoniste des groupes et de la géométrie.

102 : Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.

1 Le cercle $\mathbb{S}_1$.

1. Paramétrisations du cercle.

- [AF] def : groupe $\mathbb{U}$, rq : lien avec le cercle unité, thm : l'isomorphisme de $\mathbb{R}_+^* \times \mathbb{U}$ dans $\mathbb{C}^*$, prop : $x \mapsto \exp(ix)$ de $\mathbb{R}$ dans $\mathbb{U}$ est surjectif - isomorphisme $\mathbb{Z}/2\pi\mathbb{Z} \sim \mathbb{U}$, def : sin et cos, appli : formule de Moivre - formule d'Euler, ex : somme des termes d'une progression géométrique, ex : linéarisation de $\cos^n(x)$, ex : polynôme de Tchebychev.
- [COM] prop : paramétrisation du cercle unité, appli : solution de l'équation de Diophante.

2. Groupe des rotations.

- [AF] def-prop : argument d'un nombre complexe, ex : forme trigonométrique, def : argument principal.
- [AUD] def-prop : $O^+(2)$ est isomorphe et homéomorphe au groupe multiplicatif $\mathcal{U}$, def-prop : isomorphisme $\mathbb{R}/2\pi\mathbb{Z} \sim O^+(2)$ et rotation d'angle θ , def : angle orienté de vecteurs, rq : tout angle orienté possède des mesures - lien avec l'argument, prop : isomorphisme du groupe des angles orientés dans $\mathbb{R}/2\pi\mathbb{Z}$, rq : faire attention à l'orientation choisie.

2 Racines de l'unité.

1. Groupes cycliques.

- [COM et AF] def-prop : $\mathbb{U}_n = \{z \mid z^n = 1\}$ est un sous-groupe de $\mathbb{C}^*$, ex : étude de $\mathbb{U}_k \cap \mathbb{U}_m$, ex : étude de $\text{Hom}(\mathbb{U}_{10}, \mathbb{U}_7)$ et $\text{Hom}(\mathbb{U}_{10}, \mathbb{U}_6)$, prop : sous-groupe de $\mathbb{U}$ et lien avec les sous-groupes de $\mathbb{R}$, prop : $\mathbb{U}_n$ est cyclique d'ordre n et engendré par $\exp(2i\pi/n)$, def : racines n -ième de l'unité - nombre des racine n -ièmes primitives de l'unité, ex : générateurs du groupe $\mathbb{U}_{18}$, prop : lien avec $\mathbb{Z}/n\mathbb{Z}$, thm : le seul sous-groupe fini de cardinal n de $(\mathbb{C}^*, \times)$ est $\mathbb{U}_n$, ex : éléments d'ordre 6 dans $\mathbb{U}_{30}$, ex : $\mathbb{U}_n \sim \mathbb{U}_p \times \mathbb{U}_q$ ssi p et q sont premiers entre-eux et $pq = n$, appli : $n = \sum_{d|n} \varphi(d)$, appli : $\mathbb{U}_n = \cup_{d|n} \Delta_d$.
- [ULM] appli : les racines n -ième de l'unité sont les sommets d'un polygone régulier à n côtés - définition du groupe diédral d'indice n - son ordre et ses générateurs.

2. Polynômes cyclotomiques.

- [COM] def : polynôme cyclotomique d'indice n - son degré est $\varphi(n)$, exemples, prop : un polynôme cyclotomique est unitaire à coefficients entiers - formule explicite des polynômes cyclotomiques, exemple : pour n impair $\phi_{2n}(X) = \phi_n(-X)$,  thm : **irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$** , coro : si ω est une racine n -ième de l'unité alors $\phi_n(X)$ est le polynôme minimal de ω , ex : $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ et réductible dans $\mathbb{F}_p$ pour tout nombre premier p .

3 Caractères linéaires d'un groupe abélien.

- [PEY] [A DETAILLER SELON LA PLACE] def : caractère linéaire et dual d'un groupe, ex : cas d'un groupe fini d'ordre n , thm : structure des groupes abéliens finis, coro : thm d'isomorphisme, prop : base orthonormal des caractères linéaires, def : l'espace hermitien $\mathbb{C}[G]$ - convolution, exemple, def : coefficients de Fourier - transformation de Fourier, prop : formule d'inversion, thm : convolution et transformée de Fourier,  appli : **transformation de Fourier discrète et calcul du déterminant circulant**, appli : marche aléatoire et transformation de Fourier discrète.

Références :

Arnaudiès - Fraysse, Cours de mathématiques 1 - Algèbre.

Combes, Algèbre et géométrie.

Audin, Géométrie.

Peyré, L'algèbre discrète de la transformée de Fourier.

103 : Exemples de sous-groupes distingués et de groupes quotients. Applications.

1 Quotients de groupes.

On veut essayer de se ramener à des groupes que l'on connaît pour avoir des propriétés ou pour classer les groupes. Comment décomposer un groupe en groupes plus simples ?

1. Sous-groupes distingués.

► [THG] *On veut factoriser un groupe via un morphisme de groupes en prenant son quotient par un de ses sous-groupes. Or on a une structure de groupe sur le quotient si le sous-groupe possède une propriété supplémentaire : la distinction.*

def : sous-groupe distingué, notation, exemples : cas des groupes commutatifs - les sous-groupes du centre d'un groupe sont distingués, prop : tout sous-groupe d'indice 2 est distingué, ex (cf ULM) : $\langle r \rangle \triangleleft D_n - A_n \triangleleft \mathfrak{S}_n$, prop : le noyau d'un morphisme est distingué, ex : le centre de G avec $K^* \triangleleft GL_n(K) - SL_n(K) \triangleleft GL_n(K) - SO_n(\mathbb{R}) \triangleleft O_n(\mathbb{R}) - A_n \triangleleft S_n$ - groupe des translations d'un espace affine est distingué dans le groupe affine, thm de Sylow, coro : G a un p -Sylow distingué ssi il a un unique p -Sylow, ex : tout groupe d'ordre 40 possède un sous-groupe distingué, def : sous-groupe dérivé, notation, thm : propriété universelle du groupe dérivé, exemple : cas de $S_3 - A'_4$ est le groupe des bitranspositions $D_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2. Groupe quotient.

► [THG] *Une des raisons d'utiliser des sous-groupes distingués est qu'ils fournissent des relations de congruence respectant la structure de groupe : on dit que cette relation est compatible avec la loi du groupe. De plus, la congruence modulo un sg distingué est la seule relation compatible avec la loi de G .*

thm : si $H \triangleleft G$ alors la surjection canonique est un morphisme de groupes - réciproquement : les seules relations s'équivalences donnant un groupe quotient intéressant sont celles modulo un sg distingué, ex : $\mathbb{Z}/n\mathbb{Z}$, thm : factorisation des morphismes de groupes, corollaire : 1er thm d'isomorphisme, exemples : $\mathbb{Z}/n\mathbb{Z} \simeq \nu_n - GL_n/SL_n(K) \simeq K^* - O_n(\mathbb{R})/SO_n(\mathbb{R}) \simeq \nu_2 - S_n/A_n \simeq \nu_2$.

► [COM] appli : nombre de carré dans $\mathbb{F}_q$.

► [ULM] thm : 2ième thm d'isomorphisme, ex : $\mathfrak{S}_4/V_4 \simeq \mathfrak{S}_3$, 3ième thm d'isomorphisme, ex : $(\mathbb{Z}/10\mathbb{Z})/(2\mathbb{Z}/10\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} - \mathfrak{S}_4/A_4 \simeq (\mathfrak{S}_4/V_4)/(A_4/V_4)$.

3. Groupes simples [SI POSSIBLE].

On cherche à étudier les "briques" élémentaires de la décomposition d'un groupe.

► [COM] def : groupe simple, prop : un groupe est d'ordre premier ssi il est cyclique et simple, c-ex : le groupe A_4 n'est pas simple, ex : A_n est simple pour $n \geq 5$, rq : la classification des groupes simples finis est terminé.

2 Table des caractères et sous-groupes distingués.

► [COL] [A DETAILLER SELON LA PLACE] def : caractère, ex : caractère linéaire, def : table des caractères.

► [RAU] prop : bijection entre les caractères de degré 1 de G et ceux de G/G' , ex : table des caractères de S_4 .

► [ULM et PEY] def : noyau d'un caractère,  **prop : tout sous-groupe distingué de G s'exprime en fonction du noyau de ses caractères**, exemple : table de caractère de D_6 , coro : un groupe est simple ssi tout caractère irréductible a un noyau trivial.

3 Le groupe en fonction de ses sous-groupes.

Comment reconstruire le groupe à partir de ses sous-groupes ?

1. Le produit direct.

- [COM] def : produit direct, ex : si f est la bijection de $\mathcal{P}(E)$ sur $\{0,1\}^E$ on étudie la structure de groupe sur $\mathcal{P}(E)$, prop : caractérisation du produit direct, ex : $\mathbb{U}_6 \simeq \mathbb{U}_3 \times \mathbb{U}_2$.
- [H2G2]  appli : groupe d'isométrie du tétraèdre et du cube.
- [ULM] : ex : $\mathfrak{A}_4$ est d'ordre 12 n'est pas simple et fournit un contre-exemple au théorème de Lagrange.

2. Le produit semi-direct.

- [THG] def : produit semi-direct, prop : condition d'isomorphisme entre G et $H_1 \rtimes H_2$ - produit semi-direct interne, prop : lien produit semi-direct et produit direct, exemples : tout produit direct est un produit semi-direct - cas d'un espace affine produit semi-direct de V et $GL(V)$ - $GL_n(K) \simeq K^* \rtimes SL_n(K)$ - $O_n(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z} \rtimes SO_n(\mathbb{R})$ - $\mathfrak{S}_n \simeq \mathbb{Z}/2\mathbb{Z} \rtimes A_n$, appli : forme du groupe des isométries affines de $\mathbb{R}^n$, prop : condition pour que $G \simeq \nu_q \rtimes \nu_p$, rq : il peut y avoir plusieurs produits semi-directs de 2 même groupes qui peuvent être ou non isomorphes, exemples : produit semi-direct de $\mathbb{Z}/7\mathbb{Z}$ par $\mathbb{Z}/3\mathbb{Z}$.
- [COM] appli : a isomorphisme près un groupe d'ordre $2p$ n'a que deux structures possibles.

Références :

Cortella, Théorie des groupes.
Combes, Algèbre et géométrie.
Ulmer, Théorie des groupes.
Colmez, Eléments d'analyse et d'algèbre.
Rauch, Les groupes finis et leurs représentations.
Peyré, L'algèbre discrète et la transformée de Fourier.
Histoire hédoniste des groupes et de la géométrie.

104 : Groupes finis. Exemples et applications.

1 Structure des groupes finis.

1. Ordre.

- [THG] def : ordre d'un élément, exemples : les racines primitives de l'unité - les transpositions - les symétries - les rotations.
- [ULM] appli : le groupe diédral est le sous-groupe des isométries du plan affine qui laisse un n -gone invariant - D_n est d'ordre $2n$ - il est engendré par la symétrie axiale et une rotation - le sous-groupe $\langle r \rangle$ est distingué d'ordre n .
- [THG] def : équivalence modulo un sous-groupe, notation : G/H , thm de Lagrange, def : indice d'un sous-groupe, coro : l'ordre d'un élément divise l'ordre du groupe.
- [COM] ex : étude de $\mathbb{U}_k \cup \mathbb{U}_m$.

2. Groupes abéliens finis.

- [COM] def : groupe cyclique, exemples : $\mathbb{Z}/n\mathbb{Z}$ - $\mathbb{U}_n$.
- [ULM] c-ex : $GL_2(\mathbb{F}_2)$ n'est pas cyclique.
- [COM] prop : ordre d'un élément - générateurs des groupes cycliques, ex : générateurs du groupe $\mathbb{Z}/12\mathbb{Z}$ - $\mathbb{U}_{18}$, ex : nombre d'éléments d'ordre 2 dans $\mathbb{Z}/n\mathbb{Z}$, prop : isomorphisme avec G cyclique et $\mathbb{Z}/n\mathbb{Z}$, théorème Chinois (cf ULM), appli : résolution de système de congruence,  thm : **structure des groupes abéliens finis**, corollaire : décomposition en composantes primaires d'un groupe, exemple : décomposition de $\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}$.

3. Sous-groupe d'un groupe fini.

- [COM] prop : sous-groupe d'un groupe cyclique, ex : les sous-groupes de $\mathbb{Z}/20\mathbb{Z}$, ex : les éléments d'ordre 6 dans le groupe $\mathbb{U}_{30}$, appli : $n = \sum_{d|n} \varphi(d)$.
- [THG] def : p -Sylow, exemple, thm de Sylow, ex : nombre de 3-Sylow dans S_4 - tout groupe d'ordre 40 possède un sous-groupe distingué.
- [COM] def : produit direct, prop : caractérisation du produit direct, ex : $\mathbb{U}_6 \simeq \mathbb{U}_3 \times \mathbb{U}_2$.
- [THG] [SI POSSIBLE] def : produit semi-direct, prop : condition d'isomorphisme entre G et $H_1 \rtimes H_2$ - produit semi-direct interne, exemples : cas d'un espace affine produit semi-direct de V et $GL(V)$ - $GL_n(K) \simeq K^* \rtimes SL_n(K)$ - $O_n(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z} \rtimes SO_n(\mathbb{R})$, appli : forme du groupe des isométries affines de $\mathbb{R}^n$.
- [ULM] ex : $\mathfrak{A}_4$ est d'ordre 12 n'est pas simple et fournit un contre-exemple au théorème de Lagrange.

2 Actions de groupes.

1. Orbites et stabilisateurs.

- [THG] def : action de groupes, def : orbite-stabilisateur, exemple : actions naturelles - actions de $GL(E)$ sur $\mathbb{P}(E)$, prop : bijection entre G/S_x et O_x .
- [FG] appli : dénombrement des matrices diagonalisables de $M_n(\mathbb{F}_q)$.
- [COM] prop : action d'un groupe fini sur un ensemble fini (équation des classes - formule de Burnside), appli : $p \mid \binom{p}{k}$, appli : $n^p = n \bmod(p)$, appli : nombre de colliers différents avec 4 perles bleues - 3 blanches - 2 rouges, appli : thm de Cauchy.

2. Le groupe symétrique.

- [THG] *Un des intérêt du groupe des bijections d'un ensemble fini est de pouvoir identifier un groupe fini G à un sous-groupe de $\mathfrak{S}_n$*
prop : identifier G à un sous-groupe de $\mathfrak{S}(G)$ et si E est fini alors $\mathfrak{S}_n \simeq \mathfrak{S}(E)$.
- [COM] prop : toute permutation s'écrit de manière unique comme un produit de cycle disjoint, exemple (ordre d'une permutation), prop : générateur du groupe symétrique.
- [THG] ex : action naturelle de $\mathfrak{S}_n$ sur $\{1, \dots, n\}$ et lien avec le support - cycle - orbite - stabilisateur.

-
- [THG] def : signature, thm : la signature est l'unique morphisme non trivial de $\mathfrak{S}_n$ dans $\mathbb{C}^*$, def : groupe alterné, prop : le groupe alterné est engendré par les 3-cycles, ex : $\mathfrak{S}_n \simeq \mathfrak{A}_{n+2}$, ex : si G est un sous-groupe de $\mathfrak{S}_n$ contenant une permutation impaire $G \cap \mathfrak{A}_n$ est un sous-groupe d'indice 2 de G , ex : $\mathfrak{S}_n \simeq \mathbb{Z}/2\mathbb{Z} \rtimes A_n$.
 - [H2G2]  appli : groupe d'isométrie du tétrèdre et du cube.

3 Représentations et tables des caractères.

- [COL et RAU] def : représentation - dimension d'une représentation, ex : représentation de dimension 2 de $\mathfrak{S}_3$, def : caractère d'une représentation, propriétés des caractères, ex : représentations de permutation, def : représentation irréductible, thm de Maschke, def : table des caractères, thm principal sur les caractères.
- [PEY]  ex : table de caractère de $\mathfrak{S}_4$, ex : table de caractère de D_n .
- [ULM et PEY] def : noyau d'un caractère, prop : tout sous-groupe distingué de G s'exprime en fonction du noyau de ses caractères, exemple : table de caractère de D_6 , coro : un groupe est simple ssi tout caractère irréductible a un noyau trivial.

Références :

Cortella, Théorie des groupes.
 Combes, Algèbre et géométrie.
 Ulmer, Théorie des groupes.
 Colmez, Eléments d'analyse et d'algèbre.
 Rauch, Les groupes finis et leurs représentations.
 Peyré, L'algèbre discrète et la transformée de Fourier.
 Histoire hédoniste des groupes et de la géométrie.

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

1 $\mathfrak{S}(E)$ et son action naturelle.

1. Permutations d'un ensemble fini.

- [THG] def : groupe $\mathfrak{S}(E)$ - groupe symétrique, ex : $\mathfrak{S}_3$ est le plus petit groupe non commutatif, prop (thm de Cayley) : action de G sur lui-même - identifier G à un sous-groupe de $\mathfrak{S}(G)$, prop : $\mathfrak{S}(E) \simeq \mathfrak{S}_n$, notations et terminologie : permutation - k -cycle - support, prop : ordre des k -cycle - deux permutations à supports disjoints commutent - prop : toute permutation se décompose en un unique produit de cycles disjoints, exemple : décomposition et ordre d'une permutation.
- [COM] ex : centre de $\mathfrak{S}_n$, ex : nombre d'éléments d'ordre p premier dans $\mathfrak{S}_p$.
- [RAU et THG] prop : l'action naturelle de $\mathfrak{S}_n$ sur $\{1, \dots, n\}$ est transitive et la relation orbite stabilisateur donne le cardinal de $\mathfrak{S}_n$ - action de $\langle \sigma \rangle$ sur $\{1, \dots, n\}$ (on retrouve la notion de support - de cycle - décomposition en cycles disjoints - stabilisateur et ordre d'une orbite).
- [THG] appli : définition des polynômes symétriques.
- [GOU] exemples.

2. Signature et groupe alterné.

- [THG] def : signature, exemple : image de la signature, lemme : expression de la signature comme un produit de "taux d'accroissement", thm : la signature est l'unique morphisme de groupes non trivial de $\mathfrak{S}_n$ dans $\mathbb{C}^*$, ex [COM] : signature, def : sous-groupe alterné.
- [COM] prop : A_n est un sous-groupe distingué d'indice 2 de $\mathfrak{S}_n$ et son cardinal est $n!/2$, ex : A_n est le groupe dérivé de $\mathfrak{S}_n$, ex : dans A_4 il n'existe pas de sous-groupe d'ordre 6 bien que 6 divise l'ordre de A_4 .
- [GOU] appli : définition du déterminant.
- [THG] appli : matrice de permutations.

2 Structure de groupes : classes de conjugaison et générateurs.

- [COM et THG] prop : cycles conjugués, ex : $\mathfrak{S}_n$ agit transitivement par conjugaison sur l'ensemble des transpositions, ex [ULM] : 2 cycles conjugués, prop : générateurs du groupe symétrique, exemple, corollaire : la parité du nombre de transpositions utilisées ne dépend pas de la décomposition : la signature est un invariant, prop : A_n est engendré par les 3-cycles qui sont tous conjugués dans A_n dès que $n \geq 5$, c-ex : ils ne sont pas conjugués pour $n = 3, 4$.
- [PER] ex : le groupe dérivé de A_n est A_n .
- [ULM] appli : A_5 est simple, c-ex : A_4 n'est pas simple, appli : les sous-groupes distingués de $\mathfrak{S}_n$ pour $n \geq 5$.
- [H2G2]  appli : les groupes d'isométrie du tétraèdre et du cube.
- [THG] prop : $\mathfrak{S}_n = \mathbb{Z}/2\mathbb{Z} \rtimes A_n$, ex : cas $n = 3$.

3 Action de groupes.

1. Action d'un groupe sur un ensemble fini.

- [THG] thm : équation aux classes.
- [COM] appli (arithmétique) : $n^p = n \bmod(p)$, corollaire : thm de Burnside.
- [COM] appli (dénombrement) : nombre de colliers possibles en fonction des perles de couleurs.
- [THG] appli : thm de Sylow, ex : tout groupe d'ordre 40 possède un sous-groupe distingué, ex : nombre de 3-Sylow dans $\mathfrak{S}_4$.

2. Représentations linéaires de groupes finis.

- [COL et RAU] def : représentation - dimension d'une représentation, ex : représentation de dimension 2 de $\mathfrak{S}_3$, def : caractère d'une représentation, propriétés des caractères, ex : représentations de permutation, ex : représentation régulière, def : représentation irréductible, thm de Maschke, def : table des caractères, thm

principal sur les caractères.

► [PEY]  ex : table de caractère de $\mathfrak{S}_4$, appli : décomposition de l'action de $\mathfrak{S}_4$ sur les faces du cube (représentation de permutations).

Références :

Cortella, Théorie des groupes.

Combes, Algèbre et géométrie.

Ulmer, Théorie des groupes.

Colmez, Eléments d'analyse et d'algèbre.

Rauch, Les groupes finis et leurs représentations.

Peyré, L'algèbre discrète et la transformée de Fourier.

Histoire hédoniste des groupes et de la géométrie.

Gourdon, Algèbre.

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

1 Le groupe linéaire : une interprétation matricielle.

1. Le groupe linéaire et spécial linéaire.
 - [PER] def : $GL(E) - GL_n(\mathbb{K})$, rq : isomorphisme $GL(E) \simeq GL_n(\mathbb{K})$ non canonique, rq : l'intérêt est de pouvoir utiliser les outils du calcul matriciel pour étudier $GL(E)$.
 - [GOU] prop : $f \in GL(E) \Leftrightarrow f$ injective $\Leftrightarrow f$ surjective $\Leftrightarrow \det(f) \neq 0$ en dimension finie, c-ex : faux en dimension infinie.
 - [OA] ex : groupes linéaires isomorphes.
 - [PER] def : $SL(E)$ via le déterminant (qui réalise un morphisme de $GL(E)$ dans k^*), rq : $SL(E)$ est donc un ss-groupe distingué, prop : $GL(E)$ est le produit semi-direct de $SL(E)$ par k^* , appli : cardinaux de $GL(\mathbb{F}_q)$ et de $SL(\mathbb{F}_q)$.
2. Générateurs.
 - [PER] def-prop : dilatations - transvections.
 - [XENS2]  prop : **générateurs de SL_n et de $GL_n(\mathbb{R})$, appli : $SL_n(\mathbb{R})$ est connexe par arcs.**
 - [PER] appli : centre de $GL(E)$ et $SL(E)$.
3. Topologie.
 - [MT] prop : $GL_n(K)$ est un ouvert dense dans $M_n(K)$, appli : $\chi_{AB} = \chi_{BA}$, prop : $GL_n(\mathbb{C})$ est connexe - $GL_n(\mathbb{R})$ n'est pas connexe, prop : les composantes connexes de $GL_n(\mathbb{R})$.
 - [XENS3] appli : composantes connexes de l'ensemble des formes quadratiques non dégénérées.

2 Exemples de sous-groupes finis de $GL_n(\mathbb{K})$. [SI POSSIBLE]

➤ [OA] def : matrice de permutations, ex : matrice de transposition, prop : l'inclusion $\mathfrak{S}_n \hookrightarrow GL_n(K)$, rq : tout groupe d'ordre n peut s'identifier à un sous-groupe de $GL_n(\mathbb{K})$, prop : les sous-groupes finis de $GL_m(k)$ de cardinal n sont conjugués à un sous-groupe des matrices diagonales (k algébriquement clos - n premier avec $\text{car}(k)$), contres-exemples.

3 Action de $GL_n(R)$ sur $S_n(R)$ par congruence.

1. Action par congruence.
 - [H2G2 et GRI] def : action de $GL_n(R)$ sur $S_n(R)$ par congruence - matrices congruentes, rq : deux matrices sont congruentes ssi elles sont les matrices de la même forme quadratique dans des bases différentes, thm de Sylvester : classification sur $\mathbb{R}$ (invariants : la signature - représentants), appli : classification des quadriques.
 - [ROU] appli : le lemme de Morse.
2. Le groupe orthogonal $O_n(\mathbb{R})$.
 - [H2G2] def : groupe orthogonal $O_n(\mathbb{R})$ d'une forme quadratique Q comme le stabilisateur de I_n pour l'action par congruence.
 - [GRI] ex : description de $O_2(\mathbb{R})$ - dessins en ANNEXE, appli : angle non orienté et orienté en dimension 2, thm : réduction des endomorphismes orthogonaux, ex : description de $O_3(\mathbb{R})$ - dessins en ANNEXE, exemple.
 - [MT] prop : $SO_n(\mathbb{R})$ est un ouvert connexe - $O_n(\mathbb{R})$ possède 2 composantes connexes.
 - [H2G2] prop : $O_n(\mathbb{R})$ et $SO_n(\mathbb{R})$ sont compacts.

► [PER] def : réflexion et retournement, prop : $O(E)$ est engendré par les réflexions - $SO(E)$ par les retournements.

3. Le groupe $S_n^{++}(\mathbb{R})$.

► [H2G2 et GOU] def : $S_n^{++}(\mathbb{R})$ comme l'orbite de I_n pour l'action par congruence, prop : c'est l'ensemble des matrices symétriques définies positives, appli : existence et unicité de la racine carrée, appli : décomposition polaire, appli : définition de la norme subordonnée matricielle 2.

4 Représentations linéaires.

► [COL et RAU] def : représentation - dimension d'une représentation, ex : représentation de dimension 2 de $\mathfrak{S}_3$, def : caractère d'une représentation, propriétés des caractères, ex : représentations de permutation, def : représentation irréductible, thm de Maschke, def : table des caractères, thm principal sur les caractères.

► [PEY] ex : table de caractère de $\mathfrak{S}_4$, ex : table de caractère de D_n .

► [ULM et PEY] def : noyau d'un caractère,  prop : tout sous-groupe distingué de G s'exprime en fonction du noyau de ses caractères, exemple : table de caractère de D_6 , coro : un groupe est simple ssi tout caractère irréductible a un noyau trivial.

Références :

Perrin, Cours d'algèbre.

Caldero - Germoni, Histoire hédoniste des groupes en géométrie.

Grifone, Algèbre linéaire.

Gourdon, Algèbre.

Objectif Agrégation.

Mneimné Testard, Groupes de Lie classiques.

Colmez, Elements d'analyse et d'algèbre.

Rauch, Les groupes et leurs représentations.

Peyre, Transformée de Fourier discrète.

Rouvière, Petite guide de calcul différentiel.

Oraux X - ENS, Algèbre 2 et 3.

107 : Représentations et caractères d'un groupe fini sur un $\mathbb{C}$ -espace vectoriel. Exemples.

1 Décomposition de représentations linéaires.

1. Représentations linéaires.

- [COL] : def : représentation linéaire (donner les 2 définitions équivalentes), def : représentation fidèle, rq : en dimension finie le choix d'une base fournit une représentation concrète comme groupe de matrices, exemples : représentations de $\mathbb{Z}$ - de $\mathbb{Z}/n\mathbb{Z}$ - de $\mathbb{Z}^2$.
- [RAU] ex : le groupe des isométries du tétraèdre G_T et du cube G_C sont des représentations de $\mathfrak{S}_4$.
- [COL] def : dimension d'une représentation - matrice d'une représentation et le morphisme de groupes qu'elle induit, remarque : diagonalisabilité d'une représentation dans le cas d'un groupe fini), ex : construction d'une représentation de dimension 2 de $\mathfrak{S}_3$, ex : représentations de permutation - représentation régulière, def/prop : représentation de $\text{Hom}(V_1, V_2)$ - représentations isomorphes (donner les différents points de vue), exemple : classification des représentations de $\mathbb{Z}$ à iso près.
- [RAU] ex : G_T et G_C ne sont pas équivalentes.

2. Représentations irréductibles.

- [COL] : def : sous-représentation - représentation irréductible, ex : représentation de $\mathfrak{S}_3$ sur $\mathbb{C}^2$, ex : cas de $\mathbb{Z}$ (faire le parallèle avec la diagonalisation).
- [RAU] ex : G_T et G_C sont irréductibles. ???
- [COL] def : sommes directes de représentations, thm : existence d'un produit scalaire invariant sous l'action de G , thm de Maschke.

2 Théorie des caractères.

1. Caractères d'une représentation linéaire.

- [COL] : def : caractère d'une représentation, propriétés des caractères, ex : caractère linéaire - la signature est un caractère, ex : caractère d'une représentation de permutation et d'une représentation régulière, prop : si G est fini $\chi_{\text{Hom}(V_1, V_2)}(g) = \chi_{V_1}(g)\chi_{V_2}(g)$ - l'égalité $\chi_{V_1}(g) = \chi_{V_2}(g)$ pour tout $g \in G$, ex : représentation duale et son caractère.

2. Fonctions centrales.

- [COL] : lemme de Schur, ex : tout élément de $\text{Hom}(V_1, V_2)$ est de la forme λu si V_1 et V_2 sont iso et u morphisme de représentations, def [ULM] : fonction centrale, prop : propriétés de l'application moyenne (csq de Schur), thm : orthogonalité des caractères, def : table de caractères.
- [RAU] : thm principal sur les caractères.
- [COL] : corollaire : même caractère implique iso - caractérisation de l'irréductibilité d'une représentation.
- [RAU et PEY] :  ex : table des caractères de $\mathfrak{S}_4$, ex : table de D_n , appli : décomposition de l'action de $\mathfrak{S}_4$ sur les faces du cube.
- [ULM] def : noyau d'un caractère, prop : noyaux de caractères et sous-groupes distingués, exemple, appli : caractérisation de la simplicité d'un groupe, exemple : A_5 .

3. Cas des groupes commutatifs : la transformée de Fourier.

- [COL et PEY] : thm : toute représentation irréductible est de dimension 1 - les caractères irréductibles sont les caractères linéaires, def : produit de convolution sur $\mathbb{C}[G]$, exemple, def : coefficient - transformée de Fourier, thm : convolution et transformée de Fourier, def : transformée de Fourier discrète, ex : la matrice de $\mathcal{F}$ est une Vandermonde, ex : interpolation trigonométrique, appli : marche aléatoire et transformée de Fourier discrète, prop : transformée de Fourier inverse - formule de Plancherel, ex : matrice circulante, .

appli : déterminant circulant et transformation de Fourier discrète.

Références :

Ulmer, Théorie des groupes.

Colmez, Eléments d'analyse et d'algèbre.

Rauch, Les groupes finis et leurs représentations.

Peyré, L'algèbre discrète et la transformée de Fourier.

Caldero - Germoni, Histoire hédoniste des groupes et de la géométrie.

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

1 Générateurs d'un groupe.

1. Groupes monogènes.

► [THG] notation : sous-groupe engendré par X une partie d'un groupe G , prop : expression des éléments de X , def : famille qui engendre G - groupe monogène, exemples : $\mathbb{Z}$ et $\mathbb{U}_n$ est monogène - les sg de $\mathbb{Z}$ sont monogènes - un sg de type fini de $(\mathbb{Q}, +)$ est monogène mais pas de type fini - tout groupe fini est de type fini, rq : expliciter les morphismes de groupes, prop : $G \simeq (\mathbb{Z}, +)$ ou $G \simeq \mathbb{U}_r$ selon si G est monogène infini ou d'ordre r .

► [COM] def : groupe cyclique, exemples : $\mathbb{Z}/n\mathbb{Z} - \mathbb{U}_n$, prop : générateurs d'un groupe cyclique, exemple : générateurs de $(\mathbb{Z}/12\mathbb{Z}, +)$ et $(\mathbb{U}_{18}, *)$, rq : les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les inversibles de l'anneau, prop : homomorphisme entre groupes cycliques, appli : caractérisation de $\text{Aut}(G)$, exemple : $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) - \text{Aut}(\mathbb{Z}/5\mathbb{Z})$ est cyclique, thm : reste chinois, exemple, appli : résolution d'un système de congruence, prop : sg d'un groupe cyclique, exemple : sg de $\mathbb{Z}/20\mathbb{Z}$, exemple : les éléments d'ordre 6 dans $\mathbb{U}_{30}$, appli : $n = \sum_{d|n} \varphi(d)$, prop : morphismes entre 2 groupes cycliques, exemple : études des morphismes de $\mathbb{Z}/21\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$.

2. Groupe abélien.

► [COM] thm de structure des groupes abéliens - invariants de G , coro : sous-groupe et décomposition en facteurs premiers de n - composantes primaires, exemple : composantes primaires de $\mathbb{U}_{90}$, exemple : décomposition canonique de $(\mathbb{Z}/60\mathbb{Z}) \times (\mathbb{Z}/72\mathbb{Z})$.

2 Le groupe symétrique.

► [COM] def : permutations - groupe symétrique - cycles et transposition, appli [THG] : def de la sous-algèbre des polynômes symétriques, prop : décomposition en cycles disjoints, exemple, prop : les permutations engendrent $\mathfrak{S}_n$.

► [THG] exemple, def : inversion d'une permutation - signature, exemple, appli : def du déterminant, thm : l'application sg est l'unique morphisme de groupes non trivial de $\mathfrak{S}_n$ dans $\mathbb{C}^*$, def : groupe alterné, prop : les 3-cycles engendrent $\mathfrak{A}_n$, exemples.

► [??]  thm : les transvections engendrent $SL(E)$, coro : les transvections et les dilatations engendrent $GL(E)$.

3 Le groupe linéaire $GL(E)$.

1. Groupe linéaire et groupe orthogonal.

► [PER] Cadre : E est un k -ev avec k un corps quelconque, def : $GL(E) - SL(E)$, rq : l'isomorphisme non canonique entre $GL(E)$ et $GL_n(\mathbb{R})$, prop-def : dilatations - transvections.

► [XENS]  thm : les transvections engendrent $SL(E)$, coro : les transvections et les dilatations engendrent $GL(E)$.

► [OA - GRI] appli : matrice de permutations et algorithme du pivot de Gauss, exemple.

► [MT] prop : $GL_n(\mathbb{C})$ est connexe, appli : connexité de l'ensemble des projecteurs de rang p , appli : $SL(E)$ est connexe par arcs - $GL_n(\mathbb{R})$ n'est pas connexe mais a deux composantes connexes homéomorphes.

► [PER] cadre : E est $\mathbb{R}$ -ev de dimension finie, def : $O(E)$ et $SO(E)$, rq : l'isomorphisme avec $O_n(\mathbb{R})$ et $SO_n(\mathbb{R})$, exemple d'isométrie : réflexion et renversement, thm : $O(E)$ est engendré par les réflexions orthogonales, thm : $SO_n(\mathbb{R})$ est engendré par les renversements.

2. Représentations linéaires.

► [COL et RAU] def : représentation - dimension d'une représentation, ex : représentation de dimension 2 de $\mathfrak{S}_3$, rq : cas des groupes définis par des générateurs et relations, exemples, def : caractère d'une représentation, propriétés des caractères, ex : représentations de permutation, def : représentation irréductible, thm de Maschke, def : table des caractères, thm principal sur les caractères.

► [PEY] ex : table de caractère de $\mathfrak{S}_4$.

► [ULM] appli (le groupe diédral) : définition (vision géométrique) - son ordre - ses générateurs - [PEY] sa

table de caractère.

Références :

Perrin, Cours d'algèbre.

Combes, Algèbre et géométrie.

Cortella, Théorie des groupes.

Colmez, Elements d'analyse et d'algèbre.

Rauch, Les groupes finis et leurs représentations.

Ulmer, Théorie des groupes.

Grifonne, Algèbre linéaire.

Mneimé - Testard, Introduction à la théorie des groupes de Lie classiques.

Oraux X-ENS, Algèbre 2.

110 : Caractères d'un groupe abélien fini et transformée de Fourier discrète. Applications.

1 Caractères d'un groupe abélien fini.

1. Groupe dual.

► [PEY] def : caractères et dual d'un groupe, rq : $\widehat{G}$ est un groupe pour la multiplication des applications, exemple : avec G de cardinal n c'est la groupe des racines n -ième de l'unité, prop : dual d'un groupe cyclique, rq : isomorphisme non canonique, rq : l'étude des groupes cycliques est important - $|G| = |\widehat{G}|$, c-ex : c'est faux si G n'est pas commutatif - $\widehat{\widehat{G}} \simeq G$.

2. Dual d'un groupe abélien fini.

► [PEY]  thm : **structure des groupes abéliens**, coro : thm d'isomorphisme (il n'est pas canonique), def : bidual, prop : isomorphisme canonique, lemme : $\sum_{g \in G} \chi(g) = 0$ si $\chi \neq 1$ ou $|G|$ si $\chi = 1$, prop : orthogonalité des caractères, ex : relation d'orthogonalité "duale", appli : dénombrement de solutions.

3. Table des caractères.

► [COL et RAU] def : représentation, ex : représentations de $\mathbb{Z}/n\mathbb{Z}$, propriétés des caractères, ex : représentations de permutation, def : représentation irréductible, exemple des groupes abéliens, rq : lien avec la réduction simultanée, thm de Maschke, thm principal sur les caractères.

► [PEY] ex : table de caractère de $\mathbb{Z}/n\mathbb{Z}$.

2 L'algèbre du groupe G .

1. L'espace hermitien $\mathbb{C}[G]$.

► [PEY] def : espace des fonctions sur G - produit scalaire associé, rq : invariance par translation, prop : base canonique de $\mathbb{C}[G]$ - structure d'ev sur $\mathbb{C}$, rq : décomposition d'une fonction dans cette base, rq : cette base n'est pas très pratique, prop (cas cyclique) : $\widehat{G}$ forme une bon de $\mathbb{C}[G]$, prop : $\widehat{G}$ est une bon de $\mathbb{C}[G]$.

2. Produit de convolution.

► [PEY] def : produit de convolution sur $\mathbb{C}[G]$, exemple : convolution par une fonction δ_g , prop : le produit de convolution munit l'ev $\mathbb{C}[G]$ d'une structure d'algèbre, prop : morphisme d'algèbre, rq : correspondance entre les morphismes de groupes de G dans $\mathbb{C}^*$ et les morphismes d'algèbre de $\mathbb{C}[G]$ dans $\mathbb{C}$, appli : interprétation probabiliste.

3 Transformée de Fourier.

1. Transformée de Fourier sur un groupe fini.

► [PEY] def : coefficients de Fourier - application $c : \mathbb{C}[G] \rightarrow \mathbb{C}[\widehat{G}]$, def : transformée de Fourier, prop : formule d'inversion, prop : isomorphisme de Fourier, prop : formule de Plancherel, prop : morphisme d'algèbre (étendre χ en un morphisme d'algèbre), thm : convolution et transformée de Fourier,  appli : **déterminant circulant et transformation de Fourier discrète**.

2. Transformée de Fourier discrète.

► [PEY] def : transformée de Fourier discrète, ex : la matrice de $\mathcal{F}$ est une matrice de Vandermonde, ex : interpolation trigonométrique, rq : lien avec la transformée de Fourier sur un groupe fini, prop : transformée de Fourier inverse - formule de Plancherel, ex : matrice circulante, appli : traitement du signal.

Références :

Peyré, L'algèbre discrète de la transformée de Fourier.

Colmez, Elements d'analyse et d'algèbre.

Rauch, Les groupes finis et leur représentations.

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

1 Congruence d'entiers : le groupe $\mathbb{Z}/n\mathbb{Z}$.

- [COM] rq : $\mathbb{Z}$ est euclidien donc principal - ses idéaux - ses idéaux maximaux donc premiers - son groupe des inversibles, def : congruence de 2 entiers, notation, rq : relation compatible avec les opérations de $\mathbb{Z}$, def : ensemble $(\mathbb{Z}/n\mathbb{Z}, +)$, prop : c'est un groupe abélien cyclique d'ordre n , def : indicatrice d'Euler, prop : générateurs de groupes cycliques, ex : générateurs de $\mathbb{Z}/12\mathbb{Z}$, ex : éléments d'ordre 2 dans $\mathbb{Z}/n\mathbb{Z}$, lemme : isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur G , ex : $\mathbb{U}_n \sim \mathbb{Z}/n\mathbb{Z}$, prop : unique sous groupe d'ordre $d|n$, ex : sous-groupes de $\mathbb{Z}/20\mathbb{Z}$, ex : $n = \sum_{d|n} \phi(d)$.
- [???] prop : morphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(\mathbb{Z}/m\mathbb{Z}, +)$.
- [COM] ex : expression de tous les morphismes de $\mathbb{Z}/21\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$ - de $\mathbb{Z}/18\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$,  prop : **décomposition cyclique d'un groupe abélien fini**, appli : existence d'une décomposition primaire pour un groupe abélien, ex : décomposition canonique de $\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}$.

2 Structure de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

1. Inversibles de $\mathbb{Z}/n\mathbb{Z}$.
 - [COM] rq : $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau, prop : inversibles de l'anneau, appli : critères de divisibilité, appli : résolution de $522x + 2214y = 36$, coro : appli : résolution d'un système de congruence, prop : [PER] : automorphisme de $\mathbb{Z}/n\mathbb{Z}$, (rq : la description de $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ est importante pour déterminer des produits semi-direct), ex : le groupe $\text{Aut}(\mathbb{Z}/5\mathbb{Z})$ est cyclique - ses éléments - ses générateurs, prop : idéaux et idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$, ex : quotient de $\mathbb{Z}/n\mathbb{Z}$ par un idéal maximal, prop : $\mathbb{Z}/p\mathbb{Z}$ est un corps ssi p est premier, exemple.
2. Théorème des restes chinois.
 - [COM] thm des restes chinois, ex : dans $\mathbb{Z}/pq\mathbb{Z}$ il existe 4 éléments idempotents - il existe 4 endomorphismes de l'anneau A dans lui même, c-ex : $\mathbb{Z}/4\mathbb{Z}$ n'est pas iso à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, appli : résolution d'un système de congruences.
 - [???] parler des nilpotents et des idempotents de $\mathbb{Z}/n\mathbb{Z}$. ???

3 Application à l'arithmétique dans $\mathbb{Z}$.

1. Nombres premiers.
 - [COM] prop : théorème de Fermat-Euler et de Wilson, ex : chiffre des unités de 27^{1995} .
 - [GOU] appli : chiffrement RSA, c-ex : la réciproque du théorème de Fermat est fausse - nombres pseudo-premiers en base a et nombre de Carmichael.
 - [COM] def : indicatrice d'Euler, appli : multiplicativité de l'indicatrice d'Euler - indicatrice d'Euler et décomposition en facteurs premiers - $\varphi(mn)$ avec m et n pas premier.
2. Résidus quadratiques.
 - [COM] def : résidu quadratique, ex : discriminant d'une forme quadratique, prop : caractérisation des carrés dans $\mathbb{F}_p$, ex : -1 est un résidu quadratique pour $p = 4k + 1$, appli : résolutions d'équation diophantienne - $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p$, ex : résolution de $5x^2 + 3y^2 = 11 \pmod{13}$.
 - [PER]  **thm des deux carrés**.
 - [DUV] appli : résolution d'une équation diophantienne avec le thm des 2 carrés, def : symbole de Legendre, rq : critère d'Euler, exemples de calculs, coro : multiplicativité du symbole de Legendre, thm : loi de réciprocité quadratique, exemples de calculs, appli : résolution de $x^2 + 7x - 2 = 0 \pmod{31}$.
 - [GOU] appli : 5 est un carré dans $\mathbb{F}_p$ ssi $p \equiv \pm 1 \pmod{10}$ - infinité de nombre premier de la forme $10n - 1$.

4 Application à l'étude de l'irréductibilité de polynômes.

1. Irréductibilité dans $\mathbb{Z}/p\mathbb{Z}[X]$.

► [GOZ] thm : $\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$ avec π irréductible de degré n , *rq* : l'étude des polynômes irréductibles sur $\mathbb{F}_p$ permet de construire les corps finis, *coro* : il existe des polynômes irréductibles de tout degré, thm : facteurs irréductibles de $X^{p^n} - X$, appli : dénombrement des polynômes irréductibles sur $\mathbb{F}_q$, exemples.

2. Irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$.

► [COM] thm : f irréductible dans $A[X]$ ssi f irréductible dans $K[X]$ avec K corps des fractions dans A factoriel, ex : $X^3 - 2X + 3/4$ est irréductible dans $\mathbb{Q}[X]$, *rq* : cas des polynômes de degré 2 ou 3, ex : $X^2 + X + 4$ est irréductible dans $\mathbb{Z}/7\mathbb{Z}[X]$, *c-ex* : faux pour les degrés ≥ 4 , *prop* : critère d'irréductibilité d'Eisenstein, exemples, *prop* : critère de réduction, exemples, *def* : polynôme cyclotomique, *prop* : expression par récurrence, exemples, thm : irréductibilité des polynômes cyclotomiques, ex : $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ et est réductible dans $\mathbb{F}_p[X]$, appli : polynôme minimal d'une racine n -ième de l'unité.

Références :

Combes, Algèbre et géométrie.

Perrin, Cours d'algèbre.

Gourdon, Algèbre.

Gozard, Théorie de Galois.

Duverney, Théorie des nombres.

121 : Nombres premiers. Applications.

1 Arithmétique dans $\mathbb{Z}$.

1. Nombres premiers.

- [GOU] def : nombre premier, ex [COM] : 401 est premier (mentionner le critère avec $\sqrt{p}$), prop : l'ensemble des nombres premiers est infini, prop : nombres premiers entre-eux, prop : si p ne divise pas a alors $\text{pgcd}(p, a) = 1$, thm de Bézout, lemme de Gauss, appli [COM] : résolution d'une équation diophantienne, lemme : p premier alors $p \mid \binom{p}{k}$.
- [GOU] remarques sur la répartition des nombres premiers : crible d'Eratosthène - théorème des nombres premiers (ADMIS).

2. Anneaux $\mathbb{Z}/n\mathbb{Z}$.

- [GOU] prop : $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier, thm de Fermat, corollaire de Wilson, c-ex : la réciproque du thm de Fermat est fautive - nombres pseudo-premiers et nombres de Carmichael.
- [COM] prop : Fermat-Euler, ex : chiffre des unités de 27^{1995} , thm chinois, appli : résolution d'un système d'équations diophantienne.

3. Décomposition en facteurs premiers.

- [GOU] thm fondamental de l'arithmétique, remarque : expression du pgcd et du ppcm, appli : infinité de nombres premiers de type $6k - 1$, appli : résolution de $x^2 + y^2 = z^2$.
- [COM] appli : divergence de $\sum 1/p$ (p premier), def-prop : fonction d'Euler (def - multiplicativité - expression en fonction de la décomposition en nombres premiers - $n = \sum_{d|n} \varphi(d)$).
- [GOU] appli : chiffrement RSA.
- [FGN] def-prop : fonction de Möbius (def - multiplicativité - formule d'inversion), appli : polynômes irréductibles sur $\mathbb{F}_q$.

2 Groupes finis.

- [COM] thm de Lagrange, ex : si K et M sont d'ordres k et m avec $k^m = 1$ alors $K \cap M = \{e\}$, def : groupe simple, prop : G est d'ordre premier ssi il est cyclique et simple, coro : si G est d'ordre p^2 avec p premier alors G est abélien, def : p -groupe - p -sous-groupe - p -groupe de Sylow, thm de Sylow, coro : sous-groupe distingué et groupe de Sylow, ex : structure d'un groupe fini d'ordre 153, ex : un groupe d'ordre 56 n'est pas simple.

3 Corps finis.

1. Corps finis et polynômes irréductibles.

- [COM] def : caractéristique, ex : si A est intègre alors sa caractéristique est un nombre premier, ex : calcul d'un inverse via Bezout, appli : morphisme de Frobenius, appli : nombres de Mersenne (cf [GOU]), prop : sous-corps premier, coro : cardinal d'un corps fini, prop : un polynôme P est irréductible ssi $K[X]/P$ est un corps, exemple : $\mathbb{R}[X]/(X^2 + 1)$ est un corps.
- [COM] prop : critère d'Eisenstein, exemples : irréductibilité de $X^n - 2$ - $X^3 - 3X + 1$, thm de réduction pour l'irréductibilité, exemple [PER] : $X^3 + 6X^2 + 5X - 7$ est irréductible, def : polynômes cyclotomiques, prop : formule explicite, exemples,  **appli : irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$** , prop : cas particulier du thm de Dirichlet, rq : énoncé du thm de Dirichlet (ADMIS).

2. Carrés dans $\mathbb{F}_p$.

- [COM et PER] def : résidu quadratique, appli : discriminant d'une forme quadratique à deux valeurs possibles - classification des formes quadratiques, prop : les carrés de $\mathbb{F}_p$, ex : pour $p = 4k + 1$ - 1 est un résidu

quadratique, appli : équation diophantienne $x^2 + y^2 = pz^2$, appli : résolution $5x^2 + 3y^2 = 11 \pmod{13}$.

➤ [PER]  appli : thm des deux carrés.

➤ [DUV] appli : résolution d'une équation diophantienne avec le thm des 2 carrés, def : symbole de Legendre, rq : critère d'Euler, exemples de calculs, coro : multiplicativité du symbole de Legendre, thm : loi de réciprocité quadratique, exemples de calculs, appli : résolution de $x^2 + 7x - 2 = 0 \pmod{31}$.

➤ [GOU] appli : 5 est un carré dans $\mathbb{F}_p$ ssi $p = \pm 1 \pmod{10}$ - infinité de nombre premier de la forme $10n - 1$.

Références :

Combes, Algèbre et géométrie.

Perrin, Cours d'algèbre.

Gourdon, Algèbre.

Francinou - Gianella, Exercices de mathématiques pour l'agrégation.

Duverney, Théorie des nombres.

122 : Anneaux principaux. Exemples et applications.

Les anneaux principaux sont un type d'anneaux commutatifs très important dans la théorie de la divisibilité. En particulier, on va voir que l'on peut étendre deux théorèmes importants concernant l'anneau des entiers relatifs : le théorème de Bézout et la décomposition en facteurs premiers. On veut aussi faire le lien avec l'arithmétique des polynômes et présenter des applications de la principalité, notamment sur la réduction.

Cadre : A est un anneau commutatif unitaire.

1 Anneaux principaux.

1. Idéaux et anneaux principaux.

- [COM] def : idéal premier - anneau principal, rq : un corps est un anneau principal car $\{0\}$ et K sont ses seuls idéaux, exemple : $\mathbb{Z}$ et $K[X]$ sont principaux, c-ex : un sous-anneau d'un anneau principal n'est pas principal a priori - $\mathbb{Z}[X] \subset \mathbb{Q}[X]$, appli : définition du polynôme minimal.
- [FG] : ex : si A principal alors $S^{-1}A$ est principal, csq : $\mathbb{D}$ est un anneau principal.

2. Un exemple fondamental : les anneaux euclidiens.

- [COM] def : anneau euclidien, prop : tout anneau euclidien est principal, ex : $\mathbb{Z}$ avec $|\cdot|$ - $k[X]$ est principal avec le degré.
- [PER] ex : l'anneau des entiers de Gauss $\mathbb{Z}[i]$ est euclidien (description de l'anneau - la "norme" - ses inversibles), c-ex : la réciproque est fautive avec $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$.
- [FG] ex : les séries formelles $k[[X]]$ avec la valuation, décrire ses inversibles et ses idéaux.

2 Arithmétique dans un anneau principal.

1. Divisibilité dans un anneau principal.

- [COM] def (anneau qcq) : a divise b - élément irréductible (ou premier) - éléments premiers entre-eux, rq : traduction en terme d'idéaux, ex : si $b|a$ et $a|b$ alors a et b sont associés.
- [FG] ex : les irréductibles de $k[[X]]$ sont les associés de X .
- [COM] coro : pA est maximal ssi p est irréductible, prop : il existe un ppcm et un pgcd dans un anneau principal, rq : il n'y a pas unicité (ou alors aux inversibles près), coro : relation de Bézout, coro : thm de Bézout, coro : lemme de Gauss, ex : cas d'éléments premiers entre-eux, appli : l'algorithme d'Euclide permet de calculer un pgcd, exemple : relation de Bézout entre 2214 et 522, appli : existence d'une racine multiple dans $\mathbb{C}$, appli : éléments inversibles de A/aA .

2. Caractère factoriel d'un anneau principal.

- [COM] def : anneau factoriel - décomposition en irréductibles, prop : un anneau principal est factoriel, c-ex : la réciproque est fautive avec $\mathbb{Z}[X]$, exemples [PER] : représentants de $\mathbb{Z}$ et de $\mathbb{K}[X]$, coro : diviseurs d'un élément, coro : caractérisation du pgcd et du ppcm, appli : irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$.
- [PER et DUV]  appli : thm des 2 carrés, appli : résolution de $y^2 = x^3 - 2$.
- [COM] ex : décomposition en facteurs irréductibles de $z = 69 + 45i$, ex : un calcul de pgcd, ex : une décomposition en somme de 2 carrés.
- [PER] c-ex : la relation de Bézout dans un anneau factoriel non principal.
- [FG] prop : un anneau factoriel vérifiant Bézout est principal.

3. Théorème Chinois.

- [COM] prop : thm des restes Chinois, coro : dans $\mathbb{Z}/n\mathbb{Z}$, appli : résolution d'un système de congruence, appli : détermination d'un polynôme connaissant ses restes par des divisions euclidiennes.
- [OA] : appli (réduction) : décomposition de $k[u]$ en les facteurs irréductibles du polynôme minimal avec le

lemme Chinois.

► [??] appli : soit $M = D + N$ la décomposition de Dunford de M alors il existe un polynôme P tel que $D = P(M)$ et $P(0) = 0$.

3 Etude de polynômes dans un anneau principal.

1. Motivation : quotients dans les anneaux principaux.

► [COM] prop : p irréductible ssi pA est un idéal maximal ssi pA est un idéal premier ssi A/pA est un corps, ex : $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier, appli : construction du corps $\mathbb{C}$.

► [PER] prop : $A[X]$ est principal ssi A est un corps.

► [GOZ] appli : construction des corps finis, exemples.

2. Polynômes irréductibles : l'outil de la factorialité.

► [COM] def : contenu, lemme de Gauss, exemples, thm : un polynôme est irréductible dans $A[X]$ ssi il est irréductible dans son corps des fractions, exemple, prop : si A est factoriel alors $A[X]$ est factoriel, prop : un polynôme de degré ≤ 3 est irréductible dans $K[X]$ ssi il n'a pas de racines, exemple, c-ex : faux pour des degrés supérieurs, ex : irréductibilité de polynômes avec le critère d'Eisenstein, ex : irréductibilité de polynômes avec le critère de réduction,  **prop : irréductibilité des polynômes cyclotomiques dans $\mathbb{Q}[X]$** , exemples.

123 : Corps finis. Applications.

1 Existence et unicité des corps finis.

1. Caractéristique d'un corps et quelques définitions générales.
 - [COM] def : caractéristique d'un anneau, prop : si A est intègre alors la caractéristique est un nombre premier, prop : morphisme de Frobenius, def : corps - sous-corps, prop : l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier, notation : $\mathbb{F}_p$.
 - [PER] def : extension de corps, exemples, rq : structure d'ev - degré d'une extension, exemples, thm de la base télescopique, exemples, appli [COM] : l'ensemble des nombres algébriques sur K est un sous-corps de L avec $K \subset L$, def : corps de rupture - de décomposition, thm : existence et unicité, exemples.
2. Cardinal d'un corps fini.
 - [PER et COM] prop : si K et L sont des corps finis avec $K \subset L$ et $\dim_K L = n$ alors $|L| = |K|^n$, prop-def : sous-corps premier d'un corps K et description de ce sous-corps, coro : cardinal d'un corps fini, ex : il n'y a pas de corps à 6 éléments, rq : morphisme de Frobenius (c'est un automorphisme dans le cas d'un corps fini - c'est l'identité si le K est le corps premier $\mathbb{F}_p$).
3. Existence et unicité des corps finis.
 - [PER] thm : il existe un corps $\mathbb{K}$ à $q = p^n$ éléments : c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$ - unicité du corps à q éléments à isomorphisme près, notation : $\mathbb{F}_q$.
 - [GOZ] appli : dans un corps fini de caractéristique p chaque élément admet exactement une racine p -ième, appli : petit théorème de Fermat.
 - [??]  appli : dénombrement des matrices diagonalisables de $\mathbb{F}_q$.

2 Polynômes irréductibles sur $\mathbb{F}_p$ et construction des corps finis.

1. Polynômes irréductibles sur $\mathbb{F}_p$.
 - [PER] def : polynôme irréductibles, ex : les $X - a$ sont irréductibles, rq : les polynômes de degré ≤ 3 sont irréductibles ssi ils n'ont pas racines, c-ex : faux pour les degrés supérieurs, ex [COM] : $X^2 + X + 4$ est irréductible dans $\mathbb{F}_7[X]$, ex (par Frobenius) : irréductibilité de $X^p - X - 1$ sur $\mathbb{F}_p$, thm : lien entre irréductibilité et racines dans des extensions, ex : $X^4 + X + 1$ est irréductible dans $\mathbb{F}_2$, appli : irréductibilité des polynômes cyclotomiques sur $\mathbb{Z}$, thm : conservation de l'irréductibilité par extension de corps, ex : $X^3 + X + 1$ est irréductible dans $\mathbb{F}_p$ donc sur $\mathbb{F}_p^n$.
2. Construction des corps finis.
 - [GOZ] thm : si P est un polynôme irréductible sur $\mathbb{F}_p[X]$ alors $\mathbb{F}_p[X]/(P)$ est le corps de rupture de P sur $\mathbb{F}_p$ et son cardinal est $p^{\deg(P)}$, coro : $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ où P est un polynôme irréductible de degré n sur $\mathbb{F}_p$, exemples : construction du corps à 4 éléments - de $\mathbb{F}_8$ et $\mathbb{F}_9$, prop : facteurs irréductibles de $X^{p^n} - X$, coro : il existe un polynôme irréductible de tout degré sur $\mathbb{F}_p$, appli : nombre de polynômes irréductibles de degré 2 et 3 sur $\mathbb{F}_p$.
 - [FG]  appli : dénombrement des polynômes irréductibles sur $\mathbb{F}_q$.

3 Structure des corps finis.

1. Le groupe multiplicatif $\mathbb{F}_q^*$.
 - [PER] thm : le groupe multiplicatif $\mathbb{F}_q^*$ est un groupe cyclique donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.

2. Sous-corps d'un corps fini.

► [GOZ et FG] prop : sous-corps d'un corps fini, corollaire : $\mathbb{F}_q$ est un sous-corps de $\mathbb{F}_{q'}$ ssi q' est une puissance de q , rq : $\mathbb{F}_{p^n}$ peut alors être vu comme un $\mathbb{F}_{p^d}$ -ev de dimension $n|d$, exemples : sous corps de $\mathbb{F}_{2^{20}}$.

3. Clôture algébrique d'un corps fini.

► [GOZ et FG] def : corps algébriquement clos - clôture algébrique, exemple, prop : un corps fini n'est jamais algébriquement clos, prop : la clôture algébrique de $\mathbb{F}_{p^n}$ coïncide avec celle de $\mathbb{F}_p$, rq : il suffit de connaître la clôture algébrique de $\mathbb{F}_p$, prop : $K = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$ est une clôture algébrique de $\mathbb{F}_p$.

4 Carrés dans $\mathbb{F}_q$.

► [COM et PER] def : résidu quadratique, prop : les carrés de $\mathbb{F}_p$, ex : pour $p = 4k + 1 - 1$ est un résidu quadratique, appli : équation diophantienne $x^2 + y^2 = pz^2$, appli : résolution $5x^2 + 3y^2 = 11 \pmod{13}$, ex : $ax^2 + by^2 = 1$ admet toujours au moins une solution dans les corps finis, appli : classification des formes quadratiques sur $\mathbb{F}_q$, appli : thm des deux carrés.

► [DUV] def : symbole de Legendre, rq : critère d'Euler, exemples de calculs, coro : multiplicativité du symbole de Legendre, thm : loi de réciprocité quadratique, exemples de calculs, appli : résolution de $x^2 + 7x - 2 = 0 \pmod{31}$.

► [GOU] appli : 5 est un carré dans $\mathbb{F}_p$ ssi $p = \pm 1 \pmod{10}$ - infinité de nombre premier de la forme $10n - 1$.

Références :

Gozard, Théorie de Galois.

Perrin, Cours d'algèbre.

Francinou - Gianella, Algèbre 1.

Combes, Algèbre et géométrie.

125 : Extension de corps. Exemples et applications.

1 Corps et extension de corps.

- [COM] def : caractéristique d'un anneau, prop : si A est intègre alors la caractéristique est un nombre premier, prop : morphisme de Frobenius, def : corps - sous-corps, prop : l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier, prop : la caractéristique d'un corps est soit 0 soit un nombre premier, def : sous-corps premier, rq [PER] : si K est fini le morphisme de Frobenius est un automorphisme et si K est le corps premier $\mathbb{F}_p$ alors c'est l'identité, coro : le cardinal d'un corps fini est p^m avec p sa caractéristique.
- [PER et COM] def : extension de corps, ex : $\mathbb{R} \subset \mathbb{C}$, def : corps engendré par une partie, ex : extension finie, rq : structure d'espace vectoriel - degré d'une extension - cas des corps finis, thm : base télescopique, exemples : $[\mathbb{C} : \mathbb{R}] = 2$ - $[\mathbb{R} : \mathbb{Q}] = +\infty$.
- [GOZ] prop : $K[X]/(P)$ est un corps ssi P est irréductible - c'est une extension de degré $\deg(P)$ de base $(1, X, X^2, \dots, X^{d-1})$.

2 Adjonction de racines.

- [PER] Objectifs : soit $P \in K[X]$ irréductible. Existe-t'il une extension dans laquelle P admette une racine α ? Existe-t'il une extension dans laquelle P soit décomposé en produit de facteurs de degré 1?

1. Eléments algébriques.

- [PER et COM] : def : élément algébrique, ex : les nombres $\sqrt{2}, i, \sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$, thm : caractérisation si α est algébrique - polynôme minimal - $(1, \alpha, \dots, \alpha^{n-1})$ est une base de $K[\alpha]$ sur K , ex : polynôme minimal de $\sqrt[3]{2}$ irréductible d'après Eisenstein, ex : étude de $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, appli : polynôme minimal en réduction et réduction des endomorphismes symétriques, ex : anneau des entiers de Gauss $\mathbb{Z}[i]$,  **appli : irréductibilité des polynômes cyclotomiques**, coro : si ω est une racine n -ième de l'unité alors $\phi_n(X)$ est le polynôme minimal de ω , ex : $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ et réductible dans $\mathbb{F}_p$ pour tout nombre premier p .

2. Corps de rupture et de décomposition.

- [GOZ] : def : corps de rupture, rq : c'est une extension algébrique de K , thm : existence et unicité du corps de rupture à isomorphisme près, ex : $\mathbb{F}_p[X]/(P)$ est le corps de rupture de P sur $\mathbb{F}_p$, appli : construction du corps $\mathbb{C}$, appli : construction du corps à 4 éléments.
- [PER] : c-ex : $P(X) = X^3 - 2$ possède une racine dans $L = \mathbb{Q}(\sqrt[3]{2})$ mais pas toutes ses racines.
- [GOZ] def : corps de décomposition d'un polynôme, rq : c'est une extension algébrique, ex : $\mathbb{C}$ est un corps de décomposition pour $X^2 + 1$ thm : existence et unicité du corps de décomposition à isomorphisme près.
- [PER] ex : dans $\mathbb{Q}$ corps de décomposition de $P(X) = X^3 - 2$ et de $P(X) = X^4 - 2$, appli : il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_p$ - existence et unicité des corps finis, ex : irréductibilité de $X^p - X - 1$ sur $\mathbb{F}_p$.
- [FG]  **appli : polynômes irréductibles de $\mathbb{F}_q$.**

3. Clôture algébrique.

- [GOZ] def-prop : corps algébriquement clos, ex : $\mathbb{Q}$ n'est pas algébriquement clos, prop : tout corps algébriquement clos est infini, thm : d'Alembert-Gauss, def : clôture algébrique, ex : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.
- [PER] : ex : clôture algébrique de $\mathbb{F}_p$.
- [GOZ] corollaire : polynômes irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$, thm (Steinitz) (ADMIS) : unicité de la clôture algébrique à isomorphisme près.

Références :

Gozard, Théorie de Galois.

Combes, Algèbre et géométrie.

Perrin, Cours d'algèbre.

Francinou - Gianella, Exercice pour l'agrégation Algèbre 1.

126 : Exemples d'équations diophantiennes.

► [DUV] def : équation diophantienne.

1 Quelques méthodes pratiques d'arithmétique et d'algèbre linéaire.

1. L'équation $ax + by = c$.

► [COM] rq : $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau - groupe des inversibles, appli : critères de divisibilité, thm de Bezout, lemme de Gauss, appli : résolution de $ax + by = c$, ex : résolution de $522x + 2214y = 36$, appli (utilisation des formules de Cramer) : résolution d'un système de congruences.

2. Equation de degré 1 en n variables.

► [BER p.248] prop : résolution de $a_1x_1 + \dots + a_nx_n = b$, exemple : $3x + 4y + 7z = b$.

► [GOU]  thm de Carathéodory et système diophantien.

3. Méthode de la réduction modulaire.

► [COM] thm chinois, appli : résolution d'un système de congruence via l'algorithme d'Euclide, ex : résolution d'un système de congruence de trois équations, expliquer le principe de la réduction modulaire, ex : les triplets pythagoricien (2 n'est pas un carré modulo 4).

4. Méthode de la descente infinie.

► [COM] principe de la méthode, exemples qui n'ont pas de solutions non triviales comme $x^4 + y^4 = z^2$ - $x^4 + y^4 = z^4$.

2 Utilisation de résidus quadratiques.

► [COM] def : résidu quadratique, appli : discriminant d'une forme quadratique sur un corps fini admet deux valeurs possibles, prop : caractérisation des carrés dans $\mathbb{F}_p$.

► [PER] appli : classification des formes quadratiques.

► [DUV] def : symbole de Legendre, rq : critère d'Euler, exemples de calculs, coro : multiplicativité du symbole de Legendre, thm : loi de réciprocité quadratique, exemples de calculs, appli : résolution de $x^2 + 7x - 2 = 0 \pmod{31}$.

► [COM] appli : $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p$, ex : résolution de $5x^2 + 3y^2 = 1 \pmod{13}$.

3 Utilisation d'un corps de nombres quadratiques.

► [COM] rq : on se place dans $\mathbb{Q}(\sigma)$ avec σ une racine dans $\mathbb{C}$ de $X^2 - d$ avec $d \in \mathbb{Z} - \{0, 1\}$ sans facteurs carrés - écriture de $\mathbb{Q}(\sigma)$ avec une base, def : conjugué - norme, notation : les entiers de $\mathbb{Q}(\sigma)$ - c'est un anneau, prop : caractérisation des entiers de $\mathbb{Q}(\sigma)$, thm : cns pour que la norme soit un stathme euclidien.

► [PER] ex : les entiers de Gauss - les unités - les irréductibles, appli :  thm des 2 carrés + [DUV] csq : critère en fonction de la décomposition en produit de facteurs premiers d'un entier, ex [DUV] : résolution de $585 = a^2 + b^2$.

► [DUV] ex : résolution de d'équations de Mordell $y^2 = x^3 - 1$ - $y^2 = x^3 - 2$ - $y^2 = x^3 - 11$.

4 Méthode géométrique : paramétrisation rationnelle du cercle.

► [COM] rq : paramétrisation rationnelle du cercle, ex : résolution de $x^2 + y^2 = z^2$, appli : les équations diophantiennes $x^4 + y^4 = z^2$ et $x^4 + y^4 = z^4$ n'ont pas de solutions non-triviales, rq : méthode de descente infinie de Fermat, ex : résolution de $x^2 + y^2 = pz^2$, appli : généralisation aux courbes planes d'équations $p(x, y, 1) = 0$ qui possèdent un bon paramétrage rationnel, ex (folium de Descartes) : $x^3 + y^3 = xyz$.

Références :

Combes, Algèbre et géométrie.

Duverney, Théorie des nombres.

Perrin, Cours d'algèbre.

Berhuy, Modules : théorie, pratique et un peu d'arithmétique.

Gourdon, Algèbre.

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

Cadre : A est un anneau intègre si rien n'est précisé.

1 Polynômes irréductibles.

1. Irréductibilité.

- [PER] def irréductibilité.
- [GOZ] def : racine-multiplicité-polynôme scindé, prop : irréductibilité des polynômes de $k[X]$ (polynôme de degré 1 irréductible, tout polynôme irréductible de degré > 1 n'a pas de racine dans k , les polynômes de degré 2 ou 3 dans $k[X]$ sont exactement les polynômes qui n'ont pas de racines dans k), c-ex : un polynôme qui n'a pas de racine n'est pas forcément irréductible $(X^2 + 1)^2$ dans $\mathbb{Q}[X]$.
- [COM] thm : $\frac{k[X]}{(P)}$ est un corps $\Leftrightarrow P$ irréductible.
- [OA] c-ex : dans $\mathbb{Z}[X]$ $X^2 + 1$ inversible mais $\mathbb{Z}[X]/(X^2 + 1)$ pas un corps.

2. Factorialité.

- [COM] thm : un polynôme de contenu 1 est irréductible dans $A[X]$ ssi il est irréductible dans $\text{Frac}(A)[X]$, exemple, prop : si A est factoriel alors $A[X]$ aussi, exemple, prop : critère d'irréductibilité de Eisenstein, exemples avec et sans changement de variable, prop : réduction et irréductibilité, exemples.

3. Polynômes cyclotomiques.

- [COM] def : polynôme cyclotomique d'indice n - son degré est $\phi(n)$, exemples, prop : un polynôme cyclotomique est unitaire à coefficients entiers - formule explicite des polynômes cyclotomiques, exemple : pour n impair $\phi_{2n}(X) = \phi_n(-X)$,  thm : **irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$** , coro : si ω est une racine n -ième de l'unité alors $\phi_n(X)$ est le polynôme minimal de ω , ex : $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ et réductible dans $\mathbb{F}_p$ pour tout nombre premier p .

2 Adjonction de racines.

► [PER] Objectifs : soit $P \in K[X]$ irréductible. Existe-t'il une extension dans laquelle P admette une racine a ? Existe-t'il une extension dans laquelle P soit décomposé en produit de facteurs de degré 1 ?

1. Élément algébrique et polynôme minimal.

- [COM] def : élément algébrique, thm : caractérisation d'un élément algébrique (polynôme minimal - degré - base), corollaires, appli : algèbre linéaire et polynôme minimal, thm : base télescopique, ex : étude de $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, ex : $X^4 - 2X^2 + 9$ est irréductible dans $\mathbb{Q}[X]$.

2. Corps de rupture.

- [GOZ] def : corps de rupture, rq : c'est une extension algébrique de K , thm : existence et unicité du corps de rupture à isomorphisme près, appli : construction du corps $\mathbb{C}$, coro : si $P \in K[X]$ alors il existe une extension algébrique monogène de K tel que P possède au moins une racine, appli : construction du corps à 4 éléments.
- [PER] [SI POSSIBLE] thm : P est irréductible sur k ssi P n'a pas de racines dans les extensions K de k vérifiant $[K : k] \leq n/2$, ex : $X^4 + X + 1$ est irréductible dans $\mathbb{F}_2$, thm : conservation de l'irréductibilité par extension de corps, c-ex : sans l'hypothèse m et n premiers entre-eux avec $X^4 + 1$ irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{Q}(i)$, ex : $X^3 + X + 1$ irréductible que $\mathbb{Q}(i)$ comme sur $\mathbb{Q}$, rq : $P(X) = X^3 - 2$ possède une racine dans $L = \mathbb{Q}(\sqrt[3]{2})$ mais pas toutes ses racines...

3. Corps de décomposition.

- [GOZ] def : corps de décomposition d'un polynôme, rq : c'est une extension algébrique, ex : $\mathbb{C}$ est un corps de décomposition pour $X^2 + 1$ thm : existence et unicité du corps de décomposition à isomorphisme près.

-
- [PER] ex : dans $\mathbb{Q}$ corps de décomposition de $P(X) = X^3 - 2$ et de $P(X) = X^4 - 2$.
 - [PER] appli : existence et unicité des corps finis, ex : irréductibilité de $X^p - X - 1$ sur $\mathbb{F}_p$.
 - [FG]  appli : dénombrement des polynômes irréductibles sur $\mathbb{F}_q$.

4. Clôture algébrique.

- [GOZ] def-prop : corps algébriquement clos, ex : $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos, prop : tout corps algébriquement clos est infini, thm : d'Alembert-Gauss, def : clôture algébrique, ex : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.
- [PER] ex : clôture algébrique de $\mathbb{F}_p$.
- [GOZ] corollaire : polynômes irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

Références :

Perrin, Cours d'algèbre.

Combes, Algèbre et géométrie.

Francinou - Gianella, Exercices de mathématiques pour l'agrégation, Algèbre 1.

Gozard, Théorie de Galois.

142 : Algèbre des polynômes à plusieurs indéterminées. Applications.

Cadre : A est un anneau commutatif unitaire et K un corps.

1 Polynômes à plusieurs indéterminées.

1. L'algèbre $A[X_1, \dots, X_n]$.

- [RDO] def : multi-indice, def : polynômes à n indéterminées, def-prop : les opérations, prop : $A[X_1, \dots, X_n]$ est une algèbre, rq : écriture de P comme combinaisons linéaires de $(X_1^{i_1}, \dots, X_n^{i_n})$, thm : isomorphisme canonique, appli : transfert du caractère intègre.
- [???] ex : le déterminant - la trace sont des polynômes à plusieurs indéterminées.

2. Degrés et polynômes homogènes.

- [RDO] def : degré partiel et conventions, def : degré total, propriétés du degré total, rq : cas intègre, exemple [???], def : polynômes homogènes, ex : degré total pour un polynôme p -homogène, prop : un produit de polynômes homogènes est homogène, ex : degré du produit pour un anneau intègre, ex [???] : classification des polynômes homogènes de degré ≤ 2 (deg 0 : constante - deg 1 : forme linéaire - deg 2 : forme quadratique), def : polynôme dérivé partiel, exemple, thm d'Euler.

3. Action de $\mathfrak{S}_n$ sur $A[X_1, \dots, X_n]$.

- [RDO] def : l'action de $\mathfrak{S}_n$ sur $A[X_1, \dots, X_n]$, ex : si P homogène alors $\sigma(P)$ est homogène, def : polynôme symétrique, rq : il suffit de vérifier l'invariance pour les transpositions, thm-def : polynômes symétriques élémentaires (ils sont homogènes), notations, exemple, prop : lien entre P et les polynômes symétriques élémentaires, appli : relation racines coefficient dans $A[X]$, def : poids d'un monôme - ordre d'un polynôme symétrique, thm de structure : existence d'un polynôme Q en les polynômes élémentaires symétriques égal à P en fonction du poids et du degré, ex : détail de l'algorithme sur un exemple, thm-def : formule de Newton, exemple.
- [???]  appli : thm de Kronecker.
- [GOU] appli : algorithme de Faddev.

2 Arithmétique dans $A[X_1, \dots, X_n]$ avec K commutatif.

- [RDO] rq : intégrité de $K[X_1, \dots, X_n]$ - absence de division euclidienne (anneau non euclidien), prop : divisibilité par $X_n - B$, exemple, corollaire : divisibilité par le produit, thm : absence du caractère principal pour $n \geq 2$ - caractère factoriel, conséquences : décomposition en produit de polynômes irréductibles - existence du PGCD et PPCM - thm de Gauss - le théorème de Bézout est faux.
- [PER] appli : irréductibilité de polynômes via le caractère factoriel (critère d'Eisenstein - critère de réduction), ex (application de Gauss) : irréductibilité de polynômes dans $k[X, Y]$, ex (critère d'Eisenstein) : irréductibilité de $Y^2 - X(X-1)(X-2)$, ex (réduction) : $X^2 + Y^2 + 1$ est irréductible dans $\mathbb{R}[X]$, ex : $\mathbb{C}[X, Y]/(Y - X^2)$ est principal.

3 Fonctions polynômes.

- [RDO] def : fonction polynômes de n variables, thm : identification entre fonction polynôme et un polynôme à n indéterminés.
- [GOB] def : identité entre m polynômes, exemple : $(X + Y)^p$ dans $\mathbb{Z}[X, Y]$ et dans $\mathbb{F}_p[X, Y]$, prop : prolongement des identités, appli : si $M, N \in M_n(K)$ alors $\chi(MN) = \chi(NM)$, prop : dans $\mathbb{R}$ ou $\mathbb{C}$, appli [???] : thm de Caley-Hamilton.
- [GRI] appli : une forme quadratique est une fonction polynôme d'un polynôme 2-homogène - thm d'inertie de Sylvester - classification des formes quadratiques en dimension 2 et 3 par leur signature - annexe (dessins).

Références :

Ramis - Deschamps - Odoux, Cours de mathématiques spéciale : Algèbre 1.

Goblot, Algèbre commutative.

Perrin, Cours d'algèbre.

Grifone, Algèbre linéaire.

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

1 Structure de $K[X]$.

1. Racines d'un polynôme.

- [GOU] def : racine d'un polynôme, prop : relation de divisibilité, def : ordre d'une racine, thm : ordre d'une racine et dérivé d'un polynôme en caractéristique zéro, c-ex : c'est faux en caractéristique non nulle, rq : le thm reste vrai pour les racines simples, appli (localisation des racines de P') : thm de Gauss-Lucas, prop : sur un corps un polynôme de degré n admet au plus n racines, c-ex : faux sur un anneau, appli : polynôme interpolateur de Lagrange, prop : si K est infini et $\forall x \in K \ P(x) = 0$ alors $P = 0$, c-ex : faux sur les corps finis, rq : on a alors une bijection entre $K[X]$ et les fonctions polynômes de K dans K , def : polynôme scindé.
- [OA] appli : les racines dépendent localement de façon C^∞ du polynôme, appli : l'ensemble des polynômes scindés à racines simples est un ouvert de $\mathbb{R}_n[X]$.
- [FG] appli : continuité des racines de polynômes.
- [GOU] appli (réduction des matrices) : les valeurs propres d'un endomorphisme sont les racines de son polynôme caractéristique, ex : matrice compagnon et polynôme caractéristique.

2. Irréductibilité de polynômes.

- [COM] def : polynôme irréductible, ex : les polynômes de degré 1 sont irréductibles - polynôme de degré 2 ou 3 irréductible ssi il n'a pas de racines dans K , c-ex : faux pour les degrés supérieurs, thm : un polynôme est irréductible dans $A[X]$ ssi il est irréductible dans $\text{Frac}(A)[X]$, ex : $X^3 - 2X + 3/4$ est irréductible dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$, prop : critère d'Eisenstein, exemple : avec et sans changement de variables, critère de réduction, exemple, exemple : irréductibilité des polynômes cyclotomiques, ex : $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ mais réductible dans $\mathbb{F}_p[X]$.
- [PER] prop : conservation de l'irréductibilité par extension de corps, exemple.
- [GOU et GOZ] thm de d'Alembert-Gauss, ex : irréductible de $\mathbb{R}[X]$ et $\mathbb{C}[X]$, appli : toute matrice de $M_n(\mathbb{C})$ est trigonalisable.

2 Polynômes symétriques et fonctions symétriques élémentaires.

1. Relation coefficients-racines.

- [RDO] prop : action de $\mathfrak{S}_n$ sur $A[X_1, \dots, X_n]$, def : polynôme symétrique, rq : il suffit de vérifier l'égalité pour une transposition, def : polynôme symétrique élémentaire, prop : expression d'un polynôme en fonction des Σ_p .
- [GOU] ex : polynômes symétriques, ex : polynômes symétriques élémentaires.
- [RDO] thm : relation coefficients-racines, rq : on n'a pas de réciproque.
- [GOU] thm : formules de Newton, application : algorithme de Faddeev.

2. Structure des polynômes symétriques.

- [RDO] def : poids d'un monôme, thm : structure des polynômes symétriques, méthode de Waring (algorithme de symétrisation), exemples,  appli : thm de Kronecker.

3 Adjonction de racines.

1. Nombres algébriques.

- [COM] def : élément algébrique, prop : caractérisations de $K(\alpha)$, coro : structure d'espace vectoriel - dimension de $K(\alpha)$ sur K , coro : un polynôme annulateur de α - unitaire et irréductible est le polynôme annulateur

de α , appli (algèbre linéaire) : polynôme minimal et réduction des endomorphismes symétriques, thm de la base télescopique, appli : l'ensemble des éléments algébriques de $L \subset K$ sur K est un sous-corps de L , ex : $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, ex : irréductibilité dans $\mathbb{Q}[X]$ de $X^4 - 2X^2 + 9$.

2. Corps de rupture et de décomposition.

- [PER et GOZ] def - prop : existence et unicité du corps de rupture, ex : construction de $\mathbb{C}$ et $\mathbb{F}_4$, def - prop : existence et unicité du corps de décomposition, exemple : $\mathbb{Q}(\sqrt{2})$, ex [COM] : corps de décomposition dans $\mathbb{C}$ de $X^5 - 7$, appli : construction - existence - unicité des corps finis, def : corps algébriquement clos, c-ex : $\mathbb{Q} - \mathbb{R}$ et les corps finis ne sont pas algébriquement clos, rq : existence d'une clôture algébrique pour tout corps.
- [FG] 🍷 appli : dénombrement des polynômes irréductibles sur $\mathbb{F}_q$.

Références :

Combes, Algèbre et géométrie.

Gourdon, Algèbre.

Ramis - Deschamps - Odoux, Algèbre 1.

Perrin, Cours d'algèbre.

Gozard, Théorie de Galois.

Francinoux - Gianella, Exercices d'algèbre pour l'agrégation.

Objectif Agrégation.

150 : Exemples d'actions de groupes sur les espaces de matrices.

1 Choix d'un système de représentants : l'exemple de l'action par translation.

1. L'action par translation [A REDUIRE].

- [H2G2] def : action de groupe à gauche, def : l'action par translation de $GL_n(\mathbb{R}) \times M_n(\mathbb{R}) \longrightarrow M_n(\mathbb{R}) - (P, A) \mapsto PA$, def : invariant et invariant complet d'une action, c-ex : le rang est un invariant qui n'est pas complet, prop : une matrice est inversible ssi Id est dans l'orbite pour l'action par translation, def : représentants et système de représentants, def : stabilisateur, thm : diagramme commutatif (relation orbites-stabilisateur), rq : cas fini (égalité des cardinaux), rq : ce n'est pas un isomorphisme en général.
- [MT] appli : la décomposition polaire via une action de groupe (si $\phi : O_n \times M_n \mapsto M_n$, $(O, M) \mapsto M^t O$ alors chaque orbite contient une matrice $S \in S_n^+$; de plus, si $M \in GL_n$ alors $\exists ! S \in S_n^{++}$ dans l'orbite de M - corollaire : $GL_n \sim O_n \times S_n^{++}$).

2. Pertinence du système de représentants : l'exemple du pivot de Gauss.

- [H2G2] def : pivot - matrice échelonnée en ligne - matrice échelonnée réduite, ex : matrice échelonnée réduite, thm : toute matrice est dans l'orbite d'une matrice échelonnée réduite, rq : cette matrice s'obtient par la méthode du pivot de Gauss en multipliant à gauche par des matrices inversibles correspondant à des opérations élémentaires (cf annexe : dilatation-transvection-permutation et leur effet sur les lignes), rq : c'est l'invariant de l'action par translation, prop : un système de représentants est l'ensemble des matrices échelonnées réduites, appli : calcul du rang, de l'inverse d'une matrice.
- [GRI] appli (résolution de système linéaire) : factorisation LU d'une matrice, exemple de décomposition.

2 Description des orbites : l'exemple de l'action par conjugaison et par équivalence.

1. Réduction d'endomorphisme.

- [H2G2] def : action par conjugaison - $(P, M) \mapsto PMP^{-1}$, prop : deux matrices sont semblables ssi elles sont dans la même orbite, csq : classifier les endomorphismes revient à classifier les orbites pour cette action, ex : le déterminant - le polynôme minimal - le polynôme caractéristique - le spectre sont des invariants, prop : caractérisation de la diagonalisabilité (une matrice est dz ssi elle est dans la même orbite qu'une matrice diagonale), prop : pour l'action restreinte $GL_n(\mathbb{C}) \curvearrowright D_n(\mathbb{C})$ le polynôme caractéristique est un invariant complet et un système de représentants est donné par l'ensemble des matrices diagonales, c-ex : le polynôme minimal n'est pas un invariant complet.
- [GRI] appli : résolution d'un système de suites récurrentes.
- [GOU] appli : g est diagonalisable ssi $\Phi = \{\varphi^{-1}g\varphi, g \in Gl(E)\}$ est fermé, prop : densité des matrices diagonalisables dans $M_n(\mathbb{C})$, c-ex : faux dans $M_n(\mathbb{R})$, appli : thm de Cayley-Hamilton.
- [???]  **thm : dénombrement des matrices diagonalisables dans $\mathbb{F}_q$.**

2. Rang d'une matrice.

- [H2G2] def : action par équivalence - $GL_m(\mathbb{R}) \times GL_n(\mathbb{R}) \times M_{mn}(\mathbb{R}) \rightarrow M_{mn}(\mathbb{R}) - ((P, Q), A) \mapsto PAQ^{-1}$, thm du rang (via les actions de groupes), prop : le rang est un invariant complet et un système de représentants est l'ensemble des $(J_r)_{1 \leq r \leq \min(n, m)}$, appli : cardinal de $GL_d(\mathbb{F}_q)$ et celui des matrices de rang r .
- [GOU] appli : l'ensemble des matrices de rang inférieur à p est un fermé de $M_n(\mathbb{R})$ - adhérence de l'ensemble des matrices de rang p .

3 Etude des stabilisateurs : l'exemple d'une action infidèle, l'action par congruence.

Cadre : dans cette partie, la caractéristique du corps est différente de 2.

1. Action sur $S_n(\mathbb{K})$: réduction des formes quadratiques.
 - [H2G2 et GRI] def : action par congruence, rq : deux matrices sont congruentes ssi elles sont les matrices de la même forme quadratique dans des bases différentes.
 - [XENS]  appli : **connexité et forme quadratique réelle.**
 - [H2G2 et GRI] def : discriminant, prop : c'est un invariant, def : base orthogonale, thm : existence d'une base orthogonale, algorithme de Gauss (réduction des formes quadratiques), exemple de réduction, classification sur $\mathbb{C}$: invariants (le rang) et représentants, classification sur $\mathbb{R}$: invariants (la signature) et représentants (thm de Sylvester), classification sur $\mathbb{F}_q$: invariants (avec le discriminant) et représentants.
2. Etude d'un stabilisateur : le groupe orthogonal.
 - [H2G2] def : groupe orthogonal $O_n(\mathbb{R})$ d'une forme quadratique Q comme le stabilisateur de I_n pour l'action par congruence.
 - [GRI] ex : description de $O_2(\mathbb{R})$ - dessins en ANNEXE, appli : angle non orienté et orienté en dimension 2, thm : réduction des endomorphismes orthogonaux, ex : description de $O_3(\mathbb{R})$ - dessins en ANNEXE, exemple.
 - [MT] prop : $SO_n(\mathbb{R})$ est un ouvert connexe - $O_n(\mathbb{R})$ possède 2 composantes connexes.
 - [H2G2] prop : $O_n(\mathbb{R})$ et $SO_n(\mathbb{R})$ sont compacts.
 - [PER] def : réflexion et retournement, prop : $O(E)$ est engendré par les réflexions - $SO(E)$ par les retournements.

Références :

Caldero - Germoni, Histoire hédonistes de groupes et de géométries.

Mneimné - Testard, Groupes de Lie classiques.

Gourdon, Algèbre.

Grifonne, Algèbre linéaire.

Oraux X-ENS, Algèbre 3.

151 : Dimension d'un espace vectoriel (cas fini). Rang. Exemples et applications.

1 Familles de vecteurs d'un espace vectoriel.

1. Familles génératrices et familles libres.

- [GRI] def : famille génératrice, ex : $(1, 1)$ et $(1, -1)$ est une famille génératrice de $\mathbb{R}^2$, prop : toute famille contenant une famille génératrice est génératrice, def : espace vectoriel de dimension finie, def : famille libre - liée, ex de vecteurs libres, rq : def équivalente pour la liberté, prop : toute sous-famille d'une famille libre est libre - toute famille contenant une famille liée est liée - toute famille dont l'un des vecteurs est nul est liée, def : base, ex : base canonique de $\mathbb{R}_n[X]$, thm : existence de base, thm de la base incomplète.
- [??] appli : dans un $\mathbb{C}$ -ev de dimension finie un endomorphisme u est diagonalisable ssi tout sev stable par u admet un supplémentaire stable par u .

Tous les ev seront supposés finis.

2. Dimension.

- [GRI] thm-def : toutes les bases ont même cardinal - dimension, ex : dimension de $M_{p,n}(\mathbb{K}) = pn$, coro : dans un ev de dimension n toute famille ayant plus/moins de n éléments est/n'est pas liée/génératrice, rq : la dimension dépend de E et du corps de base, ex : $\dim_{\mathbb{C}}(\mathbb{C}) = 1$ et $\dim_{\mathbb{R}}(\mathbb{C}) = 2$, ex : un sev de dimension finie peut être de dimension finie, thm : toute famille génératrice ayant n éléments est une base - toute famille libre de n éléments est une base, prop : dimension d'un produit d'espaces, prop : dimension d'un sev, prop-def : somme directe, prop : somme directe et bases, def : sev supplémentaires, coro : existence d'un supplémentaire, rq : en dimension finie avec les dimensions, ex : dans $\mathbb{R}^2$ - dans $M_2(\mathbb{R})$, prop : Grassman, appli : dimension de l'espace vectoriel des suites vérifiant une relation de récurrence d'ordre 2, appli : dimension de l'espace de solutions d'équa diff linéaires à coefficients constants.

3. Algorithme de Gauss et rang d'une famille de vecteurs.

- [GRI] thm : opérations élémentaire sur une famille de vecteurs, rq : représentation matricielle, def : matrice échelonnée - pivot.
- [XENS]  appli : **générateurs du groupe linéaire et applications.**
- [GRI] prop : les vecteurs lignes d'une matrice et les vecteurs lignes de sa réduite échelonnée engendrent le même espace vectoriel, ex : matrice échelonnée et pivot, thm : les lignes non nulles de la matrice échelonnée réduite donne une base, def : rang d'une famille de vecteurs, exemple, appli : résoudre un système linéaire - extraire une base d'une famille génératrice - compléter une famille libre en une base - détermination d'un supplémentaire, ex : système d'équation, ex : base de $F + G$.

2 Applications linéaires entre espaces de dimensions finies.

1. Rang d'une application linéaire.

- [GRI] prop : l'image d'une famille libre par une application injective est une famille libre - cas d'une famille génératrice et d'une base, thm : deux ev sont isomorphes ssi ils ont même dimension, rq : il n'y a pas d'isomorphisme canonique, def : rang de f , thm du rang, ex : cas des projecteurs, appli : noyaux itérés et quelques conséquences, thm equivalence de l'injection-surjection-bijection d'une application linéaire.
- [DEM] appli : polynômes interpolateurs de Lagrange.
- [GRI] def : forme linéaire, prop-def : hyperplan, ex : l'espace des solutions d'un système d'équations linéaires peut être vu comme une intersection d'hyperplans.
- [GOU] appli : thm des extrema liés.
- [GRI] def : espace dual, prop : $\dim(E) = \dim(E^*)$, thm : base duale, ex de base duale, def : biduale, prop : isomorphisme entre E et E^{**} .
- [XENS] ex : dual de $M_n(K)$, application : enveloppe convexe de $O_n(\mathbb{R})$.

► [GOU]  appli : réduction de Frobenius.

2. Ecriture matricielle.

► [GRI] def : matrice d'une application linéaire, thm : isomorphisme entre les applications linéaires et l'espace des matrices, ex : matrice d'une projection - matrice de rotation, rq : structure d'anneau sur $M_n(K)$, prop : f est bijective ssi $M(f)$ est inversible, def : matrice de passage prop : changement de base sur un vecteur, exemple, changement de base d'une application linéaire - cas particulier, rq : matrice semblable, exemple, def : rang d'une matrice, prop : deux matrices qui représentent la même application linéaire dans des bases différentes ont même rang, rq : ajouter que inversible équivaut à rang n , ex : par l'algo de Gauss $\text{rg}({}^t A) = \text{rg}(A)$.

► [???]  appli : thm de Carathéodory et résolution d'équations diophantiennes.

3. Rang et déterminant.

► [GRI] rq : toutes les propriétés des déterminants relatives aux colonnes sont vraies pour les lignes, thm : base et déterminant, exemple, def : mineur, exemple, thm : liberté d'une famille et mineur, exemple, thm : le rang d'une matrice est l'ordre maximal des mineurs non nuls extraits de A , def : système de Cramer, thm de Cramer (existence et unicité d'une solution), thm de Rouché-Fontené, exemple.

3 Nombres algébriques.

► [COM] def : élément algébrique, ex : les nombres $\sqrt{2}, i, \sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$, thm : caractérisation si α est algébrique - polynôme minimal - $(1, \alpha, \dots, \alpha^{n-1})$ est une base de $K[\alpha]$ sur K , ex : polynôme minimal de $\sqrt[n]{2}$ irréductible d'après Eisenstein, ex : étude de $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, appli : polynôme minimal en réduction et réduction des endomorphismes symétriques, ex : anneau des entiers de Gauss $\mathbb{Z}[i]$, appli : irréductibilité des polynômes cyclotomiques, coro : si ω est une racine n -ième de l'unité alors $\phi_n(X)$ est le polynôme minimal de ω , ex : $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ et réductible dans $\mathbb{F}_p$ pour tout nombre premier p .

Références :

Grifone, Algèbre linéaire.

Perrin, Cours d'algèbre.

Gozard, Théorie de Galois.

Demailly, Analyse numérique.

Gourdon, Algèbre.

Combes, Algèbre et géométrie.

152 : Déterminant. Exemples et applications.

1 Définitions du déterminant.

1. Déterminant d'une famille de vecteurs.

- [GOU] def : application p -linéaire - forme p -linéaire sur E - notations : $\mathcal{L}(E_1, \dots, E_p, F)$ et $\mathcal{L}_p(E, K)$, exemples, prop : dimension de $\mathcal{L}_p(E, K)$, thm : l'ensemble des formes n -linéaires alternées sur un espace de dim n est un ev de dimension 1, def : déterminant d'une famille de vecteurs, ex : $f_u = \text{tr}(u)f$.
- [GRI] appli (théorie du rang) : caractérisation des bases.
- [ROU]  appli : thm de extrema liés et inégalité de Hadamard.

2. Déterminant d'une matrice et d'un endomorphisme.

- [GOU] def : déterminant d'une matrice.
- [GRI] ex : cas $n = 3$ - formule de Sarrus.
- [GOU] prop : déterminant par blocs, propriétés : det et trace - inversibilité d'une matrice et déterminant - $\det(AB) = \det(BA)$ - $\det(AB) = \det(A)\det(B)$ pour $A, B \in M_n(K)$ - deux matrices semblables ont même déterminant.
- [GRI] def : det d'un endomorphisme, ex : det d'une symétrie par rapport à un plan parallèlement à une droite.
- [PEY]  prop : calcul du déterminant circulant par la transformée de Fourier discrète.

3. Interprétation géométrique du déterminant.

- [GRI] thm : le volume du parallélépipède engendré par $v_1, \dots, v_n$ est $|\det(v_1, \dots, v_n)|$, ex : en dimension 2 - dessin du parallélogramme, ex : aire d'un triangle.
- [GOU] thm : inégalité d'Hadamard (majoration du volume), ex : majoration d'un déterminant, def : matrice de Gram, appli : matrice de Gram et distance à un sev.
- [OA] appli : thm de changement de variables dans une intégrale.
- [GOU] exemple : passage en coordonnées polaires dans le plan et calcul de $\int_{\mathbb{R}} e^{-x^2} dx$.

2 Calculs de déterminants.

1. Pivot de Gauss ; mineurs et cofacteurs.

- [GOU] prop : déterminant par blocs (cas triangulaire), ex : $\det(\exp(A)) = \exp(\text{tr}(A))$, appli : déterminant d'une matrice définie par blocs, rq : csq d'une permutation sur les colonnes ou les lignes - ajout d'une combinaison linéaire des autres colonnes, exemple : pivot de Gauss pour le calcul d'un déterminant, def : mineurs - cofacteurs - comatrice, prop : développement selon une ligne ou une colonne, ex : déterminant de Vandermonde, appli : si $\text{tr}(u^p) = 0$ alors u est nilpotente, ex : déterminant de Cauchy, appli (Cauchy + Gram) : minimisation de $\int_0^1 (1 + a_1x + \dots + a_nx^n)^2 dx$.
- [GRI] exemple : inverse avec la comatrice, appli (théorie du rang) : détermination du rang d'une matrice, exemple.

2. Résolution de systèmes linéaires.

- [GRI] def : système de Cramer - expression matricielle - expression vectorielle, thm de Cramer, exemple.

3. Le polynôme caractéristique.

- [???] $K[X]$ est un anneau intègre donc se plonge dans son corps des fractions $K(X)$ et la def du déterminant assure que $\forall M \in M_n(K[X]) \quad \det(M) \in K[X]$.
- [GOU] prop : polynômes caractéristiques et valeurs propres d'un endomorphisme, rq : $\chi_A(0) = \det(A)$, exemple, ex : polynôme caractéristique de la matrice compagnon, appli : thm de Cayley Hamilton.

3 Régularité du déterminant.

- [GOU ana] prop : l'application $\det$ est $\mathcal{C}^\infty$.
- [GOU et OA] appli (continuité du $\det$) : $GL_n(K)$ est un ouvert dense dans $M_n(K)$, appli (caractère polynomial du $\det$) : deux matrices réelles semblables dans $\mathbb{C}$ sont semblables dans $\mathbb{R}$, appli : surjectivité de l'exponentielle.
- [ROU] prop : différentielle du déterminant, appli : dérivée du wronskien.

Références :

Gourdon, Algèbre.

Grifone, Algèbre linéaire.

Gourdon, Analyse.

Objectif agrégation.

Peyre, Transformée de Fourier discrète.

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

1 L'algèbre des polynômes d'endomorphisme $\mathbb{K}[u]$.

1. L'algèbre $\mathbb{K}[u]$ et polynôme minimal.
 - [OA et COG] notation du polynôme d'endo (cf [GOU]), def du morphisme d'évaluation et de $K[u]$, prop : $K[u]$ est une sous-algèbre commutative de $\mathcal{L}(E)$, def du polynôme minimal π_u , def : P polynôme annulateur de u , rq : $\pi_u | P$, appli [GOU] : si $P(u) = 0$ et $P(0) \neq 0$ alors u est inversible et $u^{-1} \in K[u]$.
 - [MX] appli : calcul d'une inverse de matrice avec un polynôme annulateur.
 - [COG] $K[u]$ est une sous-algèbre de $\mathcal{L}(E)$ de dimension $\deg(\pi_u)$ et de base $(id, u, \dots, u^{\deg(\pi_u)-1})$, appli : calcul de A^n .
2. Décomposition de $K[u]$ et sous-espaces stables.
 - [OA] def : sous-espace stable, notation des restrictions, rq : $\ker P(u)$ et $\text{Im} P(u)$ sont stables par u , appli : lien avec les polynômes.
 - [GRI] ex : dans un espace euclidien si F est stable par u alors $F^\perp$ est stable par u^* , appli : réduction des endomorphismes normaux.
 - [COG] prop : si F s.e stable par u alors $\pi_{u_F} | \pi_u$, prop : Si $F_1, \dots, F_r$ stables par u tels que $E = \bigoplus_{j=1}^r F_j$ alors π_u est le ppcm des polynômes minimaux $\pi_{u_{F_1}}, \dots, \pi_{u_{F_r}}$.
 - [OA] lemme des noyaux, ex [GRI] : les projecteurs sont des polynômes en u et décomposition spectrale, rq : obtention d'une décomposition en sous-espaces stables pour u avec le lemme des noyaux et π_u ou un polynôme annulateur, appli : Si $P = Q_1 \dots Q_n$ annulateur de u (donc $E = \bigoplus \ker Q_i(u)$) alors un s.e stable par u admet une décomposition compatible avec celle de $E : F = \bigoplus (F \cap \ker Q_i(u))$.

2 Réduction de u et structure de $\mathbb{K}[u]$.

1. Sous-espaces propres.
 - [GOU] def (en dimension finie) valeur propre-spectre, rq : cas matriciel, def : sous-espace propre, def polynôme caractéristique, rq : deux matrices semblables ont même polynôme caractéristique, c-ex : réciproque fausse, prop : λ est vp ssi λ est racine de χ_u , rq : sur les corps algébriquement clos.
 - [COG] prop : si F stable par u alors $\chi_{u_F} | \chi_u$, prop : les s.e propres de u sont en somme directe, prop : la dimension du s.e propre est $\leq$ à la multiplicité algébrique.
 - [GOU] prop : valeurs propres et poly minimal, csq : spectre $\subset$ dans les racines des polynômes annulateurs, ex [OA] : symétrie et nilpotent, thm de Cayley Hamilton, corrolaire : $\pi_u | \chi_u$.
2. Diagonalisation.
 - [COG et OA] def : diagonalisabilité et équivalence avec la décomposition de E en sous-espaces propres, prop : critère de diagonalisabilité, csq : $K[u]$ est un produit de corps, ex : projecteurs, symétrie (attention caractéristique 2), critère de diago sur les corps finis.
 - [OA] ex : les restrictions d'endomorphismes diago sont diago.
3. Trigonalisation.
 - [GRI] def : endomorphisme trigonalisable, prop : critère de trigonalisation, def : sous-espaces caractéristiques, thm : trigonalisation selon les sous-espaces caractéristiques, coro : décomposition de Dunford - d et n sont des polynômes en u , appli : calcul d'exponentielle de matrices, appli : résolution d'une équation différentielle, coro : réduction de Jordan,  appli : critère de nilpotence de Cartan.

4. Décomposition de Frobenius.

- [GOU] def-notations : polynôme minimal d'un élément $\pi_{u,x}$, prop : bases de $k[u]$, thm : invariants de similitude,  thm : réduction de Frobenius, appli : matrices semblables.
- [OA] exemple : matrice de permutations.

Références :

Objectif Agrégation, Beck.

Algèbre, Xavier Gourdon.

Grifone, Algèbre linéaire.

Methodix Algèbre, Merlin.

Algèbre linéaire, Cagnet.

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

1 Sous-espaces stables et dualité.

- [OA] def : sous-espaces stables, exemple : $\text{Ker}(u)$ et $\text{Im}(u)$ sont stables par u , def : endomorphismes induits par restriction à un sous-espace stable - expression matricielle, ex : divisibilité des polynômes caractéristiques, appli : noyaux itérés, appli : noyaux itérés et endomorphismes nilpotents, lemme (commutation de 2 endomorphismes), exemples : polynômes d'endomorphismes et stabilité.
- [GOU] appli : dimension du commutant d'un endomorphisme, def : sous-ev orthogonal - application transposée, prop : $\text{rg}(u) = \text{rg}({}^t u)$ - $\text{Im}({}^t u) = (\text{Ker}(u))^\perp$, prop : F stable par u ssi $F^\perp$ stable par ${}^t u$.
- [OA ou Madère] ex : sous-espaces stables d'une matrice.
- [GRI] appli : réduction des endomorphismes normaux.
- [OA] lemme des noyaux, appli : stabilité et décomposition compatible, appli : polynôme minimal et lemme des noyaux ($\exists x \pi_{u,x} = \pi_u$).

2 Décomposition de l'espace en sous-espaces stables : réduction des endomorphismes.

1. Décomposition en sous-espaces propres : diagonalisation.

- [GRI] def : valeur et vecteur propre, rq : vecteur propre et stabilité des droites, def : u est diagonalisable si l'espace se décompose en droite stable ie s'il existe une base de vecteur propre, rq : lien avec l'écriture matriciel, def : espace propre, prop : les sous-espaces propres sont en somme directe - E est somme directe de ses sous-espaces propres ssi u est diagonalisable.
- [OA] thm : polynômes annulateurs et diagonalisation, ex : projecteurs - symétries, appli : restriction et diagonalisation.
- [GRI] appli : résolution d'une récurrence linéaire.
- [GOU] thm : diagonalisation simultanée, appli : la somme de 2 endomorphismes qui commutent est diagonalisable.
- [OA] appli : groupes linéaires isomorphes.

2. Décomposition en espaces caractéristiques : trigonalisation.

- [GRI] def : u trigonalisable, def : sous-espace caractéristique, prop : si χ_u est scindé alors E est somme directe d'espaces caractéristiques, rq : les sous-espaces caractéristiques sont stables par u , thm : réduction selon les sous-espaces caractéristiques, appli : décomposition de Dunford.
- [GOU] appli : calcul d'exponentielle, exemple.
- [GRI] appli : résolution de $X' = AX$.
- [GOU] rq : cas d'un corps algébriquement clos, appli : lemme de Schur, thm : trigonalisation simultanée.
- [OA] appli : trigonalisation d'un corchet de Lie,  appli : critère de nilpotence de Cartan.

3. Décomposition de Frobenius.

- [GOU] def-notations : polynôme minimal d'un élément $\pi_{u,x}$, prop : bases de $k[u]$, thm : invariants de similitude,  thm : réduction de Frobenius, appli : matrices semblables et réduction de Frobenius.
- [OA] : exemple : matrice de permutations.

3 Représentation d'un groupe linéaire.

► [COL et RAU] def : représentation - dimension d'une représentation, ex : représentation de dimension 2 de S_3 , ex : isométrie du tétraèdre et du cube, def : caractère d'une représentation, propriétés des caractères, ex : représentations de permutation, def : représentation irréductible, exemple des groupes abéliens, rq : lien avec la réduction simultanée, thm de Maschke, thm principal sur les caractères.

► [PEY]  ex : table de caractère de S_4 , ex : table de caractère de D_n .

Références :

Gourdon, Algèbre.

Grifone, Algèbre linéaire.

Objectif agrégation.

Colmez, Elements d'algèbre et d'analyse.

Peyré, Transformée de Fourier discrète.

Rauch, Groupes finis et représentations.

155 : Endomorphismes diagonalisables en dimension finie.

1 Diagonalisation d'endomorphisme.

1. Sous-espace propre.

► [GRI] : Correspondance endomorphisme et matrice, def : diagonalisation, def : vecteur propre - valeur propre, ex : homothétie - rotation, thm : f diago ssi il existe une base de E formée de vecteurs propres, def : espace propre, thm : f diago ssi E est somme directe de ses sep ssi la somme des dimensions des sep est égale à la dimension de E , ex : "la matrice avec plein de 1", appli : décomposition spectrale, ex : calcul d'une puissance n , corollaire : si f a n vp distinctes alors f est diago.

2. Décomposition de $K[u]$ et sous espace stable.

► [OA] def : ss espace stable, ex : le noyau et l'image de u sont stables par u , ex : dénombrement de sous-espaces stables, lemme : sous-espace stables avec $uov = vou$, ex (recherche de sous espace stable) : lien polynômes et réduction, def : polynôme minimal, remarque : isomorphisme de $k[u]$ via le lemme chinois, prop : polynôme minimal et restriction, thm : lemme des noyaux, application : stabilité et lemme des noyaux (décomposition compatible), prop : f diago ssi π_u est scindé à racines simples, corollaire : f diago ssi $\exists l \in \mathbb{N}$ tel que $k[u] \sim k^l$.

3. Diagonalisation par blocs.

► [GOU] def-notations : polynôme minimal d'un élément $\pi_{u,x}$, prop : bases de $k[u]$, prop : il existe x tel que $\pi_u = \pi_{u,x}$, thm : invariants de similitude, thm : réduction de Frobenius, appli : matrices semblables et réduction de Frobenius.

► [OA] : exemple : matrice de permutations.

2 Recherche de polynômes annulateurs.

1. Polynômes caractéristiques.

► [GRI] def : polynômes caractéristiques, exemple, rq : il ne dépend que de f et pas de la base, prop : lien vp et polynôme caractéristique, prop : dimension des sep, thm : f diago ssi le polynôme caractéristique est scindé et les dimensions des espaces propres sont maximales, exemple, thm : Cayley-Hamilton, ex : si $f^{50} = 0$ alors $f^n = 0$.

2. Polynômes annulateurs.

► [GRI] def : polynôme annulateur, prop : $\text{Sp}(f) \subset \text{Rac}(Q)$ où Q est un polynôme annulateur, c-ex : toute racine d'un polynôme annulateur n'est pas nec une vp, thm : f diago ssi il existe un polynôme annulateur scindé à racines simples.

► [??] ex : dans un $\mathbb{R}$ -ev de dimension finie, soit $u \in \mathcal{L}(E)$ non nul tel que $u^3 + u = 0$ alors le rang de u est pair.

► [OA] ex : projecteurs, ex : symétries, ex : corps finis, applications : restriction d'un endomorphisme diago.

3 Etude de l'ensemble des endomorphismes diagonalisables.

1. Diagonalisation simultanée.

► [OA] prop : réduction simultanée, corollaire : la somme de 2 endo diago qui commutent est diago, ex : groupes linéaires isomorphes, ex : diagonalisation de $M \mapsto UM - MV$ avec U, V diagonalisables, application : décomposition de Dunford,  appli : critère de nilpotence de Cartan.

2. Topologie des endomorphismes diagonalisables.

- [OA] notations et remarques : topologie sur $M_n(k)$ - notations : D_n, T_n et C_n - $k = \mathbb{R} - \mathbb{C}$, prop : adhérence et intérieur de $D_n(k)$ dans $T_n(k)$, rq : $T_n(\mathbb{R})$ est un fermé, prop : adhérence de $C_n(\mathbb{R})$ et $D_n(\mathbb{R})$ est $T_n(\mathbb{R})$.
- [GOU] ex : $\chi_{AB} = \chi_{BA}$ pour tout $A, B \in M_n(\mathbb{R})$.
- [FG] 📖 **prop : dénombrement des endomorphismes diagonalisables de $GL_n(\mathbb{F}_q)$.**

3. Cas particulier des endomorphismes normaux.

- [GRI] def : endomorphisme normal, thm : diagonalisation des endomorphismes normaux, exemples d'endomorphismes normaux : matrices symétriques réelles - hermitienne - orthogonales, appli : existence d'une racine carrée pour les matrices symétriques définies positives, appli : décomposition polaire.

Références :

Grifone, Algèbre linéaire.

Objectif Agrégation.

Gourdon, Algèbre.

156 : Exponentielle de matrices. Applications.

1 Exponentielle et Logarithme.

1. Définitions et convergence.

- [GRI et FAR] def : norme d'algèbre, ex : sur $M_n(\mathbb{R})$, def : exponentielle de matrice avec une norme d'algèbre - convergence normale de la série, rq : série entière de rayon infini et $\|\exp(X)\| \leq \exp(\|X\|)$, ex : $e^{\lambda I_n} = e^\lambda I_n$, prop [GOU] : l'exponentielle de matrice est un polynôme en X , prop : si X et Y commutent $\exp(X+Y) = \exp(X)\exp(Y)$, coro : $\exp(X)$ est inversible et $(\exp X)^{-1} = \exp(-X)$, rq [GOU] : si u et v commutent alors u et $\exp(v)$ commutent, prop : $e^{PXP^{-1}} = Pe^X P^{-1}$ si $P \in GL_n(\mathbb{K})$, coro : $\det(\exp(X)) = e^{\text{tr}(X)}$, ex : calcul d'une exponentielle si X est diagonalisable.
- [FAR et GRI] ex : calcul d'une exponentielle d'un bloc de Jordan.
- [OA] appli : décomposition de Dunford et réduction.
- [GOU] ex : calcul de l'exponentielle de matrice par les projecteurs (et Dunford), appli : si $M \in M_n(\mathbb{R})$ est l'exponentielle d'une matrice alors $\det(M) > 0$, c-ex : la réciproque est fausse.

2. Inverse de l'exponentielle.

- [FAR et OA]  thm : **image de l'exponentielle**, coro : l'application exponentielle est une application de $M_n(\mathbb{R})$ dans $GL_n(\mathbb{R})$ pas injective si $n \geq 2$ et pas surjective - l'application exponentielle est une application surjective de $M_n(\mathbb{C})$ dans $GL_n(\mathbb{C})$ (mais pas injective pour $n \geq 1$), appli : calcul de $M_n(\mathbb{R})$ pour $n \geq 2$.
- [GOU] ex : si $A \in GL(\mathbb{C})$ alors il existe B tel que $B^p = A$, c-ex : faux si A n'est pas inversible, appli : $GL_n(\mathbb{C})$ est connexe.
- [FAR] def : logarithme de matrice dans $B(I_n, 1)$, thm : dans $B(I_n, 1)$ $\exp(\log(g)) = g$ - dans $B(0, \log(2))$ $\log(\exp(X)) = X$, prop : DL au premier ordre et au seconde ordre de $e^{tX}e^{tY}$, ex : limite et exponentielle.
- [GOU] ex : limite et exponentielle.

2 Propriétés analytiques de l'exponentielle et du logarithme.

- [GRI et FAR] prop : l'application $t \in \mathbb{R} \mapsto e^{tX} \in M_n(\mathbb{K})$ est analytique réelle - $\frac{d}{dt}(\exp(tX)) = X \exp(tX)$, appli : système différentiel, exemple, appli : les sous-espaces propres sont invariants sous le flot des solutions.
- [GOU] appli : $\lim_{t \rightarrow +\infty} e^{tM} = 0$ ssi $\text{Re}(\lambda) < 0$.
- [FAR et ROU] rq : $X \mapsto e^X$ l'exponentielle est analytique en tant que série entière (au sens infiniment différentiable et de différentiel continu), thm : différentielle en 0 - difféomorphisme, thm : différentielle de l'exponentielle,  thm : **homéomorphisme de $S_n(\mathbb{R})$ sur $S_n^{++}(\mathbb{R})$** , appli : lien avec la décomposition polaire.
- [H2G2] appli : étude du groupe $O(p, q)$.

3 Algèbre associée à un groupe.

- [FAR] def : sous-groupe à un paramètre, thm : un sous-groupe à un paramètre est $\mathcal{C}^\infty$ (et même analytique) et peut se mettre sous la forme $\gamma(t) = \exp(tA)$, def : $\mathcal{L}(G)$, thm : $\mathcal{L}(G)$ est un sev de $M_n(\mathbb{R})$ - $[X, Y] \in \mathcal{L}(G)$ si $X, Y \in \mathcal{L}(G)$, exemples : $\mathcal{L}(GL_n(\mathbb{R})) = M_n(\mathbb{R})$ - $\mathcal{L}(SL_n(\mathbb{R})) = \{X \in M_n(\mathbb{R}) \mid \text{tr}(X) = 0\}$, $\mathcal{L}(SO_n(\mathbb{R})) = \{X \in M_n(\mathbb{R}) \mid {}^tX = -X\}$ - $\mathcal{L}(U_n(\mathbb{R})) = \{X \in M_n(\mathbb{R}) \mid X^* = -X\}$.

Références :

Faraut, Analyse sur les groupes de Lie.
Grifone, Algèbre linéaire.
Gourdon, Algèbre.

Objectif Agrégation.
Rouvière, Petit guide de calcul différentiel.

157 : Endomorphismes trigonalisables. Endomorphismes nilpotents.

Parler du fait que $\mathcal{N}$ est un cône ?? Rapeller la def de polynôme minimal, caractéristique, Caley Hamilton, lemme des noyaux ?

Rapeller l'objectif de la réduction de u : découper l'espace en sous-espace-espaces stables de u sur lesquels u est "plus simple". La forme la plus simple est le cas diagonale. Si u n'est pas diagonalisable, on va chercher à trigonaliser u (cela demande des hypothèses plus faibles sur u que la diagonalisation). L'objectif de cette leçon est de montrer que la forme triangulaire de u la plus simple est donnée par la réduction de Jordan : les sous-espaces stables seront alors les espaces caractéristiques de u et les restrictions de u à ces sous-espaces stables seront la somme d'une homothétie et d'un endomorphisme nilpotent.

1 Trigonalisation d'endomorphismes.

1. Endomorphismes trigonalisables.

- [GOU] def : endomorphisme trigonalisable.
- [OA] thm : polynômes annulateurs et trigonalisation.
- [GOU] rq : dans $\mathbb{C}$ tout endomorphisme est trigonalisable, c-ex : dans $\mathbb{R}$ c'est faux, ex : si F est stable par u et u trigonalisable alors u_F est trigonalisable, ex : trigonalisation d'une matrice, ex : $\det(\exp(A)) = \exp(\text{tr}(A))$, appli : dans un espace hermitien un endomorphisme est trigonalisable dans une bon.
- [OA] thm : trigonalisation simultanée, c-ex : deux matrices qui sont simultanément trigonalisables mais qui ne commutent pas, appli : une somme d'endomorphismes trigonalisables qui commutent est trigonalisable, appli : cas d'un espace hermitien.
- [OA] prop : l'ensemble des matrices diagonalisable est dense dans l'ensemble des matrices trigonalisables, prop : l'ensemble des matrices trigonalisable dans $\mathbb{R}$ est un fermé de $M_n(\mathbb{R})$.

On peut proposer une simplification de la forme triangulaire dans laquelle plusieurs des termes du bloc triangulaire sont nuls : on va réduire selon les espaces caractéristiques.

2. Réduction en blocs triangulaires.

- [GRI] def : espace caractéristique, rq : les sep sont inclus dans les sec - stabilité des sec, lemme : réduction par blocs dans le cas d'une décomposition en sev stables, thm : réduction selon les sous-espaces caractéristiques, exemple, appli : puissance d'une matrice.

On va encore chercher à simplifier la forme triangulaire grâce à la décomposition de Dunford : on va écrire u comme la somme d'un endomorphisme diagonalisable et d'un endomorphisme nilpotent.

2 Endomorphismes nilpotents.

1. Endomorphismes nilpotents.

- [OA] def : l'espace $\mathcal{N}$, ex : l'endomorphisme $\phi_A = M \mapsto AM$ est nilpotent si A est nilpotent, c-ex : $\mathcal{N}$ n'est pas un ev et n'est pas un groupe (pas stable par addition), prop : commutativité et éléments nilpotents, prop : caractérisation de $\text{Vect}(\mathcal{N})$, def : indice de nilpotence.
- [GOU] ex : inégalités sur l'indice de nilpotence, appli : calcul d'inverse.
- [OA] prop : caractérisations de la nilpotence, c-ex : la réciproque de "si u est nilpotent alors 0 est la seule valeur propre" est fausse, rq : cas de la caractéristique nulle, c-ex [???] : I_p en caractéristique p , ex : matrice nilpotente en dimension 2.
- [GRI] thm : décomposition de Dunford, exemple.
- [OA] appli : exponentielle de matrice et décomposition de Dunford.
- [GOU] appli : conditions sur M pour que $\lim_{t \rightarrow +\infty} e^{tM}$

2. Blocs de Jordan.

- [OA] def : bloc de Jordan, rq : lien avec les matrices compagnons, thm : noyaux itérés, coro : ss-espace stable pour un endomorphisme nilpotent, prop : endomorphisme nilpotent et bloc de Jordan, thm : réduction

de Jordan pour les nilpotents, appli : classes de conjugaison et endomorphismes semblables, thm de Jordan pour un endomorphisme qcq.

► [GRI] exemple.

► [GOU] appli : u et ${}^t u$ sont semblables.

► [OA]  appli : critère de nilpotence de Cartan.

Enfin, dans le cas où u n'est pas trigonalisable, on dispose d'une réduction plus générale : la réduction de Frobenius. Cette réduction généralise la réduction de Jordan et garantit que u se représente par une matrice diagonale par blocs où les blocs sont des matrices compagnons. Nous verrons que les ss-espaces stables de cette décomposition sont les espaces engendrés par un élément et que restreint à ses sous-espaces, l'endomorphisme est cyclique.

3 Endomorphismes cycliques.

► [GOU] Notations : π_u , $\mathcal{L}_u = \{P(u), P \in K[X]\}$, $\pi_{x,u}$, et E_x , prop : dimension et base de $\mathcal{L}_u$, E_x , prop : il existe $x \in E$ tel que $\pi_{x,u} = \pi_u$, def : endomorphismes cycliques, prop : def équivalentes avec $\deg(\pi_u) = n$ et $\pi_u = (-1)^n \chi_u$, prop : u cyclique $\Leftrightarrow$ il existe une base pour laquelle la matrice de u est la matrice compagnon de π_u ,  thm : **décomposition de Frobenius**, corollaire : réduction de Frobenius (préciser qu'il n'y a plus d'hypothèse sur π_u), exemple (??), appli : f et g semblables ssi ils ont les mêmes invariants de similitude, rq : cette décomposition permet de retrouver la réduction de Jordan.

Références :

Grifone, Algèbre linéaire.

Gourdon, Algèbre.

Objectif Agrégation.

Cognet, Algèbre linéaire.

158 : Matrices symétriques réelles, matrices hermitiennes.

1 Structure hermitienne et réduction.

1. Matrices symétriques et hermitiennes.

- [GRI et GOU] def : matrices symétriques - hermitiennes, ex : tMM est symétrique, rq : les éléments de la diagonale d'une matrice hermitienne sont des réels, exemples, def : matrice symétrique (resp hermitienne) positive - définie positive, rq : caractérisation en terme de valeurs propres, notations : S_n, A_n et H_n , prop : $M_n(\mathbb{R}) = S_n \oplus A_n - H_n = S_n \oplus iA_n$, rq : H_n est un $\mathbb{R}$ -ev de dimension n^2 mais n'est pas un $\mathbb{C}$ -ev.
- [ROU]  appli : réduction des formes quadratiques version différentiable, csq : interprétation topologique.

2. Formes bilinéaires et formes hermitiennes.

- [GOU et GRI] def : forme bilinéaire et forme sesquilinéaire ou hermitienne - matrice d'une forme bilinéaire et hermitienne, exemple : matrice du produit scalaire canonique sur $\mathbb{R}^n$, exemple : le produit scalaire $\int_0^1 f(t)g(t)dt$, rq : écriture en dimension finie, prop : changement de base, exemples.
- [GRI] def : endomorphisme adjoint, prop : expression de l'adjoint dans une bon, def : endomorphisme autoadjoint d'un espace euclidien et hermitien.

3. Réduction des matrices symétriques réelles et hermitiennes.

- [GRI] lemme : si une matrice est symétrique réelle ou hermitienne alors ses valeurs propres sont réelles, thm spectral pour les endomorphismes autoadjoints d'un espace euclidien et hermitien, rq : réécriture avec les matrices orthogonales et unitaires, appli : forme bilinéaire ou hermitienne qui définit un produit scalaire, exemple.
- [GOU] appli : racine carrée d'une matrice hermitienne positive, appli : diagonalisation simultanée de 2 endomorphismes autoadjoints, appli : décomposition polaire (cas symétrique réel et hermitien),  appli : exp : $H_n(\mathbb{C}) \rightarrow H_n^{++}(\mathbb{C})$ est un homéomorphisme, coro : "pseudo"-réduction simultanée de matrices symétriques-hermitiennes.

2 Formes quadratiques.

1. Représentation matricielle.

- [GOU et GRI] def : forme quadratique - hermitienne, prop : existence et unicité de la forme polaire, exemples, def : matrice d'une forme quadratique, exemples, def : rang d'une forme quadratique, def : bases orthogonales, exemple : en dimension finie, thm : existence de bases orthogonale, exemple : recherche d'une base orthogonale par la méthode de Gauss, rq : le rang de q en fonction du nombre de carrés dans la réduction de Gauss, ex : rang - base orthogonale de $A \mapsto \det(A)$ et de $q(P) = \int_0^1 P(x)P''(x)dx$.

2. Classification des formes quadratiques en terme d'actions par congruence.

- [H2G2] def : congruence, def : signature, exemple [GRI] : signature d'une forme quadratique - signature des exemples précédents, thm : le rang et la signature sont des invariants totaux pour cette action de groupes, corollaire : thm d'inertie de Sylvester, rq : classification des orbites - forme normale, ex : orbite de l'identité pour l'action de congruence réelle, exemple [GRI] : lien entre matrice définie positive - négative et signature,  appli [ROU] : le lemme de Morse, def : groupe orthogonal et stabilisateur de I_n , prop : orbite des matrices symétriques de signature (p, q) - stabilisateur de $I_{(p, q)}$, def : $O_{(p, q)}$, rq : cas hermitien, exemple [GOU] : $P \mapsto \int_{-1}^1 P(x)P(-x)dx$, def : isométrie d'une forme quadratique, rq : si q et q' sont dans la même orbite alors $O(q)$ et $O(q')$ sont isomorphes, c-ex : réciproque fausse, prop : homéomorphisme entre $O(p, q)$ et $O(p) \times O(q) \times \mathbb{R}^{pq}$.
- [ROU] appli : matrice hessienne et étude d'extremum, exemple.
- [GRI] thm (conique dans un espace euclidien) : orthonormalisation simultanée, corollaire : signature et valeurs propres, exemple, appli : classification des coniques et des quadriques.

Références :

Gourdon, Algèbre.

Grifone, Algèbre linéaire.

Caldero - Germoni, H2G2.

Rouvière, Petit guide de calcul différentiel.

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

Il existe deux manières de caractériser un sev : en se donnant une famille génératrice ou en se donnant des équations linéaires. La notion d'espace dual permet de définir d'une manière plus précise un espace "caractérisé par des équations".

1 Formes linéaires sur un espace vectoriel de dimension finie.

- [GOU] def : forme linéaire - espace dual, ex : la différentiel est une forme linéaire.
- [XENS] ex : dual de $M_n(K)$, appli : caractérisation de la trace.
- [OA] ex : une forme linéaire est soit nulle soit surjective, appli : thm de représentation de Riesz (dans un Hilbert toute forme linéaire est un ps) - csq : définition du gradient
- [GOU] def : hyperplan (en utilisant la dimension), prop : équivalence entre hyperplan et noyau d'une forme linéaire non nulle.
- [XENS] appli : tout hyperplan de $M_n(K)$ coupe $GL_n(K)$, appli : les endomorphismes qui stabilisent tous les hyperplans sont les homothéties.

2 Dualité : bases duale et antéduale.

- [GOU et GRI] def : forme linéaire coordonnée, thm : existence base duale - $\dim(E)=\dim(E^*)$, rq : E et E^* sont isomorphes, ex : base duale, appli : indépendance de formes linéaires, prop : existence base antéduale, ex : base antéduale (cf méthode de changement de base dans le dual), def : bidual, prop : E^{**} est canoniquement isomorphe à E .
- [COG] ex : polynôme interpolateur de Lagrange.

Comme E et E^ sont isomorphes, les sev de E peuvent être caractérisés par des sev de E^* . Etant donné un sev F de E engendré par une famille de vecteurs, on va chercher à déterminer un système d'équations linéaires dont les solutions sont exactement tous les vecteurs de F .*

3 Orthogonalité : une vision géométrique.

1. Orthogonalité.

- [GOU et GRI] def : $x \in E$ et $\phi \in E^*$ orthogonaux - $A^\perp$ sev de E^* orthogonal ou annulateur de A - B sev de E orthogonal de B , rq : si $\phi \in E^*$ alors $\{\phi\}$ est le noyau de ϕ , prop : propriétés d'inclusion, thm : égalité de dimension, ex : ϕ est surjective ssi $\phi_1, \dots, \phi_p$ sont linéairement indépendantes, coro : equations d'un sev en dimension finie, ex : annulateur d'un sev, prop : orthogonalité et hyperplan.
- [XENS] appli : si $f_1, \dots, f_p$ et g sont des formes linéaires sur E telles que l'intersection des $\text{Ker}(f_i)$ est inclus dans $\text{Ker}(g)$ alors $g \in \text{Vect}(f_1, \dots, f_p)$.
- [OA]  appli : **théorème des extremas liés - interprétation géométrique.**

2. Application transposée.

- [GOU et GRI] def : transposée, prop : transposée et orthogonalité, prop : propriétés de la transposée (composée - ${}^t({}^t f)$ - ${}^t(f^{-1})$), prop : stabilité de $F^\perp$ par ${}^t u$, appli : raisonnement par récurrence sur la dimension, rq : lien matriciel, ex : dans un espace euclidien et une bon la transposée coïncide avec l'adjoint, appli [GOU] : un endomorphisme est trigonalisable ssi son polynôme caractéristique est scindé,  appli : **réduction de Frobenius - invariants de similitude.**

Références :

Grifone, Algèbre linéaire.
Gourdon, Algèbre.

Objectif Agrégation.
Cognet, Algèbre linéaire.

160 : Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).

1 Adjoint d'un endomorphisme dans un espace euclidien.

1. Endomorphisme adjoint.

- [GRI] : remarque : dans un bon on a le ps $\langle x, y \rangle = {}^tXY$, prop : existence et unicité de l'adjoint, rq : lien avec la transposée dans un bon, prop : propriétés (f^* , $rg(f^*)$, $det(f^*)$, $ker(f^*)$, $im(f^*)$...), ex : si ${}^tAA = 0$ alors $A = 0$, appli : inverse généralisée et moindres carrés.
- [GOU] : lemme : si F est stable par u alors $F^\perp$ est stable par u^* .

2. Endomorphismes normaux.

- [GRI] : def : endomorphisme normal - matrice normal, ex : matrices symétriques réelles - antisymétriques réelles - orthogonales - autre matrice, rq : caractérisation avec le produit scalaire.
- [ROU] appli : lemme de Morse.
- [GOU] lemme : réduction des endomorphismes normaux sans valeurs propres réelles, thm : réduction des endomorphismes normaux dans un espace euclidien, appli : réduction des matrices antisymétrique réelle.

Nous allons étudier les endomorphismes d'un espace euclidien qui conservent la norme des vecteurs - généralisation des isométries vectorielles (rotations et réflexions).

2 Endomorphismes orthogonaux.

- [GRI] def : transformation orthogonale, prop : définitions équivalentes, rq : lien avec l'adjoint, prop : valeurs propres et déterminant, prop : une transformation orthogonale transforme tout bon en bon, def : $O_n(\mathbb{R})$ - $SO_n(\mathbb{R})$, exemple, prop : matrice de passage d'un bon à un bon est orthogonale, appli : étude de $O_2(\mathbb{R})$, appli : notion d'angle non orienté et orienté.
- [GOU] prop : si F est stable par u alors $F^\perp$ est stable par u , thm : réduction des endomorphismes orthogonaux, appli : isométrie du plan et de l'espace, appli : décomposition d'Iwasawa.
- [???]  appli : **enveloppe convexe de $O_n(\mathbb{R})$.**
- [AUD] prop : $O_n(\mathbb{R})$ est compact, prop : $SO_n(\mathbb{R})$ est connexe par arcs - $O_n(\mathbb{R})$ a deux composantes connexes par arcs homéomorphes à SO_n .

3 Endomorphismes autoadjoints.

- [GRI] def : endomorphisme autoadjoint, prop : caractérisation matricielle (matrice symétrique), thm : toute matrice symétrique est diagonalisable dans $\mathbb{R}$ et les sous-espaces propres sont 2 à 2 orthogonaux, c-ex : les matrices symétriques complexes ne sont pas nec diagonalisables, ex : si $A \in S_n(\mathbb{R})$ alors ses valeurs propres vérifient $\sum \lambda_i^2 = \sum_{i,j} a_{i,j}^2$, appli : endomorphisme diagonalisable.
- [GOU] appli : lien avec les formes quadratiques, prop : "pseudo" réduction simultanée de deux matrices symétriques, def : matrice symétrique positive - définie positive, appli : ellipsoïde de John-Loewner, prop : lien avec le spectre, appli : existence et unicité d'une racine carrée d'une matrice symétrique définie positive, appli : décomposition polaire, appli : rayon spectral d'un endo symétrique positif.
- [H2G2]  appli : **$exp : S_n(\mathbb{R}) \rightarrow S_n^{++}(\mathbb{R})$ est un homéomorphisme.**

Références :

Grifone, Algèbre linéaire.

Gourdon, Algèbre.

Audin, Géométrie.

Rouvière, Petit guide de calcul différentiel.

161 : Isométries d'un espace affine euclidien de dimension finie. Applications en dimensions 2 et 3.

► [AUD-COM] def : espace affine euclidien - espaces affines orthogonaux.

1 Groupe des isométries vectorielles : le groupe orthogonal.

► [COM et AUD] definitions équivalentes : groupe orthogonal $O(E)$, rq : si on choisie un bon on peut identifier $O(E)$ avec $O(n)$, appli : $O(n)$ est compact, def-prop : isométrie positive - sous-groupe fermé, ex : $O^+(2)$ est isomorphe et homéomorphe à $\mathbb{U}$, appli : mesure des angles, thm : réduction des endomorphismes orthogonaux, appli : $O^+(n)$ est connexe par arcs - $O(n)$ a deux composantes connexes par arcs.
► [???]  appli : enveloppe convexe de $O_n(\mathbb{R})$.

2 Groupe des isométries affines.

1. Isométrie affine.

► [COM et AUD] prop : équivalence f isométrique $\Leftrightarrow$ application linéaire associée est orthogonale $\Leftrightarrow$ existence d'un repère orthonormé, notation : $Isom(\varepsilon)$, exemples : les translations - les homothéties - les symétries orthogonales - les réflexions, coro : existence d'une application affine qui envoie un repère orthonormé sur un autre, coro : $\varepsilon \simeq \varepsilon_n(\mathbb{R})$, exemple : l'ensemble des applications affines qui stabilisent un cube est un sous-groupe des isométries de ε_3 - son ordre est 48.

2. Groupe des isométries de ε_n .

► [COM] rq : $Isom(\varepsilon)$ est un groupe, prop : $\varepsilon_n \simeq \mathbb{R}^n \times_{\varphi} O(n)$ avec φ l'action naturel de $O(n)$ sur $\mathbb{R}^n$, coro : description des isométries directes, def : déplacements et antidéplacement, ex (antidéplacement) : produit d'un nombre impair de symétries orthogonales hyperplanes, ex (déplacement) : produit d'un nombre pair de symétrie hyperplanes orthogonales - translation.
► [AUD] appli (justification du terme "déplacement") : $Isom^+(\varepsilon)$ est connexes par arcs.
► [H2G2]  appli (stabilité en dimension 3) : groupe d'isométrie du tétraèdre et du cube.

3. Générateurs du groupe.

► [COM] prop : il existe une unique isométrie affine produit de symétries hyperplanes orthogonales qui envoient n points de ε sur n autres points vérifiant $A_i A_j = A'_i A'_j$, coro : toute application isométrique est affine et est le produit de p symétries hyperplane orthogonales avec $p \leq n + 1$, ex : triangles isométriques, appli : groupe diédral (interprétation géométrique - stabilisateur d'un sommet - cardinal - générateurs), appli (stabilité en dimension 2) : si G sous-groupe fini des isométries du plan euclidien alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ ou à D_n .

3 Classification des isométries.

1. Décomposition canonique d'une isométrie.

► [COM] prop : existence d'une isométrie g de ε_n admettant un point fixe et un unique vecteur de $\text{Ker}(v_f - Id)$ tel que $f = t_x \circ g$, def : cette expression est appelée forme canonique de f , rq : l'étude de g se ramène à celle de $v_g = v_f$ qui est orthogonal (donc que l'on peut réduire, rq : les conjugués de f ont la même nature que f , exemple : si f^n a un point fixe alors f a un point fixe.

2. Classification des isométries en dimension 2.

► [COM] rq : réduction de la matrice M_f de v_f , proposition : les déplacements sont les translations et rotations autour d'un point - les antidéplacements sont les symétries orthogonales par rapport à une droite et les symétries glissées, exemple : groupe des déplacements et antidéplacements en terme d'applications dans une

bon, exemple : nombre d'isométrie telle que $f^n = r_{A,\theta}$.

3. Classification des isométries en dimension 3.

► [COM] rq : réduction de M_f , proposition : les déplacements sont les vissages - les antidéplacements sont les symétries orthogonales par rapport à un plan - les symétries planes glissées et les rotations symétrie, rq : générateurs de $\mathcal{I}^+$, tableau de synthèse (déplacement - antidéplacements - points fixes - dimension du noyau), exemple : étude des applications f et f^2 définies par un système d'équations.

Références :

Combes, Algèbre et géométrie.

Audin, Géométrie.

Caldero - Germoni, H2G2.

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

1 Solutions d'un système d'équations linéaires.

1. Système d'équations linéaires.

► [GRI] def : système linéaire de p équations en n inconnues - solutions - système compatible, rq : expression matricielle - rang du système, rq : expression vectorielle, def : système homogène, ex : il existe un unique polynôme qui prend en $x_1, \dots, x_{n+1}$ des valeurs fixés, appli : annulateur d'un sous-espace (les sev de E peuvent être caractérisés par des sous-espaces vectoriels de E^*) - def - caractérisation - $\dim(E) = \dim(F^o) + \dim(F)$, exemple.

2. Espace des solutions.

► [GRI] prop : l'ensemble des solutions des systèmes homogènes forment un espace vectoriel - dimension de l'espace des solutions en fonction du rang, ex : dimension et base d'un sev défini par un système d'équation homogène, c-ex : les solutions d'un système linéaire non homogène ne forment pas un ev, rq : un système homogène admet une solution non nulle ssi $n > r$, ex : avec une matrice carrée solution non nulle ssi $\det(A) \neq 0$, prop : l'ensemble des solutions est un sous-espace affine de $\mathbb{R}^n$ dirigé par le sev des solutions du système homogène associé, def : système de Cramer, thm de Cramer, exemple, thm de Rouché-Fontené, exemple, ex : problème géométrique (déterminer quatre points alignés connaissant les milieux de chaque segment), appli (cas des système homogènes) : r hyperplans indépendants dans un ev de dimension n définit un sev de dim $n - r$.

2 Méthode du pivot de Gauss.

1. Opérations élémentaires.

► [GRI] prop : l'ensemble des solutions d'un système linéaire ne change pas si l'on effectue des "opérations élémentaires", exemples.

► [OA] opérations élémentaires - traduction en terme de multiplication par une matrice - traduction en terme d'opérations sur le système : matrices de transvection - matrice de dilatation - matrice de transposition, appli : matrice de permutation.

► [XENS]  appli : générateurs de $GL_n(K)$ et application.

2. Système échelonné.

► [GRI] def : matrice - système échelonné, rq : principe du pivot de Gauss pour se ramener à une matrice échelonnée, exemples, exemple : mise en place de la méthode du pivot de Gauss sans variable libre et avec variables libres, appli : savoir si une famille est libre, appli : déterminer les relations linéaires liant une famille de vecteurs, appli : déterminer une base de $F \cap G$, appli : déterminer les équations d'un sous-espace, appli : compléter une famille libre en une base - détermination d'un supplémentaire.

► [OA]  appli : théorème de Carathéodory et système diophantien.

3. Aspects algorithmiques.

► [GRI et FIL] estimation du nombre d'opérations, erreurs d'arrondis - choix du pivot, thm : factorisation LU d'une matrice, ex : toute matrice définie positive admet une décomposition LU, exemple : matrice creuse, thm : factorisation de Choleski, exemple, thm : factorisation QR par Gram-Schmidt, rq : dans la pratique on ne fait pas Gram-Schmidt car elle amplifie les erreurs d'arrondis.

Les méthodes directes sont intéressantes puisqu'elles fournissent la solution exacte mais lorsque le système devient de grande taille, les calculs deviennent fastidieux. Numériquement, les erreurs d'arrondis ne donnent qu'une

*solution approchée, il peut y avoir des problèmes d'instabilité. On va donc construire une suite vectorielle conver-
geant vers la solution du système linéaire : ce le principe des méthodes itératives.*

3 Méthodes itératives.

► [FIL] def : rayon spectral, méthodologie générale, def : convergence d'un algorithme itératif, csq : l'algorithme itératif cv ssi $\lim_{k \rightarrow +\infty} B^k e^{(0)} = 0$, thm : critères de convergence, méthode de Jacobi, thm : convergence de la méthode de Jacobi, exemple, rq : cette méthode présente un critère de convergence restrictif, méthode de Gauss-Seidel, lemme : matrice symétrique définie positive et rayon spectral, thm : convergence de la méthode de Gauss-Seidel.

Références :

Grifone, Algèbre Linéaire.

Filbet, Analyse numérique.

Objectif Agrégation.

170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité et isotropie.

1 Formes bilinéaires symétriques et formes quadratiques.

► [GRI] : def : forme bilinéaire symétrique, ex : $(A, B) \mapsto \text{Tr}({}^tAB)$ et la hessienne, def : forme quadratique, thm (correspondance bijective entre les formes bilinéaires symétriques et les formes quadratiques), exemple de polarisation, prop : matrice d'une forme bilinéaire symétrique - $b(X, Y) = {}^tXBY$ - réciproque (si B est symétrique alors $(X, Y) = {}^tXBY$ est bilinéaire symétrique, ex : matrice d'une forme quadratique, prop : changement de base, def : rang - noyau d'une forme quadratique - forme quadratique non-dégénérée (donner toutes ces def pour une fbs via l'application $j : E \rightarrow E^*$), prop : $\text{rg}(q) = \text{rg}(B) - \dim(\ker(q)) = \dim(B) - \dim(q)$ non dégénérée ssi $\det(B) \neq 0$, def : forme quadratique définie - positive, rq : une forme quadratique définie positive est nécessairement non dégénérée, ex : forme quadratique non dégénérée dont on donne le noyau.

► [ROU] : appli (géo diff) : hessienne et minimum local.

2 Orthogonalité et isotropie.

1. Sous-espaces orthogonaux.

► [GRI] def : orthogonalité pour une forme bilinéaire - notation - orthogonal de $A \subset E$, prop : $A^\perp$ est un sev - $E^\perp = N(q)$ - $A \subset E \Rightarrow N(q) \subset A^\perp$, prop : si F est un sev de E alors $\dim(E) = \dim(F) + \dim(F^\perp) - \dim(F \cap N(q))$ et $F^{\perp\perp} = F + N(q)$, rq : cas où q est non dégénérée, c-ex : $q(x) = x_1^2 - x_2^2$ non dégénérée et $F = \text{Vect}(1, 1) = F^\perp$ mais $E \neq F \oplus F^\perp$.

2. Isotropie.

► [GRI] def : vecteur isotrope, rq : les formes quadratiques définies sont les seules formes quadratiques dont le seul vecteur isotrope est le vecteur nul, def : cône isotrope, rq : ce n'est pas un ev, exemples dans $\mathbb{R}^2$ et dans $\mathbb{R}^3$, dessins en annexe, prop : $N(q) \subset \mathcal{I}(q)$, c-ex : dans les ex précédents on a $N(q) = 0$ donc la réciproque est fausse, def : sev isotrope, prop : il existe des sous-espaces isotropes ssi $\mathcal{I} = \{0\}$, ex : sous-espace isotrope contenant des vecteurs isotropes non nuls, prop : $E = F \oplus F^\perp$ ssi F est non isotrope, exemples, def : sous-espace totalement isotrope, prop : caractérisation équivalente de l'isotropie totale, rq : le noyau est un sous-espace totalement isotrope, ex : forme quadratique non nulle qui admet un sous-espace totalement isotrope de dimension 2 non trivial.

3. Bases orthogonales.

► [GRI] : def : base orthogonale - base orthonormée, rq : s'il existe une base orthonormée alors q est non dégénérée, thm : existence de bases orthogonales pour une forme quadratique, thm (algorithme de Gauss), exemple, csq : détermination d'une base orthogonale, exemple, appli : classification des coniques (def : conique, théorème : classification des coniques en fonction de la signature de q , dessins en annexe).

3 Classification des formes quadratiques.

► [PER] : def : discriminant, rq : le discriminant ne dépend pas de la base.

► [GRI] : thm : classification des formes quadratiques sur $\mathbb{C}$ -ev, cor : il existe une bon ssi q est non dégénérée, thm : classification des formes quadratiques sur $\mathbb{R}$ -ev (Sylvester), ex : signature du déterminant dans $M_2(\mathbb{R})$, corollaire : existence de bon ssi $\text{sign}(q) = (n, 0)$ ssi q est définie positive.

► [ROU] :  appli : le lemme de Morse.

► [XENS]  prop : formes quadratiques et composantes connexes.

► [PER] : thm : classification des formes quadratiques sur $\mathbb{F}_q$ -ev, def : discriminant, prop : si q et q' désignent la même forme quadratique dans des bases différentes alors $\text{rg}(q) = \text{rg}(q')$ et $\text{disc}(q) = \text{disc}(q')$, c-ex : la réciproque est fausse.

4 Groupe orthogonal associé à une forme quadratique.

► [GRI] : prop : existence et unicité de l'endomorphisme adjoint, rq : dans une bon $A^* = {}^tA$, prop-def : endomorphisme orthogonal relativement à q , prop : $O(q)$ est un groupe, prop : si $f \in O(q)$ alors $\det(f) = \pm 1$, prop : $f \in O(q) \Leftrightarrow {}^tASA = S$, ex : transformation de Lorentz en dimension 2.

► [H2G2] : lemme : décomposition polaire et homéomorphisme, def : $O(p, q)$, thm : $O(p, q) \simeq O(p) \times O(q) \times \mathbb{R}^{pq}$, corollaire : $O(p, q)$ est compact ssi $p = 0$ ou $q = 0$.

Références :

Grifone, Algèbre linéaire.

Caldero, Germoni : Histoire hédonistes de groupes et de géométries.

Perrin, Cours d'algèbre.

Oraux X - ENS, Algèbre 3.

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

lien signature et discriminant ???

1 Formes quadratiques réelles.

1. Ecriture matricielle.

► [GRI] def : forme bilinéaire symétrique, ex : $(A, B) \mapsto \text{Tr}({}^tAB)$ et la hessienne, def : forme quadratique, thm (correspondance bijective entre les formes bilinéaires symétriques et les formes quadratiques), exemple de polarisation, prop : matrice d'une forme bilinéaire symétrique - $b(X, Y) = {}^tXBY$ - réciproque (si B est symétrique alors $(X, Y) = {}^tXBY$ est bilinéaire symétrique, ex : matrice d'une forme quadratique, prop : changement de base, exemple.

► [ROU] appli : réduction des formes quadratiques version différentiable, csq : interprétation topologique.

2. Dégénérescence.

► [GRI] def : rang - noyau d'une forme quadratique - forme quadratique non-dégénérée (donner toutes ces def pour une fbs via l'application $j : E \rightarrow E^*$), prop : $\text{rg}(q) = \text{rg}(B) - \dim(\ker(q))$ - q non dégénérée ssi $\det(B) \neq 0$, def : forme quadratique définie - positive, rq : une forme quadratique définie positive est nécessairement non dégénérée, ex : forme quadratique non dégénérée dont on donne le noyau.

► [ROU] appli : hessienne et étude d'extremum, exemple.

► [GOU] thm : Cauchy-Schwarz, ex : une forme positive est définie ssi elle est non dégénérée, appli : inégalité de Minkowsky.

2 Orthogonalité.

1. Sous-espaces orthogonaux.

► [GRI] def : orthogonalité pour une forme bilinéaire - notation - orthogonal de $A \subset E$, prop : $A^\perp$ est un sev - $E^\perp = N(q)$ - $A \subset E \Rightarrow N(q) \subset A^\perp$, prop : si F est un sev de E alors $\dim(E) = \dim(F) + \dim(F^\perp) - \dim(F \cap N(q))$ et $F^{\perp\perp} = F + N(q)$, rq : cas où q est non dégénérée, c-ex : $q(x) = x_1^2 - x_2^2$ non dégénérée et $F = \text{Vect}(1, 1) = F^\perp$ mais $E \neq F \oplus F^\perp$.

2. Groupe orthogonal associé à une forme quadratique.

► [GRI] rq : on veut étudier les endomorphismes qui préservent q , prop : existence et unicité de l'endomorphisme adjoint, rq : dans une bon $A^* = {}^tA$, prop-def : endomorphisme orthogonal relativement à q , prop : $O(q)$ est un groupe, prop : si $f \in O(q)$ alors $\det(f) = \pm 1$, prop : $f \in O(q) \Leftrightarrow {}^tASA = S$, ex : transformation de Lorentz en dimension 2, rq : lien avec $O(n, \mathbb{R})$.

► [H2G2] lemme : décomposition polaire et homéomorphisme.

3. Bases orthogonales.

► [GRI] def : base orthogonale - base orthonormée, rq : s'il existe une base orthonormée alors q est non dégénérée, thm : existence de bases orthogonale pour une forme quadratique, thm (algorithme de Gauss), exemple, csq : détermination d'une base orthogonale, exemple, ex : rang - base orthogonale de $A \mapsto \det(A)$ et de $q(P) = \int_0^1 P(x)P''(x)dx$, thm : orthogonalisation simultanée - formes quadratiques dans un espace euclidien.

3 Classification.

1. Classification des formes quadratiques.

► [H2G2] def : congruence, def : signature, exemple [GRI] : signature d'une forme quadratique - thm : le rang et la signature sont des invariants totaux pour cette action de groupes, corollaire : thm d'inertie de

Sylvester, rq : classification des orbites - forme normale, ex : orbite de l'identité pour l'action de congruence réelle, exemple [GRI] : lien entre matrice définie positive - négative et signature,  appli [ROU] : le lemme de Morse.

➤ [XENS]  prop : formes quadratiques et composantes connexes.

➤ [H2G2] def : groupe orthogonal et stabilisateur de I_n , prop : orbite des matrices symétriques de signature (p, q) - stabilisateur de $I_{(p,q)}$, def : $O_{(p,q)}$, rq : cas hermitien, exemple [GOU] : $P \mapsto \int_{-1}^1 P(x)P(-x)dx$, def : isométrie d'une forme quadratique, rq : si q et q' sont dans la même orbite alors $O(q)$ et $O(q')$ sont isomorphes, c-ex : réciproque fausse, prop : homéomorphisme entre $O(p, q)$ et $O(p) \times O(q) \times \mathbb{R}^{pq}$.

➤ [GRI] prop : formes quadratiques dans un espace euclidien - signatures et valeurs propres, exemple.

2. Coniques et quadriques.

➤ [GRI] réduction des coniques : définition - disjonction de cas selon que q est dégénérée ou pas puis en fonction de sa signature - thm (résumé) - dessins (ANNEXE) - réduction des quadriques : thm (résumé) - dessins (ANNEXE).

Références :

Grifone, Algèbre linéaire.

Caldero, Germoni : Histoire hédonistes de groupes et de géométries.

Gourdon, Algèbre.

Rouvière, Petit guide de calcul différentiel.

Oraux X - ENS, Algèbre 3.

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

1 Barycentres en géométrie affine.

1. Barycentre.

► [COM] def : barycentre - isobarycentre - fonction vectorielle de Leibniz, exemple : condition pour que 2 triangles aient le même isobarycentre, exemple : isobarycentre des racines primitives 15-ième de l'unité, rq : relation $\lambda_1 + \dots + \lambda_k = 1$, prop : conservation du barycentre pour les partitions de I , exemple avec 2 points : segment - milieu du segment, exemple avec 3 points : centre de gravité, exemple pour un simplexe, prop : application affine et barycentre, rq : en caractéristique 2.

2. Sous-espaces affines et barycentres.

► [COM] prop : une partie $\mathcal{F}$ de ε est un sous-espace affine ssi tout barycentre de points de $\mathcal{F}$ est un élément de $\mathcal{F}$, corollaire : sous-espace engendré par une partie.

3. Repères affines.

► [COM] def : partie affinement libre - liée - affinement génératrice - repère affine - coordonnées barycentriques, prop : caractérisation des repères affines, rq : lien repère affine et cartésien, appli : propriétés des espaces affines déduit des propriétés des espaces vectoriels, coro : existence d'une application affine qui envoie un repère affine sur un autre, exemple : triangle et permutation.

4. Espace affine hyperplan d'un espace vectoriel.

► [COM] rq : hyperplan de $\varepsilon_{n+1}(K)$ - motivation d'une telle construction : on se ramène aux outils de l'algèbre linéaire, prop : identification entre algèbre linéaire repère affine via l'hyperplan, exemple : points affinement liés et déterminant de ses coordonnées barycentriques, appli : thm de Ménélaüs.

2 Convexité.

1. Parties convexes d'un espace affine réel.

► [COM] def équivalente : partie convexe - convention, prop : l'intersection de parties convexes est convexe - l'image et l'image réciproque d'une partie convexe par une application affine est convexe, exemple : la boule unité d'un evn réel est convexe.

2. Enveloppe convexe d'une partie.

► [COM] prop - def : l'intersection de toutes les parties convexes qui contiennent X est la plus petite partie convexe de ε qui contient X - caractérisation en terme de barycentre - c'est l'enveloppe convexe, coro : enveloppe convexe et application affine, exemple : avec 2 points et 3 points, appli : thm de Gauss-Lucas sur les racines d'un polynôme dérivé.

► [??]  thm de Carathéodory et application à la résolution d'un système diophantien.

► [??]  ex : enveloppe convexe de $O_n(\mathbb{R})$.

3. Points extrémaux d'une partie convexe.

► [COM] def équivalentes : point extrémal d'une partie convexe, prop : points extrémaux et applications affines, exemple : ensemble des points extrémaux de la boule unité d'un ev euclidien, appli : l'ensemble des points extrémaux d'une partie convexe est fermé dans $C \subset \varepsilon_2$ mais c'est faux dans φ_3 .

Références :

Combes, Algèbre et géométrie.

190 : Méthodes combinatoires, problèmes de dénombrement.

1 Méthode générale de dénombrement.

1. Ensembles finis et cardinal.

► [DEB] def : ensemble fini, prop : formule du crible, exemple : cas particulier de 2 ensembles, thm : produit d'ensembles finis, ex : dénombrement des applications, ex : alphabet braille, ex : nombre de parties d'un n -ensemble.

2. Arrangements et permutations.

► [DEB] def : arrangements - permutations, rq : les arrangements p à p de E sont identifiés de I_p dans E , ex : nombre de permutations d'un n -ensemble, appli : tirage de boule, appli : nombre de trois chiffres contenant 0, 3, 6, 9, appli : nombre de nombres obtenu en permutant 1, 2, 3, 4, 5, 6, def : combinaison, def : coefficients binomiaux, remarques élémentaires, exemple : détermination des coefficients binomiaux avec les injections de I_p dans I_n , exemples : des relations sur les coefficients binomiaux, appli : la loi binomiale est bien une loi de probabilité, rq : interprétation avec le triangle de Pascal, ex : nombre de surjections de I_n sur I_p , ex : tiercé, appli : calcul du nombre d'applications de E dans $A \cup B$ est $(a + b)^n$ - formule de Newton, ex : somme des puissances d'un entier,

3. Principes usuels de combinatoire.

► [DEB] ex : principe d'addition, ex : principe de multiplication, lemme des Bergers, exemple : ensemble des surjections de X sur Y .

2 Dénombrement, théorie des groupes et corps finis.

1. Actions de groupes et dénombrement.

► [COM] def : action de groupes, exemple : action du groupe des bijections de E sur E , def : orbite - stabilisateurs, exemple, prop : équation des classes - formule de Burnside, exemple : $\text{Card}(\mathcal{P}_k(X))$ est divisible par p , appli : dénombrement des colliers.
► [H2G2] appli : groupe d'isométrie du tétraèdre et du cube - nombre de coloriage possible.

2. Corps finis.

► [PER] def - prop : corps à q éléments, exemples : cardinal de $GL_n(\mathbb{F}_q)$ et de $SL_n(\mathbb{F}_q)$, ex : dénombrement des carrés dans $\mathbb{F}_p$.
► [H2G2] appli : action de $GL_m(\mathbb{F}_q) \times GL_n(\mathbb{F}_q)$ sur $M_{m,n}(\mathbb{F}_q)$ - nombre de matrices de rang r .
► [???] ↗ appli : action de $GL_n(\mathbb{F}_q)$ sur $D_n(\mathbb{F}_q)$ - dénombrement des matrices diagonalisables sur $M_n(\mathbb{F}_q)$.

3 Utilisations de fonctions multiplicatives.

1. Indicatrice d'Euler.

► [COM] def : fonction d'Euler, prop : c'est une fonction multiplicative, prop : expression explicite en fonction de la décomposition en facteurs premiers, rq : on peut utiliser la sous-multiplicativité ou la formule du crible pour la démonstration de la formule explicite, appli : racine de l'unité et formel $n = \sum_{d|n} \varphi(d)$, appli : définition des polynômes cyclotomiques.

2. Fonction de Möbius.

► [FGN] def : fonction de Möbius, prop : multiplicativité de la fonction, prop : formule d'inversion, exemple, ↗ appli : dénombrement des polynômes irréductibles de $\mathbb{F}_q[X]$.
► [XENS] appli : probabilité que 2 nombres soient premier entre-eux.

Références :

Francinou - Gianella, Exercices de mathématiques pour l'agrégation.

De Biasi, Mathématiques pour le CAPES et l'agrégation interne.

Perrin, Cours d'algèbre.

Combes, Algèbre et géométrie. Caldero, Germoni : Histoire hédonistes de groupes et de géométries.

Oraux X-ENS, Algèbre 1.