Plans de leçons - Algèbre

Jonathan BADIN

Table des matières

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

Le matériel théorique en accord avec le programme doit être présenté, accompagné d'illustrations pertinentes. Il faut pouvoir dégager l'intérêt des notions introduites avec des exemples d'actions bien choisies pour obtenir des informations soit sur un ensemble X donné, soit sur un groupe G donné et faire apparaître des sous-groupes intéressants de G comme stabilisateurs. Par ailleurs, la présentation doit illustrer comment l'étude des orbites de certaines actions revient à classifier certains objets, soit en trouvant un représentant simple de chaque orbite, soit en dégageant des invariants caractérisant les orbites. Les actions de groupes interviennent aussi efficacement dans des problèmes de dénombrements, notamment via la formule de Burnside. Les exemples peuvent être internes à la théorie des groupes (action naturelle de S_n sur $\{1,\cdots,n\}$, action par translation ou par conjugaison, représentations de groupes, etc). Mais il est souhaitable d'emprunter aussi à d'autres domaines (action sur des anneaux, des espaces de matrices ou des espaces de polynômes, groupes d'isométries, etc). La géométrie fournit aussi de nombreux exemples pertinents (groupes d'isométries d'un polygone dans le plan ou d'un solide ou d'un polygone régulier dans l'espace). Pour aller plus loin, on peut aborder l'action de $\mathrm{PGL}_2(K)$ sur la droite projective menant au birapport ou celle de $\mathrm{SL}_2(\mathbf{Z})$ sur le demi-plan de Poincaré ou les preuves par actions de groupes des théorèmes de Sylow ou encore d'autres actions donnant lieu à des isomorphismes exceptionnels. Il est aussi possible de s'intéresser aux aspects topologiques ou différentiels liés à certaines actions.

Plan

I. Action de groupe

I.1. Action d'un groupe sur un ensemble, définition et exemples

Définition : action de groupe
Exemples : action de groupes en algèbre linéaire [CG13]

- action de $\mathrm{GL}_n(K)$ sur les espaces vectoriels ;
- action de $\mathrm{GL}_n(K)\times\mathrm{GL}_p(K)$ sur $\mathscr{M}_{n,p}(K)$ par $(P,Q)\cdot A = PAQ^{-1}$;
- action de $\mathrm{GL}_n(K)$ sur $\mathscr{M}_n(K)$ par conjugaison : $P\cdot A = PAP^{-1}$.

I.2. L'action de groupe comme machine à classifier

Définition : relation d'équivalente $x\mathscr{R}y \Leftrightarrow \exists g\in G$ tel que $g\cdot x = y$, orbite = classes d'équivalences. On note $G\cdot x$ l'orbite de x sous G [Perrin]. Vocabulaire : action transitive
Un invariant est une application sur $X\to Y$ invariant par la relation d'équivalence $\mathscr{R}$, un invariant est dit

complet si l'application quotient $X/\mathscr{R} \to Y$ est bijective.
Exemples pour les actions précédentes : [CG13]

- dimension
- rang
- invariants de similitudes

Procédé générique : tensorisation des actions. Exemples : [CG13]

- Action sur les couples de sous-espaces de même dimension, invariant $\dim(F \cap G)$ donné par la formule de Grassman
- Conjugaison sur matrices diagonalisables = codigonalisation
- Action de $\mathrm{SO}_2(\mathbf{R})$ sur $\mathbf{S}^1 \times \mathbf{S}^1$ invariant angle orienté de vecteurs
- Birapport.

I.3. Problèmes invariants et utilisations de formes normales

Lorsqu'un dans un problème, un groupe agit et si le problème est invariant par cette action on pourra se ramener à une "forme normale" pour résoudre le problème. Exemples :

- $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$ pour l'action de Steiniz. Application : tout hyperplan de $\mathscr{M}_{n,p}(\mathbf{R})$ contient une matrice inversible [Gou21] p. ?
- Forme normale de Jordan pour l'action de $\mathrm{GL}_n(\mathbf{C})$ sur $\mathscr{M}_n(\mathbf{C})$ par conjugaison. Application : toute matrice de $\mathscr{M}_n(\mathbf{C})$ est semblable à sa transposée [Gou21].

Application 20. *Ellipse de Steiner* [CG13]
Soit A, B, C trois points d'un plan affine non alignés. Il existe une unique ellipse passant par les milieux de ABC et tangente en ses milieux aux côtés du triangle.

II. Plus sur les actions de groupes

II.1. Autre point de vue sur les actions

Définition : une action est un morphisme $\varphi : G \to \mathrm{S}_X$, noyau d'une action et vocabulaire action fidèle. En particulier toute action d'un groupe simple est fidèle.

Exemple 23. Le groupe $\mathrm{PGL}_2(\mathbf{F}_q)$ agit naturellement sur la droite projective $\mathrm{P}(\mathbf{F}_q)$ donc induit un morphisme $\varphi : \mathrm{PGL}_2(\mathbf{F}_q) \to \mathrm{S}_{q+1}$. Cette action est fidèle donc le morphisme φ est injectif. En regardant les cardinaux des deux groupes, on en déduit les isomorphismes exceptionnels :

- $\mathrm{SL}_2(\mathbf{F}_2) = \mathrm{SL}_2(\mathbf{F}_2) = \mathrm{PGL}_2(\mathbf{F}_2) = \mathrm{PSL}_2(\mathbf{F}_2) \simeq \mathrm{S}_3$;
- $\mathrm{PGL}_2(\mathbf{F}_3) \simeq \mathrm{S}_4$ et $\mathrm{PSL}_2(\mathbf{F}_3) \simeq \mathrm{A}_4$;
- $\mathrm{PGL}_2(\mathbf{F}_4) = \mathrm{PSL}_2(\mathbf{F}_4) \simeq \mathrm{A}_5$;
- $\mathrm{PGL}_2(\mathbf{F}_5) \simeq \mathrm{S}_5$ et $\mathrm{PSL}_2(\mathbf{F}_5) \simeq \mathrm{A}_5$.

Exemple 24. S_n agit sur $K[X_1, \cdots, X_n]$ par permutations des variables. Si l'on restreint l'action à l'orbite $\mathrm{S}_n \cdot P$ du polynôme $P \in K[X_1, \cdots, X_n]$ on obtient un morphisme $\mathrm{S}_n \to \langle P \rangle$. Si $n \geqslant 5$ les seuls sous-groupes distingués de S_n étant $\{1\}$, A_n et S_n on en déduit que :

- soit le noyau est S_n dans ce cas P est un polynôme symétrique ;
- soit le noyau est A_n dans ce cas P est un polynôme alterné ;
- sinon toute permutation des variables de P donne un polynôme différent !

Exemple 25. Soit G un groupe quelconque. L'action par translation (à gauche) de G sur même, aussi appelée action de Cayley est défini par $g \cdot x = gx$. Ainsi le morphisme associée $\varphi : G \to \mathrm{S}(G)$ associe à g la permutation associé à la multiplication par g qui est plus précisément un dérangement. Cette action est fidèle, cela permet de voir tout groupe fini comme un sous-groupe d'un groupe de permutations d'un ensemble fini.

Application 26. Un groupe simple d'ordre pair > 2 a pour ordre un multiple de 4. [1]

1. Le très difficile théorème de Feit-Thomson dit que tout groupe fini simple non abélien est d'ordre pair, le point précédent précise donc qu'il a pour ordre un multiple de 4. Avec du matériel supplémentaire (le morphisme de transfert) on peut remplacer "multiple de 4" par multiple de 8 ou 12 et on peut encore aller plus loin...

II.2. Stabilisateurs

Définition des stabilisateurs.
Exemples dans les groupes de matrices :

1. Matrices triangulaires supérieurs comme stabilisateur de l'action sur un drapeau, plus généralement triangulaires par blocs.
2. Groupe orthogonal comme stabilisateur de l'action par congruence.
3. Commutant d'une matrice comme stabilisateur de l'action par conjugaison.

Proposition : relation orbite-stabilisateur.

Application 32. *Théorème de Cauchy*
Dans un groupe fini G si p est un diviseur premier de $|G|$ il existe au moins un élément dans G d'ordre p.

Application 33. Soit $\mathbf{F}_q$ un corps fini. Parmi les endomorphismes de $\mathbf{F}_q^d$ il y a exactement $q^{d(d-1)}$ nilpotents [**DEV1**].

II.3. Formule de Burnside

Proposition 34. *Formule de Burnside*
Soit G un groupe fini agissant sur un ensemble fini X. Le nombre d'orbite de cette action est :

$$\frac{1}{|G|}\sum_{x\in X}|\mathrm{Fix}(x)|$$

où $\mathrm{Fix}(x)=\{g\in G\ :\ g\cdot x=x\}$.

Exemple 35. Le nombre de façons de placer p chaises blanches et $n-p$ chaises noires autour d'une ronde à n places est [Gou21] :

$$\sum_{d\,|\,n}\varphi(d)\binom{n/d}{p/d}.$$

Exemple 36. La probabilité que deux éléments commutent entre eux dans un groupe est $p=\frac{r}{|G|}$ où r désigne le nombre de classes de G. En particulier $p\leqslant 5/8$ pour un groupe non abélien avec égalité pour D_4.

III. Structure des groupes finis

III.1. Exemples d'actions d'un groupe sur lui même

Action par translation

Définition : $g\cdot x=gx$ avec $(g,x)\in G\times G$. Il peut être intéressant de restreindre l'action à un sous-groupe H de G.

Proposition 37. Si H est un sous-groupe de G les orbites de l'action par translation à gauche de H sur G sont de la forme Hg où $g\in G$. En particulier lorsque G est un groupe fini on a $|G|=|H|\times|G:H|$ où $[G:H]$ est le nombrer de classes de conjugaisons appelée indice de H dans G.

Corollaire 38. Dans un groupe fini, l'ordre d'un élément divise le cardinal du groupe. En particulier tout groupe d'ordre un nombre premier est cyclique.

Rem : réciproque Lagrange.

Action par conjugaison

Définition : $g\cdot x=gxg^{-1}$.
Pro : Les orbites sont les classes de conjugaisons, le stabilisateur est le centralisateur, les points fixes de l'action est le centre du groupe.
ex : description des classes de conjugaisons de S_n.

Proposition 41. Si G est un p-groupe agissant sur un ensemble fini X l'ensemble X^G des points fixes de l'action vérifie $|X^G|=|X| \mod p$.

Corollaire 42. Le centre d'un p-groupe est non trivial.

App : structure des p-groupes.

Action par translation sur les classes d'un sous-groupes

Définition : $g \cdot (xH) = (gx)H$.
Pro : Action transitive, le stabilisateur de xH est xHx^{-1}.
app : [Per96] si G groupe infini et H sous-groupe de G d'indice fini alors G n'est pas simple.

Proposition 46. Soit G un groupe fini puis H un sous-groupe de G d'indice le plus petit facteur premier de G. Alors, H est distingué dans G.

Application 47 (DEV2). Soit p et q deux nombres premiers avec $p < q$.

- Si p ne divise pas $q-1$ alors tout sous-groupe d'ordre pq est cyclique.
- Si p divise $q-1$ alors il existe à isomorphisme près deux sous-groupes d'ordre pq, le groupe cyclique et un produit semi-direct non trivial $\mathbf{Z}/p\mathbf{Z} \ltimes_\alpha \mathbf{Z}/q\mathbf{Z}$. Une présentation du groupe est [2] : $\langle x, y \mid x^p 1, y^q = 1, xyx^{-1} = y^a \rangle$ où a est un élément d'ordre p de $\mathbf{Z}/(q-1)\mathbf{Z}$. [3]

Corollaire 48. Tout sous-groupe d'indice 2 d'un groupe fini est distingué.

Rem : on retrouve que A_n est distingué dans S_n.

Action par conjugaison sur les sous-groupes

Définition : $g \cdot H = gHg^{-1}$. Le stabilisateur d'un sous-groupe est appelée normalisateur et est noté $N_G H$. C'est le plus grand sous-groupe dans lequel H est distingué.
ex : Dans les théorèmes de Sylow le cardinal du normalisateur d'un p-Sylow est $\frac{|G|}{n_p}$.

III.2. Théorèmes de Sylow

Théorème 51. *Théorèmes de Sylow*
Soit G un groupe fini puis p un diviseur premier de son ordre. Alors,

- G possède au moins un p-Sylow ;
- les p-Sylow de G sont tous conjugués ;
- le nombre n_p de p-Sylow de G satisfait aux deux conditions

$$n_p \text{ divise } |G|, \qquad n_p \equiv 1 \mod p.$$

Exemple 52. *Exemples de sous-groupes de Sylow*

1. Un groupe abélien fini G à un unique p-Sylow appelée composante p-primaire et qui correspond à $\{x \in G \mid p^k x = 0\}$ où k désigne la valuation de p.
2. On peut réaliser D_4 comme un 2-Sylow de S_4 en regardant la permutation des sommets. L'arbitraire de la numérotation des sommets donne 3 copies de D_4, et comme les 2-Sylow sont conjugués ce sont les seuls. Les 3-Sylow de S_5 sont simplement les 3-cycles, il y en a 4.
3. Dans S_5 on a pas grand chose de plus, D_4 se réalise toujours comme un 2-Sylow, les autres sont conjugués et il y en a 15. Les 3-Sylow de S_5 sont encore les 3-cycles, il y en a maintenant 10. Pour les 5-Sylow voir le point suivant.
4. Les p-Sylow de S_p sont exactement les sous-groupes engendré par un p-cycle. Un tel sous-groupe possède $(p-1)$ générateurs et comme il y a $(p-1)!$ cycle d'ordre p, il y a $(p-2)! := n_p$ sous-groupe d'ordre p. Le théorème de congruence de Sylow dit que $n_p \equiv 1 \mod p$ on retrouve ainsi le théorème de Wilson
$$(p-1)! \equiv -1 \mod p.$$
5. Pour $q = p^r$, l'ensemble des matrices triangulaires supérieurs de diagonale $(1, \cdots, 1)$ est un p-Sylow de $\mathrm{GL}_n(\mathbf{F}_q)$. Plus généralement, on peut montrer [Caldero] que l'ensemble des p-Sylow de $\mathrm{GL}_n(\mathbf{F}_q)$ est en bijection avec l'ensemble des drapeaux complets de $\mathbf{F}_q^n$: le stabilisateur d'un drapeau complet correspond à un unique p-Sylow. On a ainsi
$$n_p(\mathrm{GL}_n(\mathbf{F}_q)) = \prod_{k=1}^{n-1} (1 + p + \cdots + p^k).$$

2. attention au passage aux notations multiplicatives
3. Pour $p = 2$ on peut prendre $a = -1$ on retrouve alors le groupe diédral D_q.

6. Pour $n = 2^k m$ avec m impair, il y a m sous-groupes de Sylow d'ordre 2^{k+1} qui sont exactement $\langle r^m, sr^j \rangle$ où $0 \leqslant j < m$. Maintenant pour p nombre premier impair, il y a un unique p-Sylow de D_n à savoir $\langle r^m \rangle$ où $n = p^k m$ avec p ne divisant pas m.

Corollaire 53. *Réciproque faible de Lagrange*
Si p est un nombre premier tel que p^i divise $|G|$ alors G a un sous-groupe d'ordre p^i. En particulier, pour tout p diviseur premier de $|G|$, G possède un élément d'ordre p (Cauchy).

Application 54. Tout groupe non abélien d'ordre < 60 n'est pas simple. Comme A_5 est un groupe simple non abélien d'ordre 60, on montre ainsi que le plus petit groupe simple non abélien est d'ordre 60, c'est même l'unique groupe simple[4] d'ordre 60.

Application 55. *Classification des groupes d'ordre 12*
IL existe à isomorphisme près 5 groupes non abéliens d'ordre 12 dont deux groupes abéliens $\mathbf{Z}/12\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ et trois groupes non-abéliens dont D_6, A_4 et un nouveau groupe le groupe dicyclique d'ordre 12 qui se présente

$$\langle a, b \mid a^3 = b^4 = bab^{-1}a^{-2} = 1 \rangle.$$

4. Pour montrer cela une idée est à partir d'un groupe simple G d'ordre 60 de chercher une action de G sur un ensemble à 5 éléments. On tombe pas trop loin en regardant l'action de G sur ces 5-Sylow, il y a 6. Comme G est simple ce morphisme est injectif, de plus G étant parfait, son image est inclus dans A_6. Ainsi, G s'identifie à un sous-groupe d'indice 6 de A_6. On peut alors En regardant l'action de G sur A_6/G on montre alors que G est isomorphe à un sous-groupe de S_5, d'indice 2 donc isomorphe à A_5.

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

Les notions élémentaires concernant les nombres complexes de module 1 (définitions, exponentielle complexe, trigonométrie, etc.) doivent être présentés, avant d'aborder l'aspect "groupe" de $\mathbf{S}^1$ en considérant son lien avec $(\mathbf{R},+)$ et en examinant ses sous-groupes (en particulier finis). Il est souhaitable de présenter des applications en géométrie plane, par exemple la constructibilité des polygones réguliers. Plus généralement, la leçon invite à expliquer où et comment les nombres complexes de module 1 et les racines de l'unité apparaissent dans divers domaines des mathématiques : spectres de matrices remarquables, polynômes cyclotomiques, et éventuellement les représentations de groupes, etc. On peut également s'intéresser aux sous-groupes compacts de $\mathbf{C}^*$. Pour aller plus loin, on peut s'intéresser aux nombres de module 1 et aux racines de l'unité dans $\mathbf{Q}[i]$ ou à la dualité des groupes abéliens finis ou encore aux transformées de Fourier discrètes et rapides. Des aspects analytiques du sujet peuvent être évoqués (théorème de relèvement, logarithme complexe, analyse de Fourier sur $\mathbf{R}^n$ mais ne doivent occuper ni le cœur de l'exposé, ni l'essentiel d'un développement.

Plan

I. Nombres complexes de module 1

Notation : $\mathbf{U} = \{z = x + \mathrm{i}y \in \mathbf{C} \mid |z| = \sqrt{x^2+y^2} = 1\}$. En identifiant $\mathbf{C}$ avec $\mathbf{R}^2$, $\mathbf{U}$ correspond au cercle unité centré en de $\mathbf{R}^2$ pour sa structure euclidienne usuelle.

I.1. Paramétrisation : exponentielle complexe

U *défini une courbe, on cherche un paramétrage mais un tel paramétrage ne saurait être unique car il dépend de la vitesse à laquelle on parcourt le cercle. On impose naturellement la condition d'un paramétrage unitaire i.e. à vitesse constante égal à 1 :* $\|\gamma'(t)\| = 1$

Lemme 1. Si γ est une application injective de classe C^1 d'un intervalle I de $\mathbf{R}$ dans $\mathbf{U}$ tel que $\|\gamma'(t)\| = 1$ à tout instant $t \in I$ alors,

$$\big(\forall t \in I,\ \gamma'(t) = \mathrm{i}\gamma(t)\big) \text{ ou } \big(\forall t \in I,\ \gamma'(t) = -\mathrm{i}\gamma(t)\big).$$

Rem : les deux alternatives correspondent aux deux orientations possibles du cercle unité.

Définition 3. On définit l'exponentielle complexe par le développement en série entière :

$$e^z := \sum_{n=0}^{+\infty} \frac{z^n}{n!}.$$

Propriétés de l'exponentielle complexe :

- morphisme : $e^{z+z'} = e^z e^z$; $(\mathbf{C}, +) \to (\mathbf{C}^*, \times)$ en particulier $(e^z)^{-1} = e^{-z}$.
- conjugué : $\overline{e^z} = e^{\bar{z}}$ en particulier $e^z \in \mathbf{U}$ si et seulement si $z \in i\mathbf{R}$.
- dérivée : $\frac{d}{dz} e^z = e^z$. On en déduit que pour I un intervalle ouvert contenant 0, pour $a \in \mathbf{C}$, la fonction $t \mapsto e^{at}$ est l'unique solution sur I de l'équation différentielle $y'(t) = a\,y(t)$ avec la condition initiale $y(0) = 1$.
- surjectivité : $\exp(\mathbf{C}) = \mathbf{C}^*$ (attention c'est plutôt difficile comme résultat).

Théorème 5. L'application $f : t \in \mathbf{R} \mapsto e^{it}$ est un morphisme de groupe surjectif de $\mathbf{R}$ dans $\mathbf{U}$. Son noyau est non trivial, il existe un unique réel strictement positif noté π tel que $\mathrm{Ker}(f) = 2\pi\mathbf{Z}$, ainsi f passe au quotient pour définir un isomorphisme

$$\overline{f} : \mathbf{R}/2\pi\mathbf{Z} \longrightarrow \mathbf{U}.$$

I.2. Mesures d'angles

Lemme 6. *Décomposition polaire*
Pour tout complexe non nul z, il existe un unique couple $(r, \theta) \in]0, +\infty[\times \mathbf{R}/2\pi\mathbf{Z}$ tel que $z = re^{i\theta}$. Nécessairement r est le modulo de z et θ est appelée *argument* de z.

Définition 7. Soient z_1 et z_2 deux nombres complexes non nuls. On définit la mesure d'angle entre z_1 et z_2 noté (z_1, z_2) comme l'élément $\theta_2 - \theta_1 \in \mathbf{R}/2\pi\mathbf{Z}$ où θ_1 et θ_2 sont respectivement les arguments de z_1 et z_2.

Rem : si z_1 et z_2 sont deux points de $\mathbf{U}$, la mesure d'angle (z_1, z_2) correspond à la longueur de la portion du cercle unité joignant z_1 à z_2. En remarque parce que pas de bonne définition de la longueur d'une courbe.

Proposition 9. *Relation de Chasles*
La loi de groupe sur $\mathbf{R}/2\pi\mathbf{Z}$ indique qu'on peut additionner des mesures d'angles. De plus pour z_1, z_2, z_3 trois nombres complexes on a :

$$(z_1, z_2) + (z_2, z_3) = (z_1, z_3).$$

Corollaire 10. La somme des angles d'un triangle tracé sur le plan complexe vaut π.

Remarque : définition du groupe des angles d'un plan affine euclidien.

I.3. Fonctions trigonométriques

def : cosinus et sinus comme partie réelle et imaginaire de l'exponentielle. Caractérisations :

- développement en série entière
- équation différentielle

Propriétés :

- Périodicité, parité
- Formules d'addition et autres formules.

Application 14. *Polynômes de Tchebychev*
Il existe un unique polynôme T_n de degré n tel que $T_n(\cos(\theta)) = \cos(n\theta)$. Ce polynôme peut s'exprimer sous la forme suivante :[5]

$$T_n(X) = \sum_{0 \leqslant 2k \leqslant n} \binom{n}{2k} X^{n-2k} (X^2 - 1)^k.$$

En particulier $\cos \frac{2k\pi}{n}$ est algébrique pour $(k, n) \in \mathbf{Z} \times \mathbf{N}_0$.

5. Ces polynômes sont important en analyse numérique car $\frac{1}{2^n} T_n$ est l'unique polynôme minimisant la quantité $\|P\|_{L^\infty(]-1,1[)}$ où P parcourt l'ensemble des polynômes unitaires de degré n. On s'en sert par exemple en interpolation.

II. Racines de l'unité

II.1. Racines n-ème de l'unité

Définition : racines n-èmes de l'unité notation $\mathbf{U}_n$.
rem : sont racines de $X^n - 1$ donc entiers algébriques.
Exemples : racines de l'unité dans le spectre de matrices remarquables :

1. tout sous-groupe fini de $\mathrm{GL}_d(\mathbf{C})$ est formé de matrices diagonalisables à spectre dans $\mathbf{U}_n$ où n désigne l'ordre du groupe.
2. Exemple explicite : groupe des matrices de permutations.
3. Application : tout sous-groupe fini de $\mathrm{GL}_d(\mathbf{Z})$ s'injecte dans $\mathrm{GL}_d(\mathbf{Z}/3\mathbf{Z})$ en particulier de cardinal inférieur à 3^{d^2}.

Proposition : $\mathbf{U}_n$ est un sous-groupe fini de $\mathbf{U}$. Il est cyclique d'ordre n, son unique sous-groupe d'ordre $d \mid n$ est $\mathbf{U}_d$. Réciproquement tout sous-groupe fini de $\mu(\mathbf{C})$ est égal à un certain $\mathbf{U}_n$. Finalement si sous-groupe distinct de $\mu_n(\mathbf{C})$ alors dense.
Définition : racines primitives, notation $\mathbf{U}_n^*$.
Pro : $\mathrm{e}^{\frac{2ik\pi}{n}}$ avec $k \wedge n = 1$ = l'ensemble des générateurs de $\mathbf{U}_n$, il y en a $\varphi(n)$.

II.2. Polynôme cyclotomiques

Définition : polynômes trigonométriques.
Théorème : Polynômes irréductibles à coefficients entiers. [**DEV1**] [Per96]

Corollaire 22. Pour $(k,n) \in \mathbf{Z} \times \mathbf{N}$ avec $n \geqslant 2$ le réel $2\cos\frac{2k\pi}{n}$ est un entier algébrique de degré $\frac{\varphi(n)}{2}$. Son polynôme minimal $\Psi_n(X)$ est définie par la relation :

$$\Psi_n(X + X^{-1}) = X^{-\varphi(n)/2}\Phi_n(X).$$

App : Polygones constructibles.
Rem : on peut aussi potentiellement en déduire sinus avec des formules de trigonométries...

II.3. Constructibilité des polygones réguliers

Définition nombres constructibles [Per96]

Lemme 27. On note Γ l'ensemble des réels constructibles i.e. les réels x tels que $(x,0)$ est un point constructible. Alors, l'ensemble des nombres constructibles est un corps de la forme $\Gamma \times \Gamma$

Proposition 28. L'ensemble Γ est un sous-corps de $\mathbf{R}$.

Théorème 29. *Théorème de Wantzel*
Un réel x est constructible si et seulement s'il existe une suite d'extensions quadratiques :

$$K_0 = \mathbf{Q} \hookrightarrow K_1 \hookrightarrow \cdots \hookrightarrow K_n \ni x.$$

Corollaire 30. Γ est le plus petit sous-corps de $\mathbf{R}$ stable par racine carrée.

Application 31 (DEV1). Si un polygone constructible est constructible alors son nombre de côtés est le produit d'une puissance de 2 et de nombres de Fermat premiers.

III. Groupes abéliens finis : structure, caractères et théorie de Fourier

III.1. Structure des groupes abéliens de type fini

Lemme 32. Soit $A \in \mathscr{M}_{n,k}(\mathbf{Z})$. Il existe une matrice $P \in \mathrm{GL}_n(\mathbf{Z})$, une matrice $Q \in \mathrm{GL}_k(\mathbf{Z})$ de déterminants ± 1 et des entiers strictement positifs d_i tels que $d_1 | d_2 | \cdots | d_l$ et,

$$PAQ = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_k & \\ & & & \mathbf{0} \end{pmatrix}.$$

De plus la suite $(d_1, \cdots, d_l)$ avec les conditions précédentes est unique.

Théorème 33. Soit G un groupe abélien de type finie. Il existe une unique suite $(d_1, \cdots, d_l)$ d'entiers strictement positif avec $d_1 | \cdots | d_l$ et un unique entier r tel que

$$G \simeq \mathbf{Z}^{d_1} \times (\mathbf{Z}/d_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_l\mathbf{Z}) \times \mathbf{Z}^r.$$

ex : prenons un ordre et regardons les groupes abéliens...
rem : algorithme pour obtenir smith. .

III.2. Caractères d'un groupe abélien fini

def : caractères d'un groupes abéliens, groupe dual.
ex : caractères d'un groupe cyclique.

Proposition 38. Tout groupe abélien fini est isomorphe à son dual. En particulier $|\widehat{G}| = |G|$.

Corollaire 39. Les caractères forment une base orthonormée de $L^2(G, \mathbf{C})$.

III.3. Transformée de Fourier sur un groupe fini

Définition 40. La transformée de Fourier d'une fonction $f \in L^2(G, \mathbf{C})$ est l'application $\widehat{f} : \widehat{G} \to \mathbf{C}$ définie par :

$$\widehat{f}(\chi) = \langle f, \chi \rangle = \sum_{g \in G} f(g)\overline{\chi(g)}.$$

Proposition 41. L'application $f \mapsto \widehat{f}$ est linéaire transformant la convolution en produit : $\widehat{f * g} = \widehat{f} \times \widehat{g}$ où $f * g(x) = \sum_{y+z=x} f(y)g(z)$.

Théorème 42. Formule d'inversion de Fourier :

$$f(g) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi.$$

Corollaire 43. L'application $f \mapsto \widehat{f}$ est à un facteur près isométrie de $L^2(G, \mathbf{C})$ sur $L^2(\widehat{G}, \mathbf{C})$ précisément :

$$\langle f, g \rangle_G = \frac{1}{|G|^2} \langle \widehat{f}, \widehat{g} \rangle.$$

Application 44 (Dev2). Soit X_n la marche aléatoire sur $\mathbf{Z}/N\mathbf{Z}$ dont la loi des sauts est $\frac{1}{3}(\delta_{-1} + \delta_0 + \delta_1)$. Alors, X_n converge en loi vers la loi uniforme et on peut estimer sa vitesse de convergence :

$$\| \mathscr{L}(X_n) - \mathscr{L}(X_\infty) \|_2 \leqslant \left| \frac{1 + 2\cos\left(\frac{2i\pi}{N}\right)}{3} \right|^n.$$

Théorème 45. Algorithme de transformée de Fourier rapide.
On peut calculer algorithmiquement la transformée Fourier sur $\mathbf{Z}/n\mathbf{Z}$ en $O(n \log(n))$.

Application 46. On peut associer à un polynôme $P = \sum_{k=0}^{d} a_k X^k$ avec $d < n$ l'élément $p = (a_0, \cdots, a_d, 0, \cdots, 0) \in \mathscr{F}(\mathbf{Z}/n\mathbf{Z}, \mathbf{C})$. Si P et Q sont deux polynômes de degré $< n/2$ alors leur produit $\sum_{k=0}^{n} c_k X^k$ correspond à la convolution de p et q dans $\mathscr{F}(\mathbf{Z}/n\mathbf{Z}, \mathbf{C})$. On peut alors calculer le produit de P par Q en appliquant la transformée de Fourier à p et q, en faisant le produit terme à terme des transformées puis en revenant avec la transformée de Fourier inverse. Avec l'algorithme précédent on a ainsi besoin de $O(n \log(n))$ opérations, une complexité inférieur à la multiplication naïve des polynômes qui demande $O(n^2)$ opérations.

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

Dans un premier temps, la notion de conjugaison dans un groupe introduite brièvement doit être développée et illustrée dans des situations variées. On doit proposer des situations où la conjugaison aide à résoudre certains problèmes (par exemple, en transformant un élément en un autre plus simple à manipuler). On peut aussi illustrer et utiliser le principe du " transport par conjugaison " voulant que hgh^{-1} ait la même " nature géométrique " que g. Ensuite, il est attendu de développer l'intérêt de la notion de sous-groupe distingué en particulier en regard de la structure de groupe obtenue par quotient d'un groupe, le lien entre sous-groupe distingué et noyau de morphisme de groupes, ainsi que la factorisation d'un morphisme de groupe au travers d'un tel quotient. Il est indispensable de proposer quelques résultats bien choisis mettant en évidence l'utilisation de ces notions : citons par exemple le lien entre les sous-groupes de l'un et de l'autre et la caractérisation interne des produits directs. L'examen de la simplicité de certains groupes peut être proposé. Comme indiqué dans le sujet, il est demandé de présenter des exemples pertinents utilisés pour obtenir des résultats significatifs. De tels exemples sont nombreux en théorie des groupes mais il est souhaitable d'en proposer dans d'autres domaines, comme en arithmétique, en géométrie et en algèbre linéaire. Pour aller plus loin, les candidates et candidats peuvent poursuivre en illustrant ces notions en théorie des représentations des groupes finis (classes de conjugaison et nombre de représentations irréductibles, treillis des sous-groupes distingués lu dans la table de caractères, etc.). La notion de produit semi-direct et les théorèmes de Sylow débordent du programme. Il est possible de les évoquer, mais en veillant à les illustrer par des exemples et des applications.

Plan

I. Conjugaison dans un groupe

I.1. Action par conjugaison

Définition de l'action par conjugaison : orbite = classes de conjugaisons, stabilisateurs = centralisateurs, préciser que l'action se fait par automorphismes (dit intérieurs). [Perrin]
Exemples :

- D_n : pour un élément de $\langle r\rangle$ sa classe de conjugaison et lui même et son inverse, ensuite $\mathrm{D}_n \setminus \langle r\rangle$ forme une classe de conjugaison si n est impair, sinon c'est la réunion des deux c=lasses de conjugaisons $\{sr^{2k}\}$ et $\{sr^{2k+1}\}$. [Ortiz p.16]

- S_n : les classes de conjugaisons sont classifier par le type de la permutation [Per96]
- $GL_n(K)$: les classes de conjugaisons correspondent aux classes de similitudes des matrices inversibles, on peut les classifier à partir des invariants de similitudes. [CG13]

Proposition 5. *Équation aux classes*
Soit $g_1, \cdots, g_r$ un système de représentant des orbites non triviales alors

$$|G| = |\mathrm{Cen}(G)| + \sum_{i=1}^{k} |\mathrm{Conj}(g_i)| = |\mathrm{Cen}(G)| + \sum_{i=1}^{k} \frac{|G|}{|\mathrm{Cen}(g_i)|}.$$

Application 6. [Per96] Les p-groupes ont un centre non trivial.

Application 7. *Théorème de Wedderburn* [Per96]
Tout corps (gauche) fini est commutatif.

rem : La formule de Burnside appliqué à l'action par conjugaison donne $r = \frac{1}{G}\sum_{g\in G} |\{x \mid gx = xg\}|$ s'interprète en disant que la probabilité que deux éléments commutent dans un groupe est égal au rapport du nombre de classes de conjugaison par l'ordre du groupe. Un résultat classique qui en découle après quelques calculs établit que pour un groupe non commutatif cette probabilité est inférieur à $\frac{5}{8}$. Cette borne est optimal, elle est atteinte pour D_4.

I.2. Sous-groupes distingués

def sous-groupes distingués. Exemples :
- Centre d'un groupe : exemples de A_n, SL_n, SO_n.
- Dans un groupe abélien tous les sous-groupes sont distingués. La réciproque est fausse : H_8 n'a que des sous-groupes distingués. [Per96]
- Sous-groupes distingués de D_n sont D_n, $\langle r^k \rangle$ avec $k \mid n$ et $\langle r^2, sr^l \rangle$ où $l \in \{0,1\}$ lorsque n est pair. [Ortiz p. 19]

Proposition 13. Le noyau d'un morphisme de groupe est un sous-groupe distingué.

Exemples :
- A_n comme noyau de la signature
- $SL_n(K)$ et $SO_n(K)$ comme noyau du déterminant
- Le centre peut s'interpréter comme le noyau de $g \mapsto c_g$ où $c_g : x \mapsto gxg^{-1}$.

I.3. Critères de distinctions sur l'ordre

Proposition 15. *Lemme d'Ore*
Soit G un groupe fini. Tout sous-groupe de G d'indice le plus petit facteur premier de G est distingué.

Exemple :

1. tout sous-groupe d'indice 2 est distingué. On retrouve ainsi que A_n est distingué dans S_n.

2. les sous-groupes maximaux d'un p-groupe sont distingués.

Théorème 18. *Théorèmes de Sylow* [Per96]
Soit G un groupe fini puis p un diviseur premier de son ordre. Alors,
- G possède au moins un p-Sylow ;
- les p-Sylow de G sont tous conjugués ;
- le nombre n_p de p-Sylow de G satisfait aux deux conditions

$$n_p \text{ divise } |G|, \qquad n_p \equiv 1 \mod p.$$

Exemple : tout groupe d'ordre p^2q possède un p-Sylow ou un q-Sylow distingué.
rem : Parfois les règles de divisibilités ne permettent de conclure sur le nombre de p-Sylow c'est par exemple le cas pour $n = 24$. L'exemple de S_4 montre en fait que les Sylow ne sont pas distingués. On peut toutefois conclure à l'existence d'un sous-groupe distingué (autre qu'un p-Sylow) en regardant l'action du groupe sur ses p-Sylow pour un p-fixé. Le noyau de cette action fournit potentiellement un s.g.d. Avec ces méthodes on peut montrer que tout groupe d'ordre inférieur à 60 possède un s.g.d.

II. Groupes quotients

II.1. Quotient par un sous-groupe distingué

Proposition 21. Soit H un sous-groupe distingué de G, on note G/H l'ensemble classes modulo H. Il existe une unique structure de groupe sur G/H qui fasse de la projection canonique $\pi : G \to G/H$ un morphisme de groupe. Ce groupe est appelé groupe quotient de G par H et sera encore noté G/H.

rem : le noyau de π est H ce qui montre que tout sous-groupe distingué est le noyau d'un morphisme de groupe. De plus cela montre la nécessité de supposer H distingué si l'on veut définir comme précédemment une structure de groupe sur G/H.

Théorème 23. Soit $f : G \to H$ un morphisme de groupe surjectif alors f se factorise en un isomorphisme $\overline{f} : G/\mathrm{Ker} f \to H$.

ex : groupe alternée,groupe linéaire, groupe orthogonal,structure du groupe des automorphismes intérieurs.

II.2. Groupe dérivée

def : groupe dérivée

Proposition 26. Soit G un groupe. Le groupe dérivée de G est un sous-groupe distingué, il vérifie la propriété suivante : tout morphisme $f : G \to A$ avec A abélien se factorise par $D(G)$.

Corollaire 27. $D(G)$ est le plus petit sous-groupe distingué de G dont le quotient est abélien, on appelle $G/D(G)$ l'abélianisé de G.

exemples : groupe alternée, groupe spécial linéaire, groupe orthogonal
rem : cas particuliers
app : Théorème de Frobenius-Zolotarev .

II.3. Correspondance des sous-groupes

Proposition 31. Soit G un groupe puis H un sous-groupe distingué. L'application $f : A \subset G \mapsto \pi_{G/H}(A)$ induit une bijection de l'ensemble des sous-groupes de G contenant H sur l'ensemble des sous-groupes de G/H qui applique les sous-groupes distingués sur les sous-groupes distingués.

Application 32. Soit G un groupe d'ordre p^n. Alors pour tout $k \in \{0, \cdots, n-1\}$, G admet un sous-groupe distingué d'ordre p^k.

remarque : structure des p-groupes, un problème difficile.

III. Décomposition des groupes

III.1. Suites de Jordan-Hölder

Proposition 34. Soit G un groupe fini. Il existe une suite $G_0 = \{1\} \subsetneq G_1 \subsetneq \cdots \subsetneq G_k = G$ tel que les quotients G_{k+1}/G_k soient simples. De plus si $(H_0, \cdots, H_l)$ est une autre suite alors $k = l$ et à permutations près les quotients sont isomorphes. Une telle suite

ex : S_4 , exemple groupe abélien
def groupes résolubles
pro : caractérisation par le groupe dérivée
exemples : les p-groupes sont résolubles
S_n n'est pas résoluble pour $n \geqslant 5$.

III.2. Décomposition des groupes usuels

Théorème 39. *Décomposition des groupes usuels* [Per96]

1. Pour $n \geqslant 5$, A_n est simple.
2. Pour $n \geqslant 3$ ou $n = 2$ et $|K| > 3$, $\mathrm{SL}_n(K)/\mathrm{Cen}(\mathrm{SL}_n(K))$ est simple ;
3. Pour $n \neq 4$, $\mathrm{SO}_n(\mathbf{R})/\mathrm{Cen}(\mathrm{SO}_n(\mathbf{R}))$ est simple. [**DEV1**]

Lemme 40. Les parties sont des systèmes générateurs conjugués :

1. les 3-cycle pour A_n et $n \geqslant 5$;

2. les transvections dans $\mathrm{SL}_n(K)$ pour $n \geqslant 3$;
3. les renversements dans $\mathrm{SO}_n(\mathbf{R})$ pour $n \geqslant 3$.

rem : les cas exceptionnels A_n ok, voir isomorphismes exceptionnels pour PSL et $\mathrm{PSO}_4 \simeq \S 0_3 \times \mathrm{SO}_3$ par les quaternions
rem : les isomorphismes exceptionnels
rem : A_5 plus petit groupe simple ensuite vient $\mathrm{PSL}_2(\mathbf{F}_7) \simeq \mathrm{PSL}_3(\mathbb{F}_2)$ d'ordre 168

III.3. Problème de l'extension

def : produit semi-direct [Per96]
ex : cas produit direct, cas pas de produit semi-direct quaternions etc...
pro : caractérisation produit semi-direct dans les extensions, caractérisation interne du produit semi-direct [Per96]

Application 47 (DEV2). Classification des groupes d'ordre pq. [Per96]

lem : quels produits semi-directs sont isomorphes

104 : Groupes finis. Exemples et applications.

Cette leçon est particulièrement vaste et il convient de faire des choix, qui devront pouvoir être justifiés. La notion d'ordre (d'un groupe, d'un élément et d'un sous-groupe) est très importante dans cette leçon ; le théorème de Lagrange est incontournable. Le théorème de structure des groupes abéliens finis doit figurer dans cette leçon. Sa démonstration est techniquement exigeante, mais il faut que l'énoncé soit bien compris, en particulier le sens précis de la clause d'unicité, et être capable de l'appliquer dans des cas particuliers. Il est souhaitable de présenter des exemples de groupes finis particulièrement utiles comme les groupes $\mathbf{Z}/n\mathbf{Z}$ et S_n, en en maîtrisant les propriétés élémentaires (générateurs, classes de conjugaison, etc.) Il est important de connaître les groupes d'ordre premier ainsi que les groupes d'ordre inférieur à 8. Des exemples de groupes finis issus de domaines autres que la théorie des groupes doivent figurer en bonne place dans cette leçon. L'étude des groupes d'isométries laissant fixe un polygone (ou un polyèdre) régulier peut être opportunément exploitée sous cet intitulé. Afin d'illustrer leur présentation, les candidates et candidats peuvent aussi s'intéresser à des groupes d'automorphismes ou étudier les groupes de symétries A_4, S_4, A_5 et relier sur ces exemples géométrie et algèbre. Pour aller plus loin, les candidates et candidats peuvent s'attarder sur la dualité dans les groupes abéliens finis. Comme application, la cyclicité du groupe multiplicatif d'un corps fini est tout à fait adaptée. Il est possible d'explorer des représentations de groupes, de donner des exemples de caractères, additifs ou multiplicatifs dans le cadre des corps finis. Il est aussi possible de s'intéresser aux sommes de Gauss. Les candidates et candidats peuvent ensuite introduire la transformée de Fourier discrète, qui pourra être vue comme son analogue analytique, avec ses formules d'inversion, sa formule de Plancherel. Ainsi, la leçon peut mener à introduire la transformée de Fourier rapide sur un groupe abélien dont l'ordre est une puissance de 2 ainsi que des applications à la multiplication d'entiers, de polynômes et éventuellement au décodage de codes via la transformée de Hadamard.

Plan

I. Arithmétique des groupes finis

I.1. Décomposition en classe, théorème de Lagrange

Proposition 1. Action par translation d'un sous-groupe, décomposition en classes.

cor : théorème de Lagrange
app : structure des groupes d'ordre premier
rem : contre-exemple théorème de Lagrange faux exemple A_4 (résolubilité)

I.2. Ordre d'un élément

Proposition 5. *Définition de l'ordre*
Soit g un élément d'un groupe fini G. Il existe un plus petit entier n tel que $g^n = 1$, dès lors le sous-groupe engendré par g est exactement $\{1, \cdots, g^{n-1}\}$ où ces n éléments sont tous distincts ce qui fait de n le cardinal de $\langle g \rangle$.

app : critère d'Euler.

Corollaire 7. L'ordre divise le cardinal du groupe donc $a^{|G|} = 1$.

ex : théorème d'Euler et cas particulier de Fermat.
app : cryptographie RSA
app en arithmétique ?

Proposition 11. Théorème de Cauchy

app : structure des groupes d'ordre 6.

I.3. Exposant d'un groupe

Définition 13. Exposant d'un groupe

Proposition 14. ppcm

Application 15. Groupe multiplicatif d'un corps

Exemple 16. Indicatrice de Carmichael.

Application 17. Pour le test de Fermat, existence de nombres de Carmichael...

II. Un peu plus sur la structure des groupes finis

II.1. Dévissage

pro : introduction groupes quotient et sous-groupes distingués
ex : donner des exemples pour digérer A_n ex : lemme d'Ore
def : groupes simples
pro : simplicité du groupe alterné
app : groupes d'ordre 8 (avec contre-exemple produit semi-direct pour la suite)

II.2. Extension

def : produit semi-direct
pro : critères de p.s.d
app : groupes d'ordre pq

II.3. Théorèmes de Sylow

Théorème 27. *Théorèmes de Sylow*
Soit G un groupe fini puis p un diviseur premier de son ordre. Alors,

- G possède au moins un p-Sylow ;
- les p-Sylow de G sont tous conjugués ;
- le nombre n_p de p-Sylow de G satisfait aux deux conditions

$$n_p \text{ divise } |G|, \qquad n_p \equiv 1 \mod p.$$

Exemple 28. Petits groupes symétriques, groupes diédraux, $\mathrm{GL}_n(\mathbf{F}_p)$.

Corollaire 29. *Réciproque faible de Lagrange*
Si p est un nombre premier tel que p^i divise $|G|$ alors G a un sous-groupe d'ordre p^i. En particulier, pour tout p diviseur premier de $|G|$, G possède un élément d'ordre p (Cauchy).

Application 30. Tout groupe non abélien d'ordre < 60 n'est pas simple. Comme A_5 est un groupe simple non abélien d'ordre 60, on montre ainsi que le plus petit groupe simple non abélien est d'ordre 60, c'est même l'unique groupe simple[6] d'ordre 60.

Application 31. *Classification des groupes d'ordre 12*
IL existe à isomorphisme près 5 groupes non abéliens d'ordre 12 dont deux groupes abéliens $\mathbf{Z}/12\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ et trois groupes non-abéliens dont D_6, A_4 et un nouveau groupe le groupe dicyclique d'ordre 12 qui se présente

$$\langle a, b \mid a^3 = b^4 = bab^{-1}a^{-2} = 1 \rangle.$$

III. Groupes abéliens finis : structure, caractères et théorie de Fourier

III.1. Structure des groupes abéliens de type fini

Proposition 32. Réduction de Smith (pas besoin de l'unicité)

Théorème 33. Structure des groupes abéliens de type fini

ex : prenons un ordre et regardons les groupes abéliens, faire pour les petits groupes abéliens (ordre inférieur à 16)...
rem : algorithme pour obtenir smith.
app : préshot groupe abélien fini isomorphe à son dual.

III.2. Caractères d'un groupe abélien fini

def : caractères d'un groupes abéliens, groupe dual.
ex : caractères d'un groupe cyclique.

Proposition 39. Un groupe abélien est isomorphe à son dual

Proposition 40. Les caractères forment une base orthonormée.

III.3. Transformée de Fourier sur un groupe fini

notations avec rappels structure L^2.
def : transformée de Fourier.

Proposition 42. Propriétés de la transformée de Fourier

Application 43. Marche aléatoire sur $\mathbf{Z}/N\mathbf{Z}$.

Algorithme de transformée de Fourier rapide.

Application 45. On peut associer à un polynôme $P = \sum_{k=0}^{d} a_k X^k$ avec $d < n$ l'élément $p = (a_0, \cdots, a_d, 0, \cdots, 0) \in \mathscr{F}(\mathbf{Z}/n\mathbf{Z}, \mathbf{C})$. Si P et Q sont deux polynômes de degré $< n/2$ alors leur produit $\sum_{k=0}^{n} c_k X^k$ correspond à la convolution de p et q dans $\mathscr{F}(\mathbf{Z}/n\mathbf{Z}, \mathbf{C})$. On peut alors calculer le produit de P par Q en appliquant la transformée de Fourier à p et q, en faisant le produit terme à terme des transformées puis en revenant avec la transformée de Fourier inverse. Avec l'algorithme précédent on a ainsi besoin de $O(n \log(n))$ opérations, une complexité inférieur à la multiplication naïve des polynômes qui demande $O(n^2)$ opérations.

6. Pour montrer cela une idée est à partir d'un groupe simple G d'ordre 60 de chercher une action de G sur un ensemble à 5 éléments. On tombe pas trop loin en regardant l'action de G sur ces 5-Sylow, il y a 6. Comme G est simple ce morphisme est injectif, de plus G étant parfait, son image est inclus dans A_6. Ainsi, G s'identifie à un sous-groupe d'indice 6 de A_6. On peut alors En regardant l'action de G sur A_6/G on montre alors que G est isomorphe à un sous-groupe de S_5, d'indice 2 donc isomorphe à A_5.

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

Parmi les attendus, il faut savoir relier la leçon avec les notions d'orbites et d'actions de groupes. Il faut aussi savoir décomposer une permutation en cycles à supports disjoints, tant sur le plan théorique (preuve du théorème de décomposition), que pratique (sur un exemple) et savoir l'utiliser pour déterminer les classes de conjugaison du groupe symétrique et pour donner des systèmes de générateurs. L'existence du morphisme signature est un résultat non trivial mais ne peut pas constituer, à elle seule, l'objet d'un développement. Il est bon d'avoir en tête que tout groupe fini se plonge dans un groupe symétrique et de savoir calculer la signature des permutations ainsi obtenues dans des cas concrets. Les applications sont nombreuses, il est très naturel de parler du déterminant, des polynômes symétriques ou des fonctions symétriques des racines d'un polynôme. On peut également parler du lien avec les groupes d'isométries des solides. Pour aller plus loin, les candidates et candidats peuvent s'intéresser par exemple aux automorphismes du groupe symétrique, à des problèmes de dénombrement, aux représentations des groupes des permutations ou encore aux permutations aléatoires.

Plan

I. Étude générale du groupe symétrique

I.1. Permutations et groupe symétrique

def : permutations d'un ensemble X.
pro : L'ensemble des permutations forme un groupe. En particulier S_n.
ex : cas $n = 0, 1, 2$.
pro : Passage de l'isomorphisme d'ensemble.
Propriétés de S_n :

- centre trivial pour $n \geqslant 3$;
- cardinal $n!$;
- S_n agit naturellement sur $[\![1, n]\!]$ via $\sigma \cdot x = \sigma(x)$. Cette action est n-transitive et fidèle.

Représentation matricielle de S_n.

I.2. Décomposition en cycles

Définition : cycle.

Proposition 8. Une permutation $\sigma \in \mathrm{S}_n$ se décompose de façon unique en produits de cycles à supports disjoints. Cette décomposition est donnée par :

$$\sigma = \prod_{x \text{ rep}} (x\, \sigma(x) \cdots \sigma^{\mathrm{ord}(x)-1}(x))$$

où le produit s'effectue sur un système de représentants des orbites de l'action naturelle de S_n restreindre à $\langle\sigma\rangle$.

ex : voir [Gou21].

Définition : profil d'une permutation.

Proposition 11. Les classes de conjugaisons de S_n sont classés par le type. Le cardinal de la classe de conjugaison de type $(k_1, \cdots, k_n)$ est :

$$\frac{n!}{\prod_{i=1}^n k_i! i^{k_i}}.$$

En particulier le nombre de classes de conjugaison est $p(n)$ le nombre de partitions de n.

Corollaire 12. Soit $\sigma^{(n)}$ une permutation aléatoire de loi uniforme puis $(C_1^{(n)}, \cdots, C_n^{(n)})$ son profil. Alors à m fixé on a :

$$(C_1^{(n)}, \cdots, C_m^{(n)}) \longrightarrow \bigotimes_{j=1}^{m} \mathrm{Poi}(1/j).$$

Proposition 13. Avec les notations précédentes :

$$\mathbf{P}(C_j^{(n)} = k) = \frac{1}{j^k k!} \sum_{l=0}^{\lceil n/j \rceil - k} \frac{(-1)^l}{l! j^l}.$$

En particulier $C_j^{(n)}$ converge en loi vers $\mathrm{Poi}(1/j)$ et,

$$d_{TV}(C_j^{(n)}, \mathrm{Poi}(1/j)) \sim \frac{2^{n_j+1}}{(n_j+1)! j^{n_j+1}} \qquad n_j = \lceil n/j \rceil.$$

I.3. Générateurs et présentation

Définition : les transpositions engendrent S_n.
app : groupe de symétrie du tétraèdre.

Proposition 16. Un ensemble de transpositions générateurs est minimal si et seulement son cardinal est $n-1$.

Remarque 17. Système de générateurs à deux éléments.

Exemples : les sauts $(i\, i+1)$ et $(1\, i)$.

Proposition 19. Présentation de groupes associés [à compléter]

II. Structure du groupe symétrique

II.1. Signature

pro : parité nombre de transposition
def signature, permutations paires et impairs
ex : signature par rapport à la décomposition en cycle
ex : multiplication par a.
pro : signatures et inversions.
ex : signature multiplication par 2. pro : déterminant

Application 27. Le nombre de dérangements pairs vs impairs est :

$$d_n^- = \frac{d_n - (-1)^{n-1}(n-1)}{2} \quad \text{et} \quad d_n^+ = \frac{d_n + (-1)^{n-1}(n-1)}{2}.$$

Corollaire 28. Avec la représentation matricielle de S_n on a $\det(P_\sigma) = \varepsilon(\sigma)$.

II.2. Groupe alterné

def : groupe alterné
rem : cas des petits groupes.
Propriétés :

1. cardinal $n!/2$;
2. centre trivial saufs petits cas ;
3. action naturelle $n-2$-transitive.

pro : les 3-cycles engendrent le groupe alterné, pour $n \geqslant 5$ ils sont conjugués (pas pour $n \leqslant 4$ savoir quoi).
cor : c'est un groupe parfait, ainsi S_n n'est pas résoluble remarque théorie de Galois
th : pour $n \geqslant 5$ le groupe alterné n'est pas simple [Per96]
description du cas $n = 4$
app : permutations des variables d'un polynôme
cor : sous-groupes d'indice n.

II.3. Automorphismes

Lemme 37. [Per96] Un automorphisme de S_n est intérieur si et seulement s'il envoie toute transposition sur une transposition.

Théorème 38. [Per96] Pour $n \neq 6$ les automorphismes de S_n sont intérieurs.

Corollaire 39. [Per96] Pour $n \neq 6$, $\mathrm{Aut}(\mathrm{S}_n) \simeq \mathrm{S}_n$.

Lemme 40. [Per96] S'il existe un sous-groupe H d'indice n de S_n non conjugué aux stabilisateurs des points, il existe un automorphisme non intérieur de S_n. L'existence d'un tel sous-groupe est équivalente à celle d'une action transitive fidèle de S_n sur un ensemble à $n+1$ éléments.

Exemple : l'action de S_5 sur ses 5 Sylow est un exemple d'une telle action. [Per96]

Proposition 41. Pour $n = 6$ il existe un automorphisme non intérieur de S_n. L'ensemble des automorphismes intérieurs forme alors un sous-groupe d'indice 2 de $\mathrm{Aut}(\mathrm{S}_n)$. En particulier $|\mathrm{Aut}(\mathrm{S}_6)| = 1440$.

III. Le groupe symétrique en pratique

III.1. Action de groupe et groupe symétrique

Proposition : Lien entre action de groupe et groupe symétrique

Exemple 43. Soit G un groupe quelconque. L'action par translation (à gauche) de G sur même, aussi appelée action de Cayley est défini par $g \cdot x = gx$. Ainsi le morphisme associée $\varphi : G \to \mathrm{S}(G)$ associe à g la permutation associé à la multiplication par g qui est plus précisément un dérangement. Cette action est fidèle, cela permet de voir tout groupe fini comme un sous-groupe d'un groupe de permutations d'un ensemble fini.

Application 44. Un groupe simple d'ordre pair > 2 a pour ordre un multiple de 4. [7]

Exemple 45. Le groupe $\mathrm{PGL}_2(\mathbf{F}_q)$ agit naturellement sur la droite projective $\mathrm{P}(\mathbf{F}_q)$ donc induit un morphisme $\varphi : \mathrm{PGL}_2(\mathbf{F}_q) \to \mathrm{S}_{q+1}$. Cette action est fidèle donc le morphisme φ est injectif. En regardant les cardinaux des deux groupes, on en déduit les isomorphismes exceptionnels :

- $\mathrm{SL}_2(\mathbf{F}_2) = \mathrm{SL}_2(\mathbf{F}_2) = \mathrm{PGL}_2(\mathbf{F}_2) = \mathrm{PSL}_2(\mathbf{F}_2) \simeq \mathrm{S}_3$;
- $\mathrm{PGL}_2(\mathbf{F}_3) \simeq \mathrm{S}_4$ et $\mathrm{PSL}_2(\mathbf{F}_3) \simeq \mathrm{A}_4$;
- $\mathrm{PGL}_2(\mathbf{F}_4) = \mathrm{PSL}_2(\mathbf{F}_4) \simeq \mathrm{A}_5$;
- $\mathrm{PGL}_2(\mathbf{F}_5) \simeq \mathrm{S}_5$ et $\mathrm{PSL}_2(\mathbf{F}_5) \simeq \mathrm{A}_5$.

Application 46. L'action de $\mathrm{PSL}_2(\mathbf{F}_5) \simeq \mathrm{S}_5$ sur la droite projective fournit une action transitive de S_5 sur un ensemble à 6 éléments. [Per96]

7. Le très difficile théorème de Feit-Thomson dit que tout groupe fini simple non abélien est d'ordre pair, le point précédent précise donc qu'il a pour ordre un multiple de 4. Avec du matériel supplémentaire (le morphisme de transfert) on peut remplacer "multiple de 4" par multiple de 8 ou 12 et on peut encore aller plus loin...

III.2. Groupe symétries de certaines figures discrètes

Proposition : groupes de symétrie des solides de Platon
pro : théorème de Klein sur les groupes de symétries
app : coloriage du cube

III.3. Groupe linéaire sur un corps fini

Théorème 50. *Théorème de Frobenius-Zolotarev*
Soit $q = p^k$ avec p premier. Pour $u \in \mathrm{GL}_d(\mathbf{F}_q)$ on a :

$$\varepsilon(u) = \det(u)^{\frac{q-1}{2}} = \begin{cases} 1 & \text{si} \quad \det(u) \text{ est un carré} \\ -1 & \text{si} \quad \det(u) \text{ n'est pas un carré} \end{cases}$$

ex : signature du Frobenius : $(-1)^{\frac{(d+1)(q-1)}{2}}$.
app : deuxième loi complémentaire.

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

Les premières définitions et propriétés générales du groupe linéaire doivent être présentées : familles de générateurs, liens avec le pivot de Gauss, sous-groupes remarquables. Il est important de savoir faire correspondre certains sous-groupes du groupe linéaire avec les stabilisateurs de certaines actions naturelles (sur des formes quadratiques, sur des drapeaux, sur une décomposition en somme directe, etc.). Il faut aussi savoir réaliser S_n dans $\mathrm{GL}_{n,p}$,K^q et faire le lien entre signature et déterminant. Il est souhaitable de dégager des propriétés particulières selon le corps de base, en particulier sa cardinalité lorsque le corps K est fini et les propriétés topologiques de ce groupe lorsque le corps est $\mathbf{R}$ ou $\mathbf{C}$. Pour aller plus loin, les candidates et candidats peuvent exploiter le fait que la théorie des représentations permet d'illustrer l'importance de $\mathrm{GL}_{n,p}$, C_q et de son sous-groupe unitaire. Ils peuvent également étudier les sous-groupes compacts maximaux et les sous-groupes fermés de $\mathrm{GL}_{n,p}$.

Plan

I. Groupe linéaire

I.1. Présentation du groupe linéaire

def : groupe linéaire et représentation matricielle [Per96]
ex : cas d'un corps fini cardinal
ex : cas $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$ groupe topologique ouvert dense de $\mathscr{M}_d(\mathbf{C})$.
Pro : Matrices de permutations
Cor : Tout sous-groupe fini s'injecte dans $\mathrm{GL}_n(K)$.
app : un théorème de Sylow
Pro : Centre réduit aux homothéties.

I.2. Déterminant et groupe spécial linéaire

Proposition 8. Le déterminant induit un morphisme surjectif de $\mathrm{GL}_n(K)$ vers $K^\times$. Son noyau est un sous-groupe distingué de $\mathrm{GL}_n(K)$ appelée groupe spécial linéaire et noté $\mathrm{SL}_n(K)$.

Corollaire 9. On a une suite exacte :

$$1 \to \mathrm{SL}_n(K) \to \mathrm{GL}_n(K) \to K^\times \to 1.$$

Cette suite est scindée ainsi $\mathrm{GL}_n(K) \simeq \mathrm{SL}_n(K) \rtimes K^\times$.

ex : cardinal dans le cas d'un corps fini.
sous-variétés sur $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$
théorème de Cartan-Von Neumann [admis]

I.3. Générateurs

Définition des transvections et dilatations
Propriétés [Per96]

Proposition 15. Les transvections engendrent $\mathrm{SL}_n(K)$. Les dilatations engendrent $\mathrm{GL}_n(K)$.

Application 16. [CG13]

1. $\mathrm{GL}_n(\mathbf{C})$ est connexe ;
2. $\mathrm{GL}_n(\mathbf{R})$ n'est pas connexe, ces deux composantes connexes sont $\mathrm{GL}_n^{\pm}(\mathbf{R})$;[8]
3. $\mathrm{SL}_n(\mathbf{R})$ et $\mathrm{SL}_n(\mathbf{C})$ sont connexes.

Application 17. *Théorème de Frobenius-Zolotarev*
Soit $q = p^k$ avec p premier. Pour $u \in \mathrm{GL}_d(\mathbf{F}_q)$ on a :

$$\varepsilon(u) = \det(u)^{\frac{q-1}{2}} = \begin{cases} 1 & \text{si} \quad \det(u) \text{ est un carré} \\ -1 & \text{si} \quad \det(u) \text{ n'est pas un carré} \end{cases}$$

Ex : Signature du Frobenius

Remarque 19.
1. Matrices de transvections élémentaires ;
2. Matrices de dilatations élémentaires non ;
3. Algorithmiquement pivot de Gauss.

II. Actions et sous-groupes

II.1. Actions usuelles

Action par conjugaison

Action par congruence

Action sur les drapeaux

Dire que ce sont les q-Sylow
Application aux q-Sylow ?

Action sur les décompositions

Application au dénombrement.

II.2. Groupe orthogonal

def : $\mathrm{O}_n(\mathbf{R})$ et $\mathrm{SO}_n(\mathbf{R})$
pro : topologie compacité, sous-variétés espace tangent, composantes connexes

Proposition 22. [CG13] Pour tout matrice $A \in \mathrm{GL}_n(\mathbf{R})$ il existe un unique couple $(O,S) \in \mathrm{O}_n(\mathbf{R}) \times \mathrm{S}_n(\mathbf{R})$ tel que $A = OS$. De plus l'application

$$(O,S) \in \mathrm{O}_n(\mathbf{R}) \times \mathrm{S}_n(\mathbf{R}) \to OS \in \mathrm{GL}_n(\mathbf{R})$$

est un homéomorphisme.

Corollaire 23. [CG13] $\mathrm{O}_n(\mathbf{R})$ est un sous-groupe compact maximal de $\mathrm{GL}_n(\mathbf{R})$ et a le même type d'homotopie que $\mathrm{GL}_n(\mathbf{R})$. [préciser]

rem : on peut montrer que tout sous-groupe compact maximal est conjugué à $\mathrm{O}_n(\mathbf{R})$.
calcul de la décomposition polaire par la méthode de Héron.

8. Ces deux composantes connexes correspondent aux bases directes et aux bases indirect selon la base canonique. Le résultat précédent s'interprète en disant qu'il est impossible de passer continument d'une base direct à une base indirect, c'est par exemple ce qu'on observe si l'on veut effectuer une symétrie axiale à une figure sur une feuille de papier, c'est impossible sans la briser.

II.3. Sous-groupes finis

Diagonalisable, co si abélien
ex : matrices de permutations.
app : borne sur les sous-groupes finis à coefficients entiers
Tout sous-groupe fini est conjugué à un sous-groupe fini de $\mathrm{O}_n(\mathbf{R})$.
Pro : Description des sous-groupes finis du plan et de l'espaces.
exemples des solides de Platon.

III. Résultats de structure

III.1. Simplicité du groupe projectif linéaire

Lem : Centre de GL et SL [Per96]
def : groupes projectifs
th : simplicité [Per96]
Action de $\mathrm{PSL}_n(K)$ sur la droite projective $\mathbf{P}^1(K)$, traduisant en terme d'injections de groupes
Sur les isomorphismes exceptionnels [Per96]

III.2. Structure du groupe des isométries

lem : générateurs de O_n [Per96]
th : simplicité du quotient [Per96]
pro : les quaternions pour $n = 3, 4$ [Per96]

III.3. Matrices triangulaires supérieurs

Dévissage avec la diagonale
résolubilité des matrices unipotentes

Théorème 36. *Théorème de Lie-Kolchin*
Tout sous-groupe connexe résoluble de $\mathrm{GL}_n(\mathbf{C})$ est conjugué à un sous-groupe des matrices triangulaires.

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

La leçon doit être illustrée par des exemples de groupes très variés, dont il est indispensable de donner des parties génératrices. La description ensembliste du groupe engendré par une partie doit être connue et les groupes monogènes et cycliques doivent être évoqués. Les groupes $\mathbf{Z}/n\mathbf{Z}$ fournissent des exemples naturels tout comme les groupes de permutations, les groupes linéaires ou leurs sous-groupes (par exemple $\mathrm{SL}_n(K), \mathrm{O}_n(\mathbf{R})$ ou $\mathrm{SO}_n(\mathbf{R})$). Ainsi, on peut s'attarder sur l'étude du groupe des permutations avec différents types de parties génératrices en discutant de leur intérêt (ordre, simplicité de A5 par exemple). On peut, en utilisant des parties génératrices pertinentes, présenter le pivot de Gauss, le calcul de l'inverse ou du rang d'une matrice, le groupe des isométries d'un triangle équilatéral. Éventuellement, il est possible de discuter des conditions nécessaires et suffisantes pour que $(\mathbf{Z}/n\mathbf{Z})^*$ soit cyclique ou la détermination de générateurs du groupe diédral. On illustre comment la connaissance de parties génératrices s'avère très utile dans certaines situations, par exemple pour l'analyse de morphismes de groupes, ou pour montrer la connexité par arcs de certains sous-groupes de $\mathrm{GL}_n(\mathbf{R})$. Pour aller plus loin,on peut s'intéresser à la présentation de certains groupes par générateurs et relations. Il est également possible de parler du logarithme discret et de ces applications à la cryptographie (algorithme de Diffie-Hellman, cryptosystème de El Gamal).

Plan

I. Parties génératrices

I.1. Définition

Lemme : sous-groupes stables par intersection
Définition : groupe engendrée par une partie
Pro : description du sous-groupe engendrée
ex : sous-groupes engendré par une famille d'éléments sur $\mathbf{Z}$.
définition : partie génératrice
ex : à quelle condition une famille est génératrices dans $\mathbf{Z}$.

I.2. Groupes engendrés par un élément

définition : groupe monogènes
pro : caractérisation des groupes cycliques = cycliques ou infini, isomorphisme.
ex : groupe des racines de l'unité.
propriétés des groupes cycliques :

1. nombres de générateurs
2. un sous-groupe de tout ordre avec description
3. app : formule d'Euler
4. caractérisation = être cyclique si et seulement si un unique sous-groupe à tout ordre
5. app : le groupe multiplicatif d'un corps est cyclique.

Théorème 7. Critère de cyclicité de $(\mathbf{Z}/n\mathbf{Z})^\times$

app : caractérisation Carmichael.
app : critère irréductibilité polynômes cyclotomiques.

I.3. Groupes engendrés par plus d'un élément

ex : système de générateur à deux éléments du groupe symétrique.
pro : Frattini (Où ?)
app : Structure des p-groupes.

II. Parties génératrices usuelles des groupes usuels

II.1. Parties génératrices

Groupe symétrique

Définition : transpositions.
Pro : les transpositions engendrent S_n.
app : groupe de symétrie du tétraèdre.
Pro : minimalité des systèmes de générateurs
ex : $(1\,i)$ et $(i\,i+1)$.
app : automorphismes intérieurs de S_n.

Groupe linéaire

Définition : transvections et dilatations
pro : les transvections engendrent SL, les dilatations engendrent GL.
app : Frobenius-Zolotarev
pro : point de vue matricielle, restriction aux transvections élémentaires (pivot de Gauss) attention pas les dilatations.

Groupe orthogonal

Définition : réflexion
pro : les réflexions engendrent $\mathrm{O}_n(\mathbf{R})$.
app : isomorphisme des quaternions
pro : représentation matricielle, matrices de Householder.

II.2. Nombres de facteurs

Groupe symétrique

pro : parité du nombre de transpositions, définition de la signature.

Proposition 26. Le nombre minimal de transpositions nécessaire pour écriture une permutation $\sigma \in \mathrm{S}_n$ est $n-k$ où k est le nombre de cycles de σ.

Groupe linéaire

def : endomorphismes exceptionnels.
pro : le nombre minimal...

Groupe orthogonal

pro : la parité du nombre de réflexions lié au déterminant.
pro : nombre minimal de réflexion.

Remarque 31. Avec la représentation de S_n dans $\mathrm{O}_n(\mathbf{R})$ on retrouve les énoncés sur les permutations.

II.3. Application à l'étude de la structure des groupes usuelles

Simplicité du groupe alterné

Lem : Les 3-cycles sont conjugués ($n \geqslant 5$) et engendrent le groupe alternée.
th : simplicité du groupe alterné ($n \geqslant 5$)
rem : que se passe t-il pour $n = 4$, les 3 cycles forment deux classes de conjugaisons distinctes.
app : nombres de valeur que peut prendre un polynôme après permutations des racines
app : pour avoir un automorphisme non intérieur de S_6 il suffit de connaitre une action transitive de S_5 sur un ensemble à 6 éléments.

Simplicité du groupe projectif linéaire

Lem : Pour $n \geqslant 3$ les transvections sont conjugués.
th : simplicité de $\mathrm{PSL}_n(K)$ dans le cas $n \geqslant 3$.
rem : extension à $n = 2$.
pro : isomorphismes exceptionnels
app : action transitive de S_5 sur un ensemble à 6 éléments.

Simplicité du groupe projectif orthogonal

Lem : les renversements engendrent S_n et son conjugués.
th : simplicité du groupe orthogonal sauf $n = 4$
pro : cas $n = 4$ avec les quaternions.

III. Présentation d'un groupe par générateur et relations

III.1. Définition

Lemme 46 (Admis)**.** Soit X un ensemble. Il existe un groupe F tel que pour tout groupe G, toute fonction $f : X \to G$ se prolonge en un morphisme de groupe $\overline{f} : F \to G$. Ce groupe G est unique à isomorphisme près et est appelé groupe libre engendré par X et est noté F_X.

Définition 47. Une présentation d'un groupe G est la donnée d'un ensemble X et d'une partie R de F_X tel que G soit isomorphisme à $F_X/ << R >>$ groupe distingué engendré par R. Dans ce cas on note :

$$G \simeq \langle X \mid R \rangle.$$

Exemple 48.
1. Une présentation de $\mathbf{Z}/n\mathbf{Z}$ est $\langle a \mid a^n = 1 \rangle$.
2. Une présentation de D_n est $\langle a, b \mid a^2 = b^n = abab = 1 \rangle$.
3. Présentations de Coxeter associé au système générateur $s_i = (i\, i+1)$

$$\begin{aligned} s_i^2 &= 1 \\ (s_i s_{i+1})^3 &= 1 \\ s_i s_j = s_j s_i \ &|i-j| \geqslant 1. \end{aligned}$$

App : il existe un automorphisme non intérieur de S_6.

III.2. Présentation des groupes abéliens : théorème de structure

Lemme 49. Soit $A \in \mathscr{M}_{n,k}(\mathbf{Z})$. Il existe une matrice $P \in \mathrm{GL}_n(\mathbf{Z})$, une matrice $Q \in \mathrm{GL}_k(\mathbf{Z})$ de déterminants ± 1 et des entiers strictement positifs d_i tels que $d_1 | d_2 | \cdots | d_l$ et,

$$PAQ = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_k & \\ & & & \mathbf{0} \end{pmatrix}.$$

De plus la suite $(d_1, \cdots, d_l)$ avec les conditions précédentes est unique.

Théorème 50. Soit G un groupe abélien de type finie. Il existe une unique suite $(d_1, \cdots, d_l)$ d'entiers strictement positif avec $d_1 | \cdots | d_l$ et un unique entier r tel que

$$G \simeq \mathbf{Z}^{d_1} \times (\mathbf{Z}/d_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_l\mathbf{Z}) \times \mathbf{Z}^r.$$

ex : prenons un ordre et regardons les groupes abéliens...
rem : algorithme pour obtenir smith. .

Application 53. Soit G un groupe abélien fini. Les caractères forment une base orthonormée de $L^2(G, \mathbf{C})$. Cela permet de définir la transformée de Fourier sur un groupe abélien fini.

120 : Anneaux Z/nZ. Applications.

Il est attendu de construire rapidement $\mathbf{Z}/n\mathbf{Z}$ puis d'en décrire les éléments inversibles, les diviseurs de zéro et les idéaux. Ensuite, le cas où l'entier n est un nombre premier doit être étudié. La fonction indicatrice d'Euler ainsi que le théorème chinois et sa réciproque sont incontournables. Il est naturel de s'intéresser à la résolution des systèmes de congruences. Les applications sont très nombreuses. Les candidates et candidats peuvent, par exemple, choisir de s'intéresser à la résolution d'équations diophantiennes (par réduction modulo n bien choisi) ou bien au cryptosystème RSA. Si des applications en sont proposées, l'étude des morphismes de groupes de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{Z}/m\mathbf{Z}$ ou le morphisme de Frobenius peuvent figurer dans la leçon. Pour aller plus loin, les candidates et candidats peuvent poursuivre en donnant une généralisation du théorème chinois lorsque deux éléments ne sont pas premiers entre eux, s'intéresser au calcul effectif des racines carrées dans $\mathbf{Z}/n\mathbf{Z}$, au logarithme discret, ou à la transformée de Fourier rapide.

I. Description de l'anneau $\mathbf{Z}/n\mathbf{Z}$

I.1. Des congruences à $\mathbf{Z}/n\mathbf{Z}$

Définir la relation mod et les règles de calculs.

Application 2. *Critère de divisibilité (Méthode de Pascal)*
Pour tester la divisibilité par d on calcule les restes de 10^k par d, cette suite est périodique on peut alors remplacer chaque puissance de d par son reste.

1. pour $d = 2$ les restes sont $1, 0, 0, 0$ etc... un nombre est divisible par 2 si et seulement si son chiffre des unités est $0, 2, 4, 6$ ou 8 ;
2. pour $d = 3$ les restes sont $1, 1, 1, 1$ etc... un nombre est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3 ;
3. etc...

Définition formelle de l'anneau $\mathbf{Z}/n\mathbf{Z}$ = classes d'équivalences avec loi induite.

Exemple 4. Soit $q = \frac{m}{n}$ une fraction rationnel irréductible. Le développement décimal de q est période de période l'ordre de 10 dans $(\mathbf{Z}/n_1\mathbf{Z})^\times$ où $n = n_1 n_2$ avec n_1 premier avec 10 et n_2 produits de 2 et de 5.

I.2. Éléments de $\mathbf{Z}/n\mathbf{Z}$.

Description de l'anneau : $\mathbf{Z}/n\mathbf{Z}$ anneau commutatif cardinal n avec :
- — inversibles = classes d'éléments premiers avec n ;
- — diviseurs de zéros = classes d'éléments non premiers avec n ;
- — nilpotents = classes d'éléments divisibles par le radical de n.

Corollaire : $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est premier
app : théorème de Wilson $(n-1)! \equiv -1 \mod n$ si et seulement si n est premier.
Corollaire : le groupe des inversibles de $\mathbf{Z}/n\mathbf{Z}$ est de cardinal $\varphi(n)$ où φ est l'indicatrice d'Euler et on a $a^{\varphi(n)} \equiv 1 \mod n$ pour tout a premier avec n.
Le dernier chiffre en base 10 de 7^{3^9} est 3 (Voyage en algébrie).
app : cryptographie RSA [Gou21].

I.3. Structure de l'anneau $\mathbf{Z}/n\mathbf{Z}$

Théorème chinois

Proposition 11. Soient $m_1, \cdots, m_k$ des entiers deux à deux premiers entre eux. Alors l'application $x \in \mathbf{Z} \mapsto (x \mod m_1, \cdots, x \mod m_k)$ se factorise en un isomorphisme d'anneaux :

$$\mathbf{Z}/m_1 \cdots m_k\mathbf{Z} \longrightarrow \mathbf{Z}/m_1\mathbf{Z} \times \cdots \times \mathbf{Z}/m_k\mathbf{Z}.$$

Ainsi quelque soit $(a_1,\cdots,a_k)\in\mathbf{Z}^n$ le système de congruences $x\equiv a_i \mod m_i$ avec $1\leqslant i\leqslant k$ admet une solution x_0 et l'ensemble des solutions est $x_0+m_1\cdots m_k\mathbf{Z}$.

app : idempotents de $\mathbf{Z}/n\mathbf{Z}$.
cor : interprétation en termes de systèmes de congruences, réciproque explicite avec théorème chinois
ex : résolution d'un système de congruences

Proposition 15. Soient $m_1,\cdots,m_k$ des entiers non nuls. Le système de congruence $x\equiv x_i \mod m_i$ possède une solution si et seulement si pour tout $i\neq j$,

$$x_i\equiv x_j \mod (m_i\wedge m_j).$$

Groupe additif

Pro : description de $(\mathbf{Z}/n\mathbf{Z},+)$.
app : $n=\sum_{d|n}\varphi(d)$.
pro : Lien entre automorphisme de $\mathbf{Z}/n\mathbf{Z}$ et inversibles de $\mathbf{Z}/n\mathbf{Z}$.
app : détermination de structure de certains produits semi-directs.

Groupe des inversibles

Référence : [Per96]
Th : structure de $(\mathbf{Z}/n\mathbf{Z})^\times$ [**DEV1**].
cor : critère de cyclicité
app : irréductibilité des polynômes cyclotomiques [Per96].
rem : en pratique il reste assez compliqué de trouver une racine primitive...
applications futurs : carrés dans $(\mathbf{Z}/n\mathbf{Z})^\times$, analyse du test de Fermat et de SS.

II. Résolutions d'équations modulaires

II.1. Réduction des équations

Principe : si $f(n)=0$ alors $f(n)\equiv 0 \mod m$.

Exemple 23. Si un nombre premier p est somme de deux carrés alors $p\equiv 1 \mod 4$.

Exemple 24. Aucun nombre de la forme $8k+7$ n'est somme de deux cubes.

Principe : si $f\in\mathbf{Z}[X]$ s'écrit $f=gh$ alors $\overline{f}=\overline{g}\overline{h}$.

Lemme 25. L'application $f=\sum_{k=0}^n a_kX^k\in\mathbf{Z}[X]\mapsto\sum_{k=0}^n\overline{a_k}X^k\in\mathbf{Z}/m\mathbf{Z}[X]$ est un morphisme d'anneau.

Exemples du Perrin sur l'irréductibilité.
Pro : critère d'Eisenstein
exemples...

II.2. Résidus quadratique

Référence : [Dem97]
Lem : dévissage avec le théorème chinois.
pro : critère d'Euler sur un groupe d'ordre pair.
cor : pour $p\neq 2$ les carrés dans $\mathbf{Z}/p^k\mathbf{Z}$ sont exactement les relèvements des carrés de $\mathbf{Z}/p\mathbf{Z}$.
app : première loi complémentaire.
rem : a inversible mod 2^k carré mod 2^k $(k\geqslant 3)$ si et seulement $a\equiv 1 \mod 8$

II.3. Loi de réciprocité quadratique

Définition : symbole de Zolotarev.

Proposition 32 (DEV2). Si p un premier impair et a un entier premier avec p alors $(a\,|\,q)$ est égal $\left(\frac{a}{p}\right)$.
Plus généralement pour $u\in\mathrm{GL}_n(\mathbf{F}_p)$ la signature de u vu comme une permutation de $\mathbf{F}_q$ est égal à $\left(\frac{\det(u)}{p}\right)$.

Application 33. Pour tout nombre premier p impair $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

Proposition : loi de réciprocité quadratique symbole de Zolotarev.
corollaire : le symbole de Zolotarev coïncide avec le symbole de Jacobi.

Application 34. A quels conditions peut on représenter un nombre premier p comme x^2+dy^2. Dans ce cas on a d carré mod p puis loi de réciprocité quadratique... Par exemple pour $d=2$ on doit avoir $p\equiv 1,3 \mod 8$.

III. Aspects numériques

III.1. Opérations et coûts

Référence : [Dem97]
Description des coûts
Proposition : exponentiation rapide
app : test de Lucas-Lehmer
ex : Test de Pépin. app : Test de Fermat.

Proposition 35. Soit n un entier composée. Un résidu $a \in (\mathbf{Z}/n\mathbf{Z})^\times$ est appelé menteur (resp. temoin) de Fermat si $a^{n-1} \equiv 1 \mod n$ resp $\not\equiv$. Il existe des nombres entiers tels que résidu soit un menteur, on les appelle les nombres de Carmichael ils sont caractérisés par : n sans facteurs premiers et $p-1$ divise $n-1$ si p divise n. Sinon, il y a moins $\frac{\varphi(n)}{2}$ menteurs.

III.2. Résidus quadratiques

Référence : [Dem97]
def : symbole de Jacobi
pro : calcul rapide
app : test de SS
pro : menteurs du test SS

III.3. Systèmes de congruences

Référence : [SP99]
Rem : la solution donnée par la proposition précédente n'est pas forcément la meilleur et peu même aboutir à des débordements de mémoires, problème que n'a pas l'algorithme de Garner
Algorithme de Garner On définit par récurrence la suite t_i avec $t_0 = 1$ et,

$$t_{i+1} = (m_1 \cdots m_i^{-1}(a_{i+1} - t_1 + t_2 m_1 + \cdots + t_i m_1 \cdots m_{i-1}) \mod m_{i+1}.$$

Alors $t_0 x_1 + t_1 x_2 + \cdots + t_{k-1} x_k$ est solution du système de congruence $x \equiv a_i \mod m_i$ avec $1 \leqslant i \leqslant k$
pro : complexité de l'algorithme $O(n \log^2(m_1 \cdots m_k))$.
app : calcul parallèle, exemples du déterminant avec bornes de Hadamard.

121 : Nombres premiers. Applications.

Le sujet de cette leçon est très vaste. Elle doit donc être abordée en faisant des choix qui devront être clairement motivés. On attend une étude purement interne à l'arithmétique des entiers, avec des applications dans différents domaines : théorie des corps finis, théorie des groupes, arithmétique des polynômes, cryptographie, etc. On peut définir certaines fonctions importantes en arithmétique, les relier aux nombres premiers et illustrer leurs utilisations. Il est recommandé de s'intéresser aux aspects algorithmiques du sujet (tests de primalité). La réduction modulo p n'est pas hors-sujet et constitue un outil puissant pour résoudre des problèmes arithmétiques simples. La répartition des nombres premiers doit être évoquée : certains résultats sont accessibles dans le cadre du programme du concours, d'autres peuvent être admis et cités pour leur importance culturelle.

Définition 1. Un entier p est dit premier lorsque p est non inversible et ne possède aucun diviseur non trivial.

I. Les nombres premiers

I.1. Décomposition des entiers

- Définition des nombres premiers
- Théorème fondamental de l'arithmétique (introduire valuation p-adique).
- Application : les problèmes de divisibilité se ramène à un problème sur les nombres premiers. Par exemple on a l'expression suivante de l'indicatrice d'Euler $\varphi(n) = (p_1 - 1)p_1^{\alpha_1} \cdots (p_k - 1)p_k^{\alpha_k - 1}$ qui peut
- Remarque : quel est le nombre typique de facteurs premiers d'un entier n ? La réponse apportée par Hardy et Ramanujan est $\log\log n$ précisément pour toute fonction $\psi : [0, +\infty) \to [0, +\infty)$ tel que $\lim_{x \to +\infty} \psi(x) = +\infty$ on a :
$$\frac{1}{N} \# \left\{ 1 \leqslant n \leqslant N \, : \, |\omega(n) - \log\log n| > \psi(n)\sqrt{\log\log n} \right\} = o(1).$$
- Remarque : difficulté factorisation d'un entier en nombres premiers

I.2. Répartition des nombres premiers

- Infinité des nombres premiers (Euclide)
- Résultats quantitatifs : second théorème de Mertens, théorème de raréfaction de Legendre, théorème des nombres premiers [admis]
- Répartition aléatoire : il existe une infinité de nombres premiers de la forme $4n + 1$ ou $4n + 3$ plus généralement théorème de la progression arithmétique de Dirichlet [admis]

I.3. Répartition des nombres premiers

II. Réduction modulaire, cas particulier des nombres premiers

II.1. L'anneau $\mathbf{Z}/n\mathbf{Z}$

- Définition avec description groupe cyclique, groupe multiplicatif, cas particulier nombre premier avec structure de corps.
- Isomorphisme chinois et conséquences ?
- Structure du groupe multiplicatif avec application à l'analyse du test de Fermat

II.2. Résidus quadratiques modulo un nombre premier

- Définition, critère d'Euler et définition du symbole de Legendre
- Loi de réciprocité quadratique avec loi complémentaire application au calcul rapide du symbole de Legendre
- Exemple : un exemple bébé
- Application : test de Solovay-Strassen

II.3. Application à l'irréductibilité des polynômes

- Définition morphisme de réduction et règles de calcul modulo p avec le Frobenius
- Préservation de l'irréductibilité avec exemples
- Critère d'Eisenstein avec exemples

III. Structure des groupes finis

III.1. Ordre des éléments

- Théorème de Lagrange
- conséquence : tout groupe d'ordre premier est cyclique
- Théorème de Cauchy
- rem : contre-exemple lorsque pas premier

III.2. Sous-groupes distingués et complémentaires

- Rappels sous-groupes distingués et quotient
- Lemme d'Ore ou théorème de Frobenius
- Rappels complémentarité et produit semi-direct
- Caractérisation complémentarité de deux sous-groupes selon leur ordre
- Application : classification des groupes d'ordre pq.

III.3. Théorèmes de Sylow

Théorème 7. *Théorèmes de Sylow*
Soit G un groupe fini puis p un diviseur premier de son ordre. Alors,

- G possède au moins un p-Sylow ;
- les p-Sylow de G sont tous conjugués ;
- le nombre n_p de p-Sylow de G satisfait aux deux conditions

$$n_p \text{ divise } |G|, \qquad n_p \equiv 1 \mod p.$$

Application 8. *Classification des groupes d'ordre 12*
IL existe à isomorphisme près 5 groupes non abéliens d'ordre 12 dont deux groupes abéliens $\mathbf{Z}/12\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ et trois groupes non-abéliens dont D_6, A_4 et un nouveau groupe le groupe dicyclique d'ordre 12 qui se présente

$$\langle a, b \mid a^3 = b^4 = bab^{-1}a^{-2} = 1 \rangle.$$

122 : Anneaux principaux. Exemples et applications.

Cette leçon ne doit pas se cantonner aux aspects théoriques. L'arithmétique des anneaux principaux doit être décrite et les démonstrations doivent être maîtrisées (lemme d'Euclide, théorème de Gauss, décomposition en irréductibles, PGCD et PPCM, équations de type $ax+by=d$, etc.). On doit présenter des exemples d'utilisation effective du lemme chinois. Les anneaux euclidiens représentent une classe importante d'anneaux principaux et l'algorithme d'Euclide a toute sa place dans cette leçon pour effectuer des calculs. Les applications en algèbre linéaire ne manquent pas et doivent être mentionnées (par exemple, le lemme des noyaux ou la notion de polynôme minimal pour un endomorphisme, pour un endomorphisme relativement à un vecteur ou pour un nombre algébrique). Si les anneaux classiques $\mathbf{Z}$ et $K[X]$ doivent impérativement figurer, il est possible d'en évoquer d'autres (décimaux, entiers de Gauss $\mathbf{Z}[\mathrm{i}]$ ou d'Eisenstein $\mathbf{Z}[\mathrm{e}^{\frac{2\mathrm{i}\pi}{3}}]$) accompagnés d'une description de leurs inversibles, de leurs irréductibles, en lien avec la résolution de problèmes arithmétiques (équations diophantiennes). Les candidates et candidats peuvent aller plus loin en s'intéressant à l'étude des réseaux, à des exemples d'anneaux non principaux, par exemple $\mathbf{Z}[X]$ ou $K[X,Y]$. À ce sujet, il sera fondamental de savoir déterminer les unités d'un anneau, et leur rôle au moment de la décomposition en facteurs premiers. De même, la résolution des systèmes linéaires sur $\mathbf{Z}$ ou le calcul effectif des facteurs invariants de matrices à coefficients dans un anneau principal peuvent être présentés en lien avec ce sujet.

I. Décomposition en facteurs irréductibles

Exemple 1. *Exemple introductif*
à quelle condition 2^n+1 est un carré ?

I.1. Critère de décomposition en facteurs irréductibles

def : éléments irréductibles, éléments premiers, caractérisation en termes d'idéaux et en termes de quotients.
propriétés d'existence et d'unicité d'une décomposition en facteurs irréductibles.
def : anneaux noethérien avec les propriétés équivalentes et propriétés de stabilité [Per96]
pro : un anneau noethérien intègre vérifie la propriété d'existence
app : $\mathbf{Z}[\alpha_1,\cdots,\alpha_d]$ vérifie la propriété d'existence.
pro : critères d'unicité sous existence [Per96] en rajoutant la ligne être un anneau à pgcd
rem :

1. la réciproque du résultat d'existence est faux $\mathbf{Z}[X_n \mid n \in \mathbf{N}]$, on peut affiner le résultat en demander seulement que tout suite croissante d'idéaux principaux est stationnaire.
2. $\mathbf{Z}[\mathrm{i}\sqrt{5}]$ n'est pas factoriel : $3\times 3=(2+\mathrm{i}\sqrt{5})(2-\mathrm{i}\sqrt{5})$.

I.2. Factorialité des anneaux principaux

def : anneaux principaux [Per96]
pro : un anneau principal est factoriel [Per96]
rem La réciproque est fausse, on peut montrer que si A à la propriété de factorialité alors $A[X]$ également quand bien même A n'est pas un corps (théorème de transfert de Gauss). Il faut demander plus de propriétés à un anneau factoriel pour qu'il soit principal, par exemple être noéthérien et que tout irréductible engendre un idéal maximal.
def : anneaux euclidiens
pro : tout anneau euclidien est principal
ex :

- Anneaux euclidiens : $\mathbf{Z}$ et $K[X]$.
- La réciproque est fausse $\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais n'est pas euclidien.

lem : lemme du Perrin pour le dernier point.

I.3. Exemples d'équations diophantiennes

Problèmes des deux carrés

voir la rédaction du problème

Équation de Mordell

faire pour $\mathbf{Z}[i\sqrt{2}]$ mettre en remarque le cas $\mathbf{Z}[i]$.

Remarque 16. Sur les anneaux $\mathbf{Z}[i\sqrt{d}]$ connaitre un peu leur histoire.

II. Relation de Bézout dans les anneaux principaux

II.1. PGCD et Relation de Bézout

def : pgcd
pro : relation de Bézout dans un anneau principal (cas général)
ex : un exemple sur les entiers pgcd + Bézout, un exemple sur les polynômes
app : décomposition caractéristique
rem : relation de Bézout pas caractéristique des anneaux principaux ex : fonctions entières. Toutefois si un anneau noethérien est de Bézout alors principal

II.2. Inversion dans le quotient, interprétation des coefficients

pro : critère d'inversion dans un quotient
ex : inversion dans un corps fini, inversion dans $\mathbf{Z}/n\mathbf{Z}$
cor : systèmes de congruences
ex : exemple de système de congruence d'entiers
ex : exemple d'interpolation polynomiale avec Lagrange
ex : Polynôme qui donne Dunford

II.3. Calcul effectif par l'algorithme d'Euclide

Algorithme d'Euclide étendue
app : permet informatique de trouver l'inverse dans $\mathbf{Z}/n\mathbf{Z}$, un corps fini et de résoudre des systèmes de congruences
app : écriture un nombre premier comme somme de deux carrés
Quelques mots sur la complexité

III. Décomposition de matrices sur un anneau principal

III.1. Réduction en une matrice échelonnée

Lemme 32. La simplification de base, il existe une matrice tel que blablabla... Dans le cadre euclidien, cette matrice est le produit de matrices correspondant à des opérations élémentaires sur les lignes.

app : Résolution de l'équation diophantienne $ax + by = c$.

Théorème 33. *Réduction d'Hermite*
Soit $A \in \mathcal{M}_{n,p}(R)$ une matrice sur un anneau principal[9] R. Il existe une matrice $P \in \mathrm{SL}_n(R)$ (resp. $Q \in \mathrm{SL}_p(R)$) tel que PA (resp. AQ) soit échelonné en lignes (resp. colonnes). De plus si l'on fixe un système de représentants des éléments de A modulo les inversibles et qu'on impose aux pivots d'être dans ce système de représentant (par exemple dans $\mathbf{Z}$ on peut imposer aux pivots d'être > 0) alors il y a unicité de la réduite d'Hermite.

Remarque 34. Dans le cadre euclidien, algorithme.

Application 35. Résolution du système diophantien $2x + 3y + 5z = 0$.

9. Cette hypothèse n'est pas optimal mais soit.

III.2. Réduction en une matrice diagonale

Théorème 36. Théorème de Smith.

Application 37. Structure des groupes abéliens de type fini

Application 38. Théorème de réduction de Frobenius [oui mais à revoir]

Remarque 39. Dans le cadre euclidien, algorithme.

Corollaire 40. Si A euclidien alors $\mathrm{GL}(A)$ engendré par les matrices élémentaires. Ce résultat est faux sur un anneau principal !

123 : Corps finis. Applications.

La construction des corps finis doit être connue et une bonne maîtrise des calculs dans les corps finis est indispensable. Le calcul des degrés des extensions, le théorème de la base télescopique, les injections des divers $\mathbf{F}_q$ sont incontournables. La structure du groupe multiplicatif doit aussi être connue. Des applications des corps finis (y compris pour $\mathbf{F}_q$ avec q non premier !) ne doivent pas être oubliées. Par exemple, l'étude de polynômes à coefficients entiers et de leur irréductibilité peut figurer dans cette leçon. L'étude des carrés dans un corps fini et la résolution d'équations de degré 2 sont des pistes intéressantes. Les candidates et candidats peuvent aller plus loin en détaillant des codes correcteurs ou en étudiant l'irréductibilité des polynômes à coefficients dans un corps fini.

I. Analyse des corps finis

Références : Perrin (chap III-2 p.72) ou Demazure (chap 9. p207)

I.1. Caractéristique et sous-corps premier

1. Caractéristique, sous-corps premier
2. Corollaire : extension de $\mathbf{Z}/p\mathbf{Z}$ en particulier de cardinal une puissance de p.

I.2. Morphisme de Frobenius

3. Lemme binomiale, il en découle que si A est un anneau de caractéristique p alors $x \mapsto x^p$ est compatible avec la somme.
4. Le frobenius = automorphisme de corps, application $\mathbf{Z}/p\mathbf{Z}$-linéaire dont l'ensemble des points fixes est le sous-corps premier.

I.3. Groupe multiplicatif

5. Le groupe multiplicatif d'un corps fini est cyclique
6. Corollaire : écriture comme corps de décomposition
7. Corollaire : automorphismes d'un corps fini

II. Structure des corps finis

II.1. Existence et unicité

Référence : Perrin p.73 [Per96]

8. Existence et unicité du corps fini à p^r éléments
9. Remarque Perrin sur l'unicité

II.2. Inclusion entre les corps finis

Référence : Demazure p.210 [Dem97]

10. Lemme de divisibilité
11. Description des inclusions entre les corps finis

II.3. Construction en tant que corps de rupture

Référence : Demazure p.219 [Dem97]

12. Relation entre polynômes irréductibles
13. Corollaire : dénombrement des polynômes irréductibles
14. Corollaire : test de primalité de Rabin

15. application : construction pratique des corps finis
16. Exemple le corps à 4 éléments avec le polynôme X^2+X+1.

III. Applications

III.1. Utilisation de racines imaginaires

Référence : Demazure chapitre 5 p.111 [Dem97]

17. Pré-requis : critère d'Euler
18. app : première loi complémentaire
19. Sommes de Gauss
20. Loi de réciprocité quadratique
21. app : critère de Solovay-Strassen
22. app : si $p = x^2+3y^2$ avec $p \neq 3$ alors $p \equiv 1 \mod 3$ et bien d'autres.

III.2. Groupe linéaire sur un corps fini

Référence : Perrin chapitre 4 autour de la page 100 [Per96]

22. $\mathrm{GL}_n(\mathbf{F}_q)$ de cardinal $(q^n-1)\cdots(q-1)$, description de sa structure
23. Isomorphismes exceptionnels
24. Deuxième plus petit groupe simple d'ordre 168.
25. Théorème de Frobenius-Zolotarev (**DEV2**)
26. ex : signature du Frobenius
27. app : deuxième loi complémentaire

III.3. Irréductibilité de polynômes à coefficients entiers

Référence : Perrin p.76-79 [Per96]

28. l'irréductibilité entraine l'irréductibilité
29. app : $X^p - X - 1$
30. pro : critère d'Eisenstein
31. app : Φ_p
32. critère d'irréductibilité dans un corps fini par les extensions
33. polynômes cyclotomiques réduits
34. rem : que dire des polynômes cyclotomiques en général

125 : Extensions de corps. Exemples et applications

Les extensions de degré fini, le théorème de la base télescopique et ses applications à l'irréductibilité de certains polynômes, ainsi que les corps finis, sont incontournables. Il est souhaitable d'introduire la notion d'élément algébrique et d'extension algébrique en en donnant des exemples. Il faut savoir calculer le polynôme minimal d'un élément algébrique dans des cas simples, notamment pour quelques racines de l'unité. La leçon peut être illustrée par des exemples d'extensions quadratiques et leurs applications en arithmétique, ainsi que par des extensions cyclotomiques. Pour aller plus loin, les candidates et candidats peuvent montrer que l'ensemble des nombres algébriques forme un corps algébriquement clos, par exemple en expliquant comment l'utilisation du résultant permet de calculer des polynômes annulateurs de sommes et de produits de nombres algébriques. Il est possible de s'intéresser aux nombres constructibles à la règle et au compas, et éventuellement s'aventurer en théorie de Galois.

I. Extensions de corps

Référence : Perrin.

I.1. Définition

1. Définition
2. Proposition fondamentale, définition du degré.
3. Remarque de Jérémy sur les subtilités liés à l'injection
4. Extensions de corps usuelles : $\mathbf{Q} \to \mathbf{R} \to \mathbf{C}$ et $K \to K(X)$.

I.2. Suites d'extensions

5. Théorème de la base télescopique
6. Corollaire : multiplicativité des degrés
7. app : une extension de degré premier est monogène
8. app : passage de l'irréductibilité par extension de corps

II. Constructions d'extensions par adjonctions d'éléments

II.1. Corps de rupture

Référence : Perrin p.70

7. Proposition/Définition avec description du degré et base explicite

Exemples d'utilisations de racines imaginaires

Référence : Demazure

8. Sommes de Gauss
9. Loi de la réciprocité quadratique
10. app : test de Pépin

II.2. Corps de décomposition

Référence : Perrin p.70

11. Proposition/définition avec majoration du degré
12. Exemples

Exemple des corps finis

13. Description des corps finis en tant que corps de décomposition
14. Procédure de construction d'un corps fini comme corps de rupture avec ce qu'il faut pour le développement
15. Exemple du corps à 4 éléments

II.3. Extension algébriquement close

Référence : Perrin p.71

16. Tout corps se plonge dans un corps algébriquement clos
17. Exemple $\mathbf{R}$ dans $\mathbf{C}$.

Application à l'algèbre linéaire

18. Trigonalisation dans un sur-corps
19. app : $\mathrm{Tr}(A^p) = \mathrm{Tr}(A)^p$ pour des matrices dans $\mathbf{Z}/p\mathbf{Z}$ et suite de Perrin (oraux-X-ENS)
20. Diagonalisation dans un sur-corps
21. Proposition/Définition corps parfait

III. Éléments algébriques d'une extension

III.1. Éléments algébriques

Référence : Perrin

22. Définition : algébrique vs transcendant
23. exemples : π, e, $\sqrt[n]{a}$
24. Proposition/Définition polynôme minimal et sous-corps engendré
25. exemples de polynômes minimaux : polynômes cyclotomiques, etc...

III.2. Corps des éléments algébriques

Référence : Perrin

26. Caractérisation des éléments algébriques
27. Corollaire : l'ensemble des éléments algébriques forme un sous-corps
28. application : clôture algébrique
29. Comment calculer le polynôme minimal d'une somme et d'un produit, exemples Ortiz ou le résultant (encore faut-il savoir ce que c'est)

III.3. Nombres constructibles

Référence : Perrin ou Audin

30. Définition
31. Résultats élémentaires dû aux constructions
32. Théorème de Wantzel
33. Corollaire : un sens de la constructibilité des polynômes cyclotomiques

127 : Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications.

Le jury souhaite proposer une leçon qui offre une ouverture large autour du thème des nombres et des corps de nombres utilisés en algèbre ou en géométrie. L'objectif n'est pas d'en présenter le plus possible, mais plutôt d'en choisir certains, suffisamment variés, en en expliquant la genèse et en soulignant leur intérêt par des applications pertinentes. Les nombres décimaux, dyadiques, etc. fournissent des ensembles de nombres dont l'étude, si elle est accompagnée d'applications pertinentes, a sa place dans cette leçon. Les questions d'approximation diophantienne et leur lien avec les fractions continues, sans toutefois être un attendu de la leçon, entrent dans la suite logique de ce type de considération. Le corps des nombres algébriques, ainsi que certains de ses sous-corps particuliers, comme celui formé par l'ensemble des nombres constructibles ou des sous-anneaux formés par certains ensembles d'entiers algébriques constituent des pistes d'étude. Les candidates et candidats qui maîtrisent ces notions pourront aussi s'aventurer du côté des nombres de Pisot. La transcendance de π et celle de e sont des résultats à connaître, et le candidat pourra en donner des applications s'il le désire, mais les démonstrations de ces résultats non triviaux ne sont pas exigibles. L' irrationalité de nombres remarquables ($\sqrt{2}$, nombre d'or, e, π) peut être abordée. Étudier les propriétés algébriques de certains ensembles de nombres (par exemple du type $\mathbf{Z}[\omega]$ où ω est un nombre algébrique) peut être une piste intéressante et mener à des applications en arithmétique. L'utilisation des nombres complexes ou, pour aller plus loin, des quaternions, en géométrie ou en arithmétique constitue aussi une piste exploitable pour cette leçon.

Plan

I. Nombres usuelles

I.1. $\mathbf{Z} \to \mathbf{Q} \to \mathbf{R} \to \mathbf{C}$

On ne se pose pas la question de la construction formel de ces structures.

- Entiers relatifs : décomposition en facteurs premiers
- Nombres rationnels : structure de corps, représentation en facteurs irréductibles
- Nombres réels : complétude, développement dans une base, caractérisation des rationnels
- Nombres complexes : écriture d'un nombre complexe, théorème de d'Alembert-Gauss

I.2. Détails sur le passage de Q à R

Référence : Gourdon et Duverney.

- Densité des nombres rationnels
- Problème d'approximation des réels par des rationnels : fractions continues, application à la résolution de l'équation de Pell-Fermat.
- Corollaire : critère d'irrationalité, exemple du nombre d'Euler

I.3. Autres extensions

Référence : Perrin

- Théorème de Frobenius partie 1
- Définition des quaternions
- Théorème : lien avec les groupes orthogonaux, application au dévissage de PSO4
- Théorème de Frobenius partie 2, remarque octonions

II. Nombres algébriques

II.1. Nombres et entiers algébriques

Référence : Perrin

- Définition, polynôme minimal, exemples
- Existence de nombres transcendants par un argument, exemple connus.
- Caractérisation et conséquence : structure de corps et d'anneau, exemples de polynômes minimaux de sommes.
- Calcul par le résultant (Sioux-Picart)

II.2. Place des nombres algébriques

- Un entier algébrique est irrationnel : exemple $\sqrt{2}$ est irrationnel.
- Qualité d'approximation par les rationnels avec le théorème de Liouville (Rouvière)
- app : construction de nombres transcendants.

II.3. Exemples des nombres constructibles

Référence : Perrin ou Audin.

- Définitions et préliminaire
- Théorème de Wantzel
- Corollaire constructibilité des polygones réguliers

III. Anneaux et corps de nombres

III.1. Corps de nombres

- Définition corps de nombres et anneaux associé, exemples des corps quadratiques
- Propriétés : intégralement clos, noethérien, pour ces anneaux principal équivaut à factoriel.
- Remarque sur les anneaux quadratiques bien peu sont factoriels... quelques uns sont euclidiens pour la norme classique (Duverney p.148).

III.2. Application à la résolution d'équations diophantiennes

Problème des deux carrés

Référence : Perrin

Équation de Mordell

Référence : Duverney

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

Les généralités sur les algèbres de polynômes à une variable sont supposées connues. Le bagage théorique permettant de définir corps de rupture et corps de décomposition doit être présenté. Ces notions doivent être illustrées dans différents types de corps (réels, rationnels, corps finis) ; les corps finis peuvent être illustrés par des exemples de polynômes irréductibles de degré 2, 3, 4 sur $\mathbf{F}_2$ ou $\mathbf{F}_3$. Il est nécessaire de présenter des critères d'irréductibilité de polynômes et les polynômes minimaux de quelques nombres algébriques, par exemple les polynômes cyclotomiques. Le théorème de la base télescopique, ainsi que les utilisations arithmétiques (utilisation de la divisibilité) que l'on peut en faire dans l'étude de l'irréductibilité des polynômes sont incontournables. Des applications du corps de décomposition doivent être mentionnées, par exemple en algèbre linéaire. Pour aller plus loin, on peut montrer que l'ensemble des nombres algébriques sur le corps Q des rationnels est un corps algébriquement clos, s'intéresser aux nombres constructibles à la règle et au compas, et éventuellement s'aventurer en théorie de Galois.

I. Polynômes irréductibles et factorialité

I.1. Polynômes irréductibles

1. Définition
2. Exemples sur $\mathbf{R}$ ou $\mathbf{C}$, sur $\mathbf{Q}$ il y a des polynômes irréductibles de tout degré par exemple $X^n - 2$.
3. Exemples des polynômes de petits degrés
4. Exemple polynôme minimal ?

I.2. Arithmétique des polynômes sur un corps

1. Division euclidienne, structure d'anneau euclidien
2. Bézout et application lemme des noyaux
3. rem : principal si et seulement si corps

I.3. Arithmétique des polynômes sur un anneau

Référence : Perrin

1. Lemme de Gauss
2. Description des irréductibles
3. Théorème de transfert

II. Adjonction de racines

II.1. Corps de rupture

Référence : Perrin

Proposition 1. Corps de rupture

Application 2. Si f est un polynôme irréductible de degré n sur K et L est une extension de K de degré m avec $n \wedge m = 1$ alors f est irréductible sur L.

Exemple 3. 1. X^3-2 est irréductible sur $\mathbf{Q}(\sqrt{3})$.

2. Sans l'hypothèse le théorème est faux comme l'illustre X^4+1 irréductible sur $\mathbf{Q}$ mais pas sur $\mathbf{Q}(\mathrm{i})$.

Application 4. Suite de Perrin.

II.2. Corps de décomposition

Application 5. Trigonalisation dans un sur-corps. Application :

1. $\mathrm{Tr}(A^p)=\mathrm{Tr}(A)^p$
2. Minoration de dimension commutant

II.3. Exemple des corps finis

1. théorème d'existence et d'unicité
2. Corollaire : Injections entre les corps finis
3. ecriture...

III. Preuve d'irréductibilité par réduction

III.1. Réduction

Lem : morphisme de réduction, cas particulier Frobenius.
ex : irréductibilité des polynômes cyclotomiques.
app : constructibilité

III.2. Préservation de l'irréductibilité

Proposition 6 (Perrin)**.** Soit A un anneau puis I un idéal premier de A. Soit $f(x)=a_nx^n+\cdots+a_0$ avec $\overline{a_n}\neq 0$. Si f est irréductible dans $B[X]$ avec $B=A/I$ alors f est irréductible sur $A[X]$.

Exemple 7. 1. X^3+7X+1 est irréductible sur $\mathbf{Z}[X]$ car en réduisant modulo 2 on a X^3+X+1 qui n'a pas de racines [Perrin adapté].

2. X^2+Y^2+1 est irréductible dans $\mathbf{R}[X,Y]=\mathbf{R}[X][Y]$ car modulo X on a Y^2+1 irréductible dans $\mathbf{R}[Y]$.

Proposition 8 (Perrin)**.** Soit K un corps fini puis $f\in K[x]$ de degré d. Alors, f est irréductible sur $K[X]$ si et seulement si f n'a pas de racines dans les extensions de K de degré $\leqslant d/2$.

Exemple 9 (Perrin)**.** $f(x)=x^4+8x^2+17x-1$ est irréductible sur $\mathbf{Z}[X]$. Modulo 2 on a x^4+x+1 qui n'a pas de racines dans $\mathbf{F}_2$, dans $\mathbf{F}_4=\{0,1,\alpha,\alpha+1\}$ avec $\alpha^2+\alpha+1=0$ on a $\alpha^3=1$ d'où $f(\alpha)=2\alpha+1=1$ et $f(\alpha+1)=f(\alpha^2)=1+\alpha^2+1=\alpha^2\neq 0$.

III.3. Critère d'Eisenstein

Proposition 10 (Perrin)**.** Soit A un anneau avec I un idéal premier. On suppose que :

1. $a_n\notin I$,
2. $a_i\in I$ pour $i=0,\cdots,n-1$;
3. $a_0^2\notin I$.

Alors f ne s'écrit pas comme produits de deux polynômes non constants. Si f est primitif, il est irréductible.

Exemple 11. 1. $y^2-x(x-1)(x-\alpha)$ pour tout $\alpha\in K$.

2. X^n-a avec $v_p(a)=1$ pour un certain p dans un anneau factoriel.
3. $f(x)=x^{p-1}+\cdots+1$ avec la substitution $x+1$.

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

Le candidat doit prendre soin de différencier le cadre théorique des anneaux factoriels ou principaux dans lequel sont définis les PGCD et PPCM et dans lequel s'appliquent les énoncés des théorèmes proposés et le cadre euclidien fournissant les algorithmes. Le champ d'étude de cette leçon ne peut se limiter au cas de Z, mais la leçon peut opportunément s'illustrer d'exemples élémentaires d'anneaux euclidiens, comme $\mathbf{Z}$ et $K[X]$. Une part substantielle de la leçon doit être consacrée à la présentation d'algorithmes : algorithme d'Euclide, algorithme binaire, algorithme d'Euclide étendu. Il est possible d'en évaluer le nombre d'étapes dans les pires cas et faire le lien avec les suites de Fibonacci. Des applications élémentaires sont particulièrement bienvenues : calcul de relations de Bezout, ré- solutions d'équations diophantiennes linéaires, inversion modulo un entier ou un polynôme, calculs d'inverses dans les corps de rupture, les corps finis. On peut aussi évoquer le théorème chinois effectif, la résolution d'un système de congruences et faire le lien avec l'interpolation de Lagrange. Pour aller plus loin, on peut évoquer le rôle de algorithme d'Euclide étendu dans de nombreux algorithmes classiques en arithmétique (factorisation d'entiers, de polynômes, etc). Décrire l'approche matricielle de l'algorithme d'Euclide et l'action de $\mathrm{SL}_2(\mathbf{Z})$ sur $\mathbf{Z}^2$ est tout à fait pertinent. On peut aussi établir l'existence d'un supplémentaire d'une droite dans $\mathbf{Z}^2$, ou d'un hyperplan de $\mathbf{Z}^n$, examiner l'éventuelle possibilité de compléter un vecteur de $\mathbf{Z}^n$ en une base. On peut aussi étudier les matrices à coefficients dans un anneau principal ou euclidien, et, de manière plus avancée, la forme normale d'Hermite et son application à la résolution d'un système d'équations diophantiennes linéaires. De même, aborder la forme normale de Smith, et son application au théorème de la base adaptée, permet de faire le lien avec la réduction des endomorphismes via le théorème des invariants de similitude. La leçon invite aussi, pour des candidates et candidats maîtrisant ces notions, à décrire le calcul de PGCD dans $\mathbf{Z}[X]$ et $K[X,Y]$, avec des applications à l'élimination de variables. On peut rappeler les relations entre PGCD et résultant et montrer comment obtenir le PGCD en échelonnant la matrice de Sylvester. Sur l'approximation diophantienne, on peut enfin envisager le développement d'un rationnel en fraction continue et l'obtention d'une approximation de Padé-Hermite à l'aide de l'algorithme d'Euclide, la recherche d'une relation de récurrence linéaire dans une suite ou le décodage des codes BCH.

Plan

Référence : Perrin et Sioux-Picard.

I. PGCD et PPCM

I.1. Définition dans un anneau abstrait

def : pgcd et ppcm de deux éléments, généralisation à une famille d'éléments.
pro : reformulation en termes d'idéaux
rem : en générale il n'y a pas existence d'un pgcd ni d'un ppcm, exemple $A = \mathbf{Z}[i\sqrt{5}]$ dans lequel 9 et $3(2+i\sqrt{5})$ n'ont pas de pgcd ni de ppcm. Par contre l'existence d'un ppcm implique l'existence d'un pgcd, la réciproque est fausse comme l'illustre 3 et $2+i\sqrt{5}$.

I.2. Propriétés des anneaux à pgcd, exemples

def : anneaux à pgcd. Lemme de Gauss, implique anneau à PPCM.
pro : anneaux factoriels à pgcd et réciproque.
ex : fonctions entières à pgcd mais pas factoriel.

I.3. Cas des anneaux de polynômes

Contenu de deux polynômes. Lemme du contenu de Gauss.
pro : transfert de Gauss du pgcd.
pro : transfert de Gauss de la factorialité.

II. Relation de Bézout

II.1. Définition dans un anneau abstrait

def : anneaux de Bézout. Cas particulier anneau principal.
ex : $K[X,Y]$ à pgcd mais pas de Bézout, $\mathscr{H}(\mathbf{C})$ est un anneau de Bézout non factoriel donc non principal, $K[X]$ anneau principal donc de Bézout
app : décomposition de Dunford [**DEV1**]
rem : pour un anneau de Bézout on a équivalence entre factoriel, principal, noethérien.
pro : interprétation des relations de Bézout comme inverse dans un quotient.

Proposition 1. *Décomposition de Dunford* [Perso] Soit u un endomorphisme avec χ_u scindé. On note $\chi_u = \prod_{i=1}^{s}(X-\lambda_i)^{\alpha_i}$ alors,

$$E = \bigoplus_{i=1}^{s} \mathrm{Ker}(u-\lambda_i \mathrm{Id}_E)^{\alpha_i}.$$

De plus les projecteurs sur les sous-espaces sont des polynômes en u. Si l'on note d l'endomorphisme tel que $d(x) = \lambda_i x$ sur $\mathrm{Ker}(u-\lambda_i \mathrm{Id}_E)^{\alpha_i}$ alors d est diagonalisable et $n = u-d$ est nilpotent de plus d et n sont des polynômes. Le couple (d,n) est l'unique couple tel que $u = d+n$ et $dn = nd$ est et appelée décomposition de Jordan-Chevalley de u.

Dans la suite on se restreindra aux anneaux principaux pour voir les conséquences des relations de Bézout.

II.2. Application à la résolution de systèmes de congruences

pro : isomorphisme, cas particulier anneaux de Bézout pour expliciter la réciproque avec des idéaux principaux.
Ex : systèmes de congruences entiers, interpolation de Lagrange.
rem : généralisation à des moduli non premiers entre eux.

II.3. Utilisation pour la réduction des matrices

Forme d'Hermite et forme de Smith
app : structure des groupes abéliens
app : réduction de Frobenius

III. Algorithmes de calculs

III.1. Division euclidienne dans un anneau abstrait

def : anneaux euclidiens, implique principal donc factoriel
ex : $\mathbf{Z}$, $K[X]$ et $\mathbf{Z}[i]$. Par contre $\mathbf{Z}[(1+i\sqrt{19})/2]$ pas euclidien mais principal.
app : algorithme d'Hermite et de Smith, exemple.

III.2. Algorithme d'Euclide

Description de l'algorithme d'Euclide.
app : décomposition d'un nombre en somme de deux carrés [**DEV2**]
th : analyse de l'algorithme d'Euclide sur les entiers
rem : algorithme d'Euclide binaire.

III.3. Calcul du pgcd de polynômes

Algorithme d'Euclide pour un corps
Généralisation pour des polynômes à coefficients dans un anneau comme **Z**.

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

Dans cette leçon, il est indispensable de bien définir l'ordre de multiplicité d'une racine (définition algébrique et analytique, quand c'est possible). Les fonctions symétriques élémentaires et les relations entre coefficients et racines doivent être maîtrisées et pouvoir être mises en oeuvre. Des méthodes, même élémentaires, de localisation des racines ont toute leur place et peuvent déboucher sur des résultats de topologie à propos de la continuité des racines. Il est pertinent d'introduire la notion de polynôme scindé et de citer le théorème de d'Alembert- Gauss. On peut faire apparaître le lien entre la recherche des racines d'un polynôme et la réduction des matrices. Les candidates et candidats peuvent également s'intéresser aux racines des polynômes orthogonaux, ou aux règles des signes de Descartes et de Sturm. L'étude des propriétés des nombres algébriques ont leur place dans cette leçon. La théorie des corps et le cas particulier des corps finis peuvent aussi être évoqués de façon pertinente. Les candidates et candidats peuvent aller plus loin en s'intéressant à des problèmes de localisation des valeurs propres, comme les disques de Gershgorin ou au calcul effectif d'expressions polynomiales symétriques des racines d'un polynôme. Il ne s'agit par contre en aucun cas d'adapter le plan de la leçon 141 : l'irréductibilité des polynômes peut être évoquée mais ne doit pas être l'élément central de la leçon.

I. Racines d'un polynôme

I.1. Définition

1. Morphisme d'évaluation, définition des racines
2. Exemple polynôme caractéristique dont les racines sont les valeurs propres

I.2. Caractérisation

Référence : Gourdon.

1. Division euclidienne, proposition : a racine de P si et seulement si $X-a$ divise P
2. Définition multiplicité d'une racine, cor : il n'y a pas plus de racines avec multiplicité que le degré. En particulier tout polynôme n'a qu'un nombre fini de racines.
3. Application : $\mathrm{GL}_n(\mathbf{C})$ est ouvert, connexe.
4. Formule de Taylor et caractérisation différentielle des racines.

I.3. Nombres algébriques

Définition 1. Soit L/K une extension de K. Pour $a \in L$ soit :

1. ev_a est injectif on a $K(a) \simeq K(X)$ est un K-espace vectoriel de dimension infinie ;
2. ev_a n'est pas injectif, son noyau est engendré par un unique polynôme irréductible unitaire π_a, dans ce cas $K(a) \simeq K[X]/(\pi_a)$ est un K-espace vectoriel de dimension $\deg \pi_a$.

Dans le premier cas on dit que a est transcendant sur K, dans le second on dit que a est algébrique sur K et on appelle π_a le polynôme minimal de a.

- Quelques exemples de polynômes minimaux
- Exemple : polynôme minimaux des racines de l'unité, application à la constructibilité des polygones réguliers.

- L'ensemble des nombres algébrique est un corps, exemples de calcul du polynôme minimaux de sommes et produits (Ortiz), remarque calcul par le résultant.

II. Scindement des polynômes

II.1. Extension de corps par ajout de racines

Référence : Perrin

- Définition corps de rupture
- Utilisation des racines imaginaires : suite de Perrin.

II.2. Corps de décomposition

- Corps de décomposition, majoration du degré
- Application à la trigonalisibilité, application au commutant
- Proposition : relations coefficients racines
- Exemple du Gourdon pour le calcul de $\zeta(2)$.

II.3. Polynômes symétriques

- Théorème fondamental des polynômes symétriques, Formules de Newton, Caractérisation des nilpotents par la trace, calcul du polynôme caractéristique.
- Cor : Si les coefficients vivent dans un sous-anneau B de A alors les polynômes symétriques en les racines aussi bien que ces racines ne vivent pas dans A.
- Application : nombres de Pisot, Kronecker.

III. Recherche des racines

Correspondance géométrique

- Matrices compagnon
- Autre preuve pour les nombres algébriques

III.1. Méthode QR

III.2. Localisation des racines

- Résultat élémentaire de localisation
- Bornes de Cauchy
- Disques de Gershgorin

III.3. Compte des racines

1. Compteur logarithmique, application disques de Gershgorin
2. Théorème de Rouché, application à la continuité des racines.

148 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

Dans cette leçon, il est indispensable de présenter les résultats fondateurs de la théorie des espaces vectoriels de dimension finie en ayant une idée de leurs preuves. Il est en particulier important de savoir justifier pourquoi un sous-espace vectoriel d'un espace vectoriel de dimension finie est aussi de dimension finie. On peut montrer, sur des exemples, comment la dimension finie intervient dans la démonstration de certains résultats (récurrence sur la dimension, égalité de sous-espaces par inclusion et égalité des dimensions, isomorphisme par injectivité et dimension, etc.). À cette occasion, on pourra signaler des résultats qui ne subsistent pas en dimension infinie. Le pivot de Gauss ainsi que les diverses notions et caractérisations du rang trouvent leur place dans cette leçon. Les applications sont nombreuses : existence de polynômes annulateurs, dimension de l'espace des formes n-linéaires alternées en dimension n, isomorphisme avec le dual dans le cadre euclidien et théorème de Riesz, espaces de solutions d'équations différentielles ordinaires, caractérisation des endomorphismes diagonalisables, décomposition d'isométries en produits de réflexions, dimensions des représentations irréductibles d'un groupe fini, théorie des corps finis, etc. Les caractérisations du rang peuvent aussi être utilisées pour démontrer l'invariance du rang par extension de corps, ou pour établir des propriétés topologiques (sur $\mathbf{R}$ ou $\mathbf{C}$). Pour aller plus loin, les candidates et candidats peuvent déterminer des degrés d'extensions dans la théorie des corps ou s'intéresser aux nombres algébriques. Il est également possible d'explorer des applications en analyse comme les extrémas liés. Dans un autre registre, il est pertinent d'évoquer la méthode des moindres carrés dans cette leçon, par exemple en faisant ressortir la condition de rang maximal pour garantir l'unicité de la solution et s'orienter vers les techniques de décomposition en valeurs singulières pour le cas général. On peut alors naturellement analyser l'approximation d'une matrice par une suite de matrices de faible rang.

Plan

Référence : Griffone

I. Bases d'un espace vectoriel

Référence : Griffone [Gri24].

I.1. Familles libres, génératrices et bases

- Définition familles libres, famille génératrice, base.
- Exemple : toute famille de polynômes de degrés distincts forme une base de $K_n[X]$.
- Opérations sur les bases : base du quotient, base du produit, base de l'ensemble des applications linéaires avec cas particulier base duale.

I.2. Constructions de bases

- Définition espaces vectoriels de dimension finie.
- Théorème : une base se situe entre une famille libre et une famille génératrice. En particulier existence de bases.
- Corollaire : base extraite et base incomplète
- Application : base adaptée

Méthode 8. La matrice associée à une famille de vecteurs $(v_1, \cdots, v_p)$ dans une base $\mathscr{B}$ est la matrice dont les vecteurs colonnes sont les composantes des v_i dans la base $\mathscr{B}$.

1. Si $(v_1, \cdots, v_p)$ est une famille génératrice de E, A la matrice de cette famille dans une base quelconque alors en appliquant la méthode d'élimination de Gauss-Jordan sans permuter les colonnes, les vecteurs dont l'indice i est telle qu'à la fin du processus la colonne i soit non nulle, forment une base de E.
2. Si $(v_1, \cdots, v_p)$ est une famille libre de E, A la matrice de cette famille dans une base quelconque, si l'on applique la méthode d'élimination de Gauss-Jordan on peut compléter cette famille en une base en ajoutant les vecteurs éléments $(0, \cdots, 0, 1, 0, \cdots, 0)^\mathsf{T}$ aux pivots manquant.

I.3. Déterminant d'une famille de vecteurs

- Définition du déterminant dans une base
- Propriété fondamental du déterminant avec formules de Cramer pour les coordonnées

II. Dimensions d'un espace vectoriel

II.1. Définition de la dimension

- Lemme d'échange
- Théorème de la dimension
- Exemples : dimension du quotient, du produit cartésien, des applications linéaires
- Conséquence : une famille libre à moins de n éléments, une famille génératrice à plus de n éléments, base = famille libre maximal = famille génératrice minimal
- Application : existence d'un polynôme annulateur pour une algèbre de dimension finie. Deux cas d'applications, dans un cas rappeler théorème de Cayley-Halmilton dans l'autre en déduire que l'ensemble des nombres algébrique est un corps.

II.2. Dimension d'un sous-espace vectoriel

- Soit E un K-espace vectoriel de dimension finie et F un s.e.v de E. Alors, F est un K-espace vectoriel de dimension et $\dim F \leqslant \dim E$ avec égalité si et seulement si $E = F$.
- Application de l'argument d'inclusion : un exemple ?
- Opérations sur les sous-espaces vectoriels : formule de Grassman
- Conséquence : caractérisation des sous-espaces supplémentaires

II.3. Dualité

Définition 18. Soit E un K-espace vectoriel de dimension finie.

- A un s.e.v F de E on associe $F^\circ = \{\phi \in E \mid \phi(x) = 0,\ \forall x \in E\}$
- A un s.e.v G de E' on associe ${}^\circ G = \{x \in E\ :\ \phi(x) = 0,\ \forall f \in G\}$.

Proposition 19. Les applications $F \mapsto F^\circ$ et $G \mapsto G^\circ$ sont des bijections réciproques de l'ensemble des sous-espaces vectorielles de E vers l'ensemble des sous-espaces vectoriels de F. De plus,

$$\dim F^\circ = \dim E - \dim F \quad \text{et} \quad \dim G^\circ = \dim E - \dim F.$$

Corollaire 20. Soit F un sous-espace vectoriel de E de dimension n. Si F est de dimension k alors F est définie par $n-k$ équations linéaires indépendantes. Inversement si F est définie par l équations linéaires indépendantes, F est de dimension k.

Application : réduction de Frobenius.

Corollaire 22. Un sous-espace vectoriel E est de dimension k est l'intersection de $n-k$ hyperplans.

III. Rang d'une application linéaire

III.1. Théorème du rang

- Définition rang d'un endomorphisme
- Premier théorème d'isomorphisme avec dire isomorphisme image noyau
- Corollaire : théorème du rang, en particulier caractérisation : injectivité, surjectivité, bijectivité.
- Application : isomorphisme de Riesz.
- Corollaire : forme normale de Jordan
- app : toute hyperplan contient une matrice inversible

III.2. Caractérisation du rang par le déterminant

- Définition mineur
- Caractérisation du rang
- Cor : semi-continuité inférieur du rang
- app : adhérence des matrices de rang fixé
- cor : l'ensemble des matrices inversibles est dense

III.3. Décomposition en valeurs singulières

- SVD
- Conséquence 1 : approximation par des matrices de rang fixé
- Conséquence 2 : problème des moindres carrés

149 : Déterminant. Exemples et applications.

Dans cette leçon, il faut commencer par définir correctement le déterminant. et savoir démontrer ses propriétés fondamentales (en particulier le fait que l'espace des formes n-linéaires alternées sur un espace de dimension n est de dimension 1). La distinction entre le déterminant d'une famille de vecteurs dans une base donnée et le déterminant d'un endomorphisme doit être comprise. L'interprétation en termes de volume est essentielle. Le calcul explicite est important, mais le jury ne peut se contenter d'un déterminant de Vandermonde ou d'un déterminant circulant. Les opérations élémentaires permettant de calculer des déterminants doivent être présentées et illustrées. Parmi les applications possibles, on peut citer le polynôme caractéristique, les déterminants de Gram (permettant des calculs de distances), le déterminant jacobien (utile en calcul intégral et en probabilités), donner des exemples d'utilisation du déterminant en géométrie (coordonnées barycentriques, colinéarité, etc.) ou son rôle dans l'étude des formes quadratiques. Il est bienvenu d'illustrer la continuité du déterminant par une application. On pourra aussi s'intéresser à la différentielle. Pour aller plus loin, les candidates et candidats peuvent s'intéresser aux calculs de déterminants sur Z. Le résultant et les applications simples à l'intersection ensembliste de deux courbes algébriques planes peuvent aussi trouver leur place dans cette leçon pour des candidates et candidats ayant une pratique de ces notions.

I. Définition du déterminant

I.1. Formes k-linéaires

Référence : Gourdon

- Définition formes k-linéaires.
- Propositions équivalentes : formes alternés et antisymétrique.
- Théorème : structure des formes k-linéaires alternés.

I.2. Notions de déterminant

- Définition du déterminant d'une famille de vecteurs, formule de changement de base
- Définition du déterminant d'un endomorphisme, multiplicativité
- Définition du déterminant d'une matrice, lien avec les deux notions précédentes, exemple déterminant d'une matrice triangulaire

I.3. Propriété fondamentale

Référence : Gourdon.

- Propriété fondamentale du déterminant, caractérisation de l'inversibilité. Plus généralement caractérisation du rang.
- Exemple du résultant
- Exemple du polynôme caractéristique
- Formules de Cramer. En particulier formule de la comatrice.

II. Interprétation géométrique

II.1. Interprétation du déterminant en tant que volume

Référence : Griffone.

- Interprétation en tant que volume du déterminant
- Exemple : points remarquables du triangle
- Corollaire : interprétation du déterminant d'un endomorphisme
- remarque : théorème de Changement de variable

II.2. Formule de Gram

Référence : Gourdon.

- Théorème : formule de Gram **(DEV1)**
- Application au théorème de Muntz.
- Cor : Inégalité de Hadamard

III. Calcul du déterminant

III.1. Opérations sur les lignes et les colonnes

- Opérations sur les lignes et les colonnes
- Exemple Vandermonde généralisée
- Méthode du pivot de gauss pour le calcul de déterminant en $O(n^3)$

III.2. Formules de récurrence

Référence : Gourdon

- Développement selon une ligne, une colonne et formules de calculs
- Exemple : déterminant tri-diagonale Gourdon.

III.3. Déterminants classiques

Référence : Gourdon.

- Déterminant de Vandermonde
- Déterminant de Cauchy
- Déterminant circulant
- Déterminant compagnon

IV. Propriétés du déterminant

IV.1. Propriétés algébriques

- Morphisme de groupe de $\mathrm{GL}_n(K)$ vers K^*, description de son noyau
- Théorème de Frobenius-Zolotarev et lemmes autour **(DEV2)**

IV.2. Propriétés analytiques

- Fonction polynomiale, continue sur $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$.
- Corollaire : $\mathrm{GL}_n(\mathbf{R})$ est un ouvert dense, plus généralement adhérence des matrices de rang fixé (Algébrie)
- Différentielle du déterminant
- Corollaire : formule de Liouville

150 : Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

Cette leçon ne doit pas être un catalogue de résultats autour de la réduction ; les polynômes d'endomorphismes doivent y occuper une place importante. Il faut consacrer une courte partie de la leçon à l'algèbre $K[u]$, en particulier connaître la dimension, et aux liens entre réduction de l'endomorphisme u et structure de l'algèbre $K[u]$. Il est ensuite possible de s'intéresser aux propriétés globales de cette algèbre (inversibles, condition nécessaire et suffisante assurant que ce soit un corps...). De même il est important de mettre en évidence les liens entre les idempotents et la décomposition en somme de sous-espaces caractéristiques. Le lemme des noyaux, les polynômes caractéristiques et minimaux doivent figurer dans la leçon. Il faut bien préciser que, dans la réduction de Dunford, les composantes sont des polynômes en l'endomorphisme, et en connaître des conséquences théoriques et pratiques. On attend que la candidate ou le candidat soit en mesure, pour une matrice simple de justifier la diagonalisabilité et de déterminer un polynôme annulateur (voire minimal). L'aspect applications est trop souvent négligé. Il est par exemple possible d'envisager des applications au calcul de A^k à l'aide d'un polynôme annulateur, aux calculs d'exponentielles de matrices ou de mener l'analyse spectrale de matrices stochastiques. Pour aller plus loin, la candidate ou le candidat pourra étudier des équations matricielles et de calcul fonctionnel, avec par exemple l'étude de l'extraction de racines ou du logarithme.

I. Polynômes d'endomorphismes

I.1. Formalisme

On se donne E un K-espace vectoriel. On note $\mathscr{L}(E)$ l'ensemble des endomorphismes de E, on rappel que les lois $(+, \cdot, \circ)$ munissent $\mathscr{L}(E)$ d'une structure de K-algèbre.

Lemme 1 (Perso)**.** Pour tout $u \in \mathscr{L}(E)$ il existe un unique morphisme de K-algèbres $K[X] \to \mathscr{L}(E)$ qui envoie X sur u. Ce morphisme sera noté ev_u et envoie le polynôme $P(X) = \sum_{k=0}^{d} a_k X^d$ sur l'endomorphisme $P(u) := \sum_{k=0}^{d} a_k u^k$ où u^k désigne la k-ème composée de u.
On note $K[u]$ l'image de ev_u, c'est une sous-algèbre commutative de $\mathscr{L}(E)$.

Proposition 2 (Perso)**.** Si E est de dimension finie le morphisme ev_u n'est pas injectif, son noyau constituée des polynômes P tels que $P(u) = 0$, dits polynômes annulateurs de u, forme un idéal non trivial de $K[X]$ qui est engendré par un unique polynôme unitaire. On définit le polynôme minimal de u que l'on note π_u l'unique générateur unitaire de l'idéal des polynômes annulateurs.

Corollaire 3. On a un isomorphisme de K-algèbre $K[u] \simeq K[X]/(\pi_u)$. En particulier :

- $K[u]$ est un K-espace vectoriel de dimension $\deg(\pi_u)$;
- les inversibles de $K[u]$ sont les $P(u)$ où P est un polynôme premier avec π_u, en particulier $K[u]$ est un corps si et seulement si π_u est irréductible ;

I.2. Propriétés des polynômes annulateurs

Proposition 4. [MM22] Si P est un polynôme annulateur de u alors les valeurs propres de u sont racines de P. De plus les valeurs propres de u sont exactement les racines de son polynôme minimal.

Exemple 5. 1. Spectre des éléments d'une représentation irréductible de groupe

2. Spectre de la multiplication à gauche et à droite par une matrice. Spectre de $M \mapsto AM + MB$.

Théorème 6. *Théorème de Cayley-Hamilton* [Gou21] ou [MM22] Le polynôme caractéristique d'un endomorphisme est un polynôme annulateur.

Corollaire 7. Le polynôme minimal est de degré $\leqslant n$. De plus on a égalité si et seulement si l'endomorphisme est cyclique.

I.3. Calcul des endomorphismes

Proposition 8. Si P est un polynôme annulateur d'un endomorphisme u alors en écrivant la division euclidienne de X^k par P : $X^k = PQ + R$ on a $u^k = R(u)$.

Exemple 9. (MM) Si u est en endomorphisme de polynôme annulateur $(X-a)(X-b)$ avec a et b distincts alors,

$$u^n = \frac{a^n - b^n}{a-b}u + \frac{ba^n - ab^n}{b-a}\mathrm{Id}$$

Lemme 10. (Gourdon) Soient $x_1, \cdots, x_s \in K$ deux à deux distincts puis $y_{i,j} \in K$ des points pour $1 \leqslant i \leqslant s$ et $0 \leqslant j < \alpha_i$. Il existe un unique polynôme $P \in K[X]$ de degré $< \alpha = \sum_{i=1}^{s} \alpha_i$ tel que $P^{(j)}(x_i) = y_{i,j}$. On peut écrire :

$$P(X) = \sum_{i=1}^{s} \sum_{j=0}^{\alpha_i - 1} y_{i,j} H_{i,j}(X)$$

où $H_{i,j}$ est de degré $< \alpha$ et vérifie $H_{i,j}^{(j')}(x_{i'}) = \delta_{i,i'}\delta_{j,j'}$.

Application 11. Soit $A \in \mathscr{M}_d(\mathbf{C})$

1. La suite A^n converge si et seulement si les valeurs propres de A différentes de 1 sont de module < 1 et si 1 est valeur propre de A que cette valeur propre soit non défective.
2. La suite A^n converge vers 0 si et seulement les valeurs propres de A sont de module < 1.

Peut être qu'on peut interpréter les résultats en sachant qui est $H_{1,1}$.

Remarque 12. On peut généraliser ce genre de calculs aux calculs sur des fonctions analytiques d'endomorphismes comme l'exponentielle.

II. Décomposition en noyaux de polynômes

II.1. Décomposition caractéristique

Proposition 13. *Lemme des noyaux*
Soit u un endomorphisme puis P un polynôme annulateur de u et $¶ = P_1 \cdots P_k$ avec les P_i deux à deux premiers entre eux. Alors,

$$E = \bigoplus_{i=1}^{k} \mathrm{Ker}\ P_i(u).$$

Corollaire 14. *Décomposition caractéristique*
Si $\pi_u = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ est la décomposition en facteurs irréductibles de π_u alors,

$$E = \bigoplus_{i=1}^{k} \mathrm{Ker}\, P_i^{\alpha_i}(u).$$

Les sous-espaces $\mathrm{Ker}\, P_i^{\alpha_i}(u)$ sont appelés sous-espaces caractéristiques de u.

Application 15. On retrouve les résultats précédents. En déduire aussi des informations sur $\exp(tu)$.

Application 16. En notant u_i l'endomorphisme induit sur $\mathrm{Ker} P_i^{\alpha_i}(u)$ on a un isomorphisme de K-algèbre :

$$K[u] \simeq K[u_1] \times \cdots \times K[u_k].$$

Les idempotents de $K[u]$ sont exactement les $\sum_{i=1}^{n} \varepsilon_i p_i$ où p_i est le projecteur sur F_i et $\varepsilon_i \in \{0, 1\}$.

II.2. Critères de diagonalisation

Proposition 17. *Critères de diagonalisation*
Soit u un endomorphisme de polynôme caractéristique scindé, les assertions suivantes sont équivalentes :

1. u est diagonalisable ;
2. pour toute valeur propre λ la multiplicité géométrique *i.e.* $\dim \mathrm{Ker}(u - \lambda \mathrm{Id})$ est égal à la multiplicité algébrique *i.e.* la multiplicité de λ dans χ_u ;
3. $P(u) = 0$ où P est le polynôme de la question précédente ou plus généralement u est annulé par un polynôme scindé à racines simples.

Corollaire 18.
1. Un endomorphisme dont le polynôme caractéristique est scindé à racines simples est diagonalisable.
2. L'endomorphisme induit par un endomorphisme diagonalisable sur un sous-espace est diagonalisable.

II.3. Écriture d+n

Proposition 19. Soit u un endomorphisme avec χ_u scindé. Il existe un unique couple (d, n) avec d diagonalisable et n nilpotent tels que $dn = nd$. De plus d et n sont des polynômes en u.

Application 20. Caractérisation de la diagonalisibilité de exp [**?**].

Remarque 21. Calcul avec Newton.

III. Décomposition en sous-espaces cycliques

III.1. Sous-espaces cycliques

Définition 22. Soit u un endomorphisme sur E. Le sous-espace u-cyclique associé à x est le sous-espace $E_x = K[u] \cdot x$ stable par x. On note $\pi_{u,x}$ le polynôme minimal induit par u sur ce sous-espace qui est l'unique générateur unitaire de l'idéal $\{P \mid P(u) \cdot x = 0\}$.

Proposition 23. Les assertions suivantes sont équivalentes :

- Dans une base matrice compagnon
- $K[u] \cdot x = E$
- polynôme minimal = polynôme caractéristique

Dans ce cas on dit que u est cyclique.

Corollaire 24. Deux endomorphismes cycliques sont semblables si et seulement s'ils ont même polynôme caractéristique.

Proposition 25. Soit u un endomorphisme cyclique. Les sous-espaces stables stables de u sont en bijection avec les diviseurs unitaire de χ_u. En particulier, il y en a un nombre fini. Inversement si le nombre de sous-espaces stables par u est fini et K est infini alors u est cyclique.

III.2. Décomposition de Frobenius

Théorème 26. Soit u un endomorphisme puis $\pi_u = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ sa décomposition en irréductibles. Il existe une décomposition en sous-espaces stables $F_{i,j}$ où l'endomorphisme induit par u sur $F_{i,j}$ est cyclique de polynômes minimal $P_i^{\alpha_{i,j}}$ avec $\alpha_i = \alpha_{i,1} \geqslant \cdots \geqslant \alpha_{i,l_i}$. De plus la donnée des $P_i^{\alpha_{i,j}}$ $(\alpha_{i,j})$ est unique.

Corollaire 27. De façon alternative on peut regrouper les termes pour dire que $E = F_1 \oplus \cdots \oplus F_k$ où le polynôme minimal π_{u,F_1} divise π_{u,F_2} ect... La suite de ses diviseurs étant unique, elle caractérise la classe de similitude de l'endomorphisme, on les appelles les invariants de similitudes.

Application 28.
1. Le commutant d'un endomorphisme est de dimension supérieur à n avec égalité si et seulement si l'endomorphisme est cyclique
2. Le bicommutant est $K[u]$

Raffinement de la décomposition ?

Proposition 29. Les assertions suivantes sont équivalentes :

- il n'existe pas de décomposition en somme directe u-stable de E non trivial
- u est cyclique de polynôme minimal la puissance d'un irréductible

On dit que u est indécomposable.

III.3. Forme normale de Jordan

Lemme 30. Si P est un polynôme irréductible la matrice C_{P^k} est semblable à :

$$\begin{pmatrix} C_P & I_d & & \\ & C_p & \ddots & \\ & & \ddots & I_d \\ & & & C_P \end{pmatrix}$$

On appelle cette matrice bloc de Jordan généralisée qu'on note $J_k(P)$.

Proposition 31. Soit u un endomorphisme sur E. Dans une base u peut s'écrire comme une matrice par blocs avec des blocs :

$$J_{k_1}(P_1), \cdots, J_{k_{i_1}}(P_1), \cdots\cdots, J_{k_r}(P_r), \cdots, J_{k_{i_r}}(P_r).$$

Le nombre de blocs de la forme $J_k(P)$ correspond au nombre de sous-espaces cycliques P^k dans la décomposition de Frobenius de u.

Corollaire : décomposition de Jordan classique [MM22].

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

Dans cette leçon, il faut présenter des propriétés de l'ensemble des sous-espaces stables par un endomorphisme. Des études détaillées sont les bienvenues, par exemple dans le cas d'une matrice diagonalisable ou dans le cas d'une matrice nilpotente d'indice maximum. L'étude des endomorphismes cycliques et des endomorphismes semi-simples trouvent tout à fait leur place dans cette leçon. Dans le cas des corps R ou C, on pourra, si on le souhaite, caractériser ces derniers par la fermeture de leur orbite. Il ne faut pas oublier d'examiner le cas des sous-espaces stables par des familles d'endomorphismes. Ceci peut déboucher par exemple sur des propriétés des endomorphismes commutant entre eux. La réduction des endomorphismes normaux et l'exemple de résolutions d'équations matricielles peuvent être présentés en applications. La décomposition de Frobenius constitue également une application intéressante de cette leçon. Pour aller plus loin, on peut envisager de développer l'utilisation de sous-espaces stables en théorie des représentations.

Plan

I. Sous-espaces stables

I.1. Sous-espaces stables

Référence : Mansuy et Mmeimé [MM22].

Définition 1. Soit u un endomorphisme d'un espace vectoriel E. Un sous-espace vectoriel F de E est dit stable par u lorsque $u(F) \subset F$. Dans ce cas on note :

1. u_F l'endomorphisme induit par u sur F ;
2. $u_{E/F}$ l'endomorphisme induit par u sur E/F.

- Exemple : un endomorphisme dont tous les sous-espaces de dimension k sont stable est une homothétie.

- Représentation matricielle dans une base adaptée
- Corollaire : le polynôme caractéristique de u est le produit des polynômes caractéristiques de u_F et $u_{E/F}$.
- Exemple : si un endomorphisme ne possède pas de sous-espaces stables non triviaux alors χ_u est irréductible. La réciproque est vraie par le lemme des noyaux.

I.2. Supplémentaire stable

- Définition supplémentaire stable
- Exemple : un endomorphisme dont le polynôme caractéristique est scindée et pour lequel tout sous-espace stable admet un supplémentaire stable est diagonalisable.
- Propriété équivalente : représentation matricielle, projecteurs commutant avec u.
- Application : théorème de Maschke

I.3. Dualité

- Rappels de dualité
- Un sous-espace $F \subset E$ est stable par u si et seulement si F° est stable par ${}^t u$.
- Application : les endomorphismes normaux de polynôme caractéristique scindé sont diagonalisables.

II. Décomposition en noyaux de polynômes

II.1. Lemme des noyaux

Proposition 14. *Lemme des noyaux*
Soit u un endomorphisme puis P un polynôme annulateur de u et $P = P_1 \cdots P_k$ avec les P_i deux à deux premiers entre eux. Alors,

$$E = \bigoplus_{i=1}^{k} \operatorname{Ker} P_i(u).$$

Corollaire 15. *Décomposition de Fiting*
Soit u un endomorphisme. Il existe une unique décomposition $E = F \oplus G$ stable par u tel que $u_{|F}$ soit inversible et $u_{|G}$ nilpotent.

Application 16. *Dénombrement des nilpotents*
Sur un espace vectoriel de dimension d sur un corps fini de cardinal q le nombre d'endomorphisme nilpotent est $q^{d(d-1)}$.

Rappels sur les polynômes annulateurs. Idéal, engendré par le polynôme minimal, un polynôme annulateur est le polynôme caractéristique.

II.2. Décomposition caractéristique

Proposition 17. *Décomposition caractéristique*
Si $\pi_u = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ est la décomposition en facteurs irréductibles de π_u alors,

$$E = \bigoplus_{i=1}^{k} \operatorname{Ker} P_i^{\alpha_i}(u).$$

Les sous-espaces $\operatorname{Ker} P_i^{\alpha_i}(u)$ sont appelés sous-espaces caractéristiques de u.

Application 18. On retrouve les résultats précédents. En déduire aussi des informations sur $\exp(tu)$.

Application 19. En notant u_i l'endomorphisme induit sur $\operatorname{Ker} P_i^{\alpha_i}(u)$ on a un isomorphisme de K-algèbre :

$$K[u] \simeq K[u_1] \times \cdots \times K[u_k].$$

Les idempotents de $K[u]$ sont exactement les $\sum_{i=1}^{n} \varepsilon_i p_i$ où p_i est le projecteur sur F_i et $\varepsilon_i \in \{0,1\}$.

Corollaire 20. Si F est un sous-espace stable de u alors $F = \bigoplus_{i=1}^{k} (F \cap K_i)$ où les K_i sont les sous-espaces caractéristiques de u.

Application 21. Si u est diagonalisable alors u admet exactement 2^n sous-espaces stables si u est à spectre simple et une infinité sinon.

II.3. Application à la diagonalisation

Proposition 22. *Critères de diagonalisation*
Soit u un endomorphisme de polynôme caractéristique scindé, les assertions suivantes sont équivalentes :

1. u est diagonalisable ;
2. pour toute valeur propre λ la multiplicité géométrique *i.e.* $\dim \mathrm{Ker}(u-\lambda \mathrm{Id})$ est égal à la multiplicité algébrique *i.e.* la multiplicité de λ dans χ_u ;
3. $P(u)=0$ où P est le polynôme de la question précédente ou plus généralement u est annulé par un polynôme scindé à racines simples.

Corollaire 23.
1. Un endomorphisme dont le polynôme caractéristique est scindé à racines simples est diagonalisable.
2. L'endomorphisme induit par un endomorphisme diagonalisable sur un sous-espace est diagonalisable.

Proposition 24. *Décomposition de Dunford*
Soit u un endomorphisme avec $\chi_u = \prod_{i=1}^{k}(X-\lambda_i)^{\alpha_i}$. Il existe un unique couple (d,n) avec d diagonalisable et n nilpotent tels que $dn=nd$. De plus d et n sont des polynômes en u et on a $P(u)=d$ pour tout polynôme P solution du système de congruences $P \equiv \lambda_i \mod (X-\lambda_i)^{\alpha_i}$.

Exemple 25. (p. 152 MM) Pour $a \neq b$ la décomposition de Dunford de $A = \begin{pmatrix} a & c & d \\ 0 & a & e \\ 0 & 0 & b \end{pmatrix}$ est $D = \begin{pmatrix} a & 0 & \frac{ce}{b-a}+d \\ 0 & a & 0 \\ 0 & 0 & b \end{pmatrix}$
et $N = A - D$.

Application 26. Soit u un endomorphisme sur un **K**-espace vectoriel. Alors $\exp(u)$ est diagonalisable si et seulement u est diagonalisable.

III. Décomposition en sous-espaces cycliques

III.1. Sous-espaces cycliques

Définition 27. Soit u un endomorphisme sur E. Le sous-espace u-cyclique associé à x est le sous-espace $E_x = K[u]\cdot x$ stable par x. On note $\pi_{u,x}$ le polynôme minimal induit par u sur ce sous-espace qui est l'unique générateur unitaire de l'idéal $\{P \mid P(u)\cdot x = 0\}$.

Proposition 28. Les assertions suivantes sont équivalentes :

- Dans une base matrice compagnon
- $K[u]\cdot x = E$
- polynôme minimal = polynôme caractéristique

Dans ce cas on dit que u est cyclique.

Corollaire 29. Deux endomorphismes cycliques sont semblables si et seulement s'ils ont même polynôme caractéristique.

Proposition 30. Soit u un endomorphisme cyclique. Les sous-espaces stables stables de u sont en bijection avec les diviseurs unitaire de χ_u. En particulier, il y en a un nombre fini. Inversement si le nombre de sous-espaces stables par u est fini et K est infini alors u est cyclique.

III.2. Décomposition de Frobenius

Théorème 31. Soit u un endomorphisme puis $\pi_u = P_1^{\alpha_1}\cdots P_k^{\alpha_k}$ sa décomposition en irréductibles. Il existe une décomposition en sous-espaces stables $F_{i,j}$ où l'endomorphisme induit par u sur $F_{i,j}$ est cyclique de polynômes minimal $P_i^{\alpha_{i,j}}$ avec $\alpha_i = \alpha_{i,1} \geqslant \cdots \geqslant \alpha_{i,l_i}$. De plus la donnée des $P_i^{\alpha_{i,j}}$ $(\alpha_{i,j})$ est unique.

Corollaire 32. De façon alternative on peut regrouper les termes pour dire que $E = F_1 \oplus \cdots \oplus F_k$ où le polynôme minimal π_{u,F_1} divise π_{u,F_2} ect... La suite de ses diviseurs étant unique, elle caractérise la classe de similitude de l'endomorphisme, on les appelles les invariants de similitudes.

Application 33.
1. Le commutant d'un endomorphisme est de dimension supérieur à n avec égalité si et seulement si l'endomorphisme est cyclique
2. Le bicommutant est $K[u]$

Raffinement de la décomposition ?

Proposition 34. Les assertions suivantes sont équivalentes :

- il n'existe pas de décomposition en somme directe u-stable de E non trivial
- u est cyclique de polynôme minimal la puissance d'un irréductible

On dit que u est indécomposable.

III.3. Forme normale de Jordan

Lemme 35. Si P est un polynôme irréductible la matrice C_{P^k} est semblable à :

$$\begin{pmatrix} C_P & I_d & & \\ & C_p & \ddots & \\ & & \ddots & I_d \\ & & & C_P \end{pmatrix}$$

On appelle cette matrice bloc de Jordan généralisée qu'on note $J_k(P)$.

Proposition 36. Soit u un endomorphisme sur E. Dans une base u peut s'écrire comme une matrice par blocs avec des blocs :

$$J_{k_1}(P_1), \cdots, J_{k_{i_1}}(P_1), \cdots\cdots, J_{k_r}(P_r), \cdots, J_{k_{i_r}}(P_r).$$

Le nombre de blocs de la forme $J_k(P)$ correspond au nombre de sous-espaces cycliques P^k dans la décomposition de Frobenius de u.

Corollaire : décomposition de Jordan classique [MM22].

152 : Endomorphismes diagonalisables en dimension finie.

Dans cette leçon, on attend des exemples naturels d'endomorphismes diagonalisables et des critères de diagonalisabilité. On doit notamment savoir expliquer pourquoi l'application induite par un endomorphisme diagonalisable sur un sous-espace stable est encore diagonalisable. Il ne faut pas oublier de parler du cas des endomorphismes symétriques, ni les familles commutantes d'endomorphismes diagonalisables. On peut étudier certaines propriétés topologiques en prenant le soin de donner des précisions sur le corps K et la topologie choisie pour $\mathcal{M}_{n,p}(K)$. Les candidates et candidats peuvent s'intéresser aux propriétés de l'exponentielle d'un endomorphisme diagonalisable. On peut dénombrer les endomorphismes diagonalisables dans les corps finis, ou possédant des propriétés données, liées à la diagonalisation. Pour aller plus loin, les candidates et candidats peuvent s'intéresser aux liens qui peuvent aussi être fait avec la théorie des représentations et la transformée de Fourier rapide.

Plan

I. Éléments pour la diagonalisation

I.1. Éléments propres

Référence : Mansuy-Mmeimé

- Notions liés aux éléments propres : valeur propre, vecteur propre, spectre, sous-espaces propres
- Proposition polynôme caractéristique, conséquence : au plus n valeurs propres
- Exemple : matrice compagnon, correspondance valeurs propres racines d'un polynôme.

I.2. Polynômes annulateurs

- Pro/déf polynômes annulateurs (avec existence), polynôme minimal
- Racines des polynômes annulateur
- Exemple : sous-groupes finis de $\mathrm{GL}_n(\mathbf{C})$
- Théorème de Cayley-Hamilton

I.3. Extension du corps des scalaires

Cadre matriciel.

- Invariance du polynôme caractéristique

- invariance dimension puis invariance du polynôme minimal
- Lemme de retour pour la réduction

II. Critères de diagonalisation

Définition 1. Soit u un endomorphisme. Les assertions suivantes sont équivalentes :

1. la matrice de u dans une base est diagonale
2. il existe une base de E formé de vecteurs propres de u
3. les sous-espaces propres de u forme une décomposition en somme directe de u.

II.1. Multiplicités

- Critère des multiplicités
- Corollaire : endomorphismes à spectre simple
- Corollaire : densité des matrices diagonalisables sur $\mathbf{C}$
- Application : théorème de Cayley-Hamilton
- Remarque : adhérence des matrices diagonalisables sur $\mathbf{R}$, invariance du critère par extension de corps

II.2. Polynômes annulateurs

- Lemme des noyaux
- Critère de diagonalisibilité
- Conséquence : endomorphisme induit par un endomorphisme diagonalisable
- Conséquence : sous-groupe fini de $\mathrm{GL}_n(\mathbf{C})$, exemple matrices de permutations
- app : tout sous-groupe fini de $\mathrm{GL}_n(\mathbf{Z})$ s'injecte dans $\mathrm{GL}_n(\mathbf{Z}/3\mathbf{Z})$, son cardinal est majorée par 3^{n^2}.
- rem : le critère pour l'extension devient sans facteur carrés sur un corps parfait blablabla et contre-exemple $P = X^p - t$ sur $\mathbf{F}_p(t)[X]$.

II.3. Supplémentaire

Théorème 2. Un endomorphisme est diagonalisable si et seulement si son polynôme caractéristique est scindée et tout sous-espace stable admet un supplémentaire stable

Corollaire 3. Les endomorphismes normaux dont le polynôme caractéristique est scindée sont diagonalisables, en base orthonormée.

Application 4. Soit $A \in \mathscr{M}_{n,p}(\mathbf{R})$ de rang r. Il existe $(U,V) \in \mathrm{O}_n(\mathbf{R}) \times \mathrm{O}_p(\mathbf{R})$ tels que $A = U\Sigma V^{\mathsf{T}}$ avec :

$$\Sigma = \begin{pmatrix} \Sigma_1 & \mathbf{0}_{r,p-r} \\ \mathbf{0}_{n-r,r} & \mathbf{0}_{n-r,p-r} \end{pmatrix} \quad \text{avec} \quad \Sigma_1 = \mathrm{diag}(\sigma_1, \cdots, \sigma_r).$$

Les réels σ_i sont des réels strictement positifs appelés valeurs singulières de A et correspondant aux racines des valeurs propres de $A^\top A$. Notons Σ_k la matrice obtenue en ne conservant dans Σ que les k plus grandes valeurs singulières, puis posons $A_k = U\Sigma V^\top$. Alors,

$$\|A - A_k\|_2 = \min_{\mathrm{rg}(B) \leqslant k} \|A - B\|_2.$$

Remarque 5. Extension de corps du critère : on a l'équivalence entre semi-simple et polynôme minimal sans facteurs carrés, on est ramené au cas précédent.

III. Pallier à la non diagonalisibilité

III.1. Trigonalisation

- Définition trigonalisation
- Caractérisation
- Application : Cayley-Hamilton
- préciser que l'on peut mettre des quantités arbitrairement petites au dessus de la diagonale
- Corollaire : théorème de Householder
- application : Gelfand et convergence suite de matrices
- application : contrôle exponentielle

III.2. Décomposition caractéristique

- Théorème
- Informations sur les degrés de nilpotences
- Application : contrôle plus précis suites de matrices et exponentielle
- Conséquence : un sous-groupe borné de $\mathrm{GL}_n(\mathbf{C})$ est formé de matrices diagonalisables.

III.3. Décomposition de Dunford

- Théorème avec indication sur comment calculer les polynômes
- Application : caractérisation diagonalisibilité exponentielle
- Application : sous-groupe borné de $\mathrm{GL}_n(\mathbf{C})$
- Remarque : méthode de Newton, extension de corps

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

Cette leçon doit aborder le bagage théorique propre aux vecteurs propres et aux valeurs propres et mettre en lumière l'exploitation de techniques d'algèbre ou d'analyse pour aborder leur recherche. Après avoir exploré la détermination théorique exacte des éléments propres, on s'intéresse à des exemples de matrices dont les éléments propres sont remarquables (matrices compagnons, matrices circulantes, matrices d'ordre fini, matrices stochastiques...) et donne des exemples de situations où la connaissance d'éléments propres s'avère utile. On doit connaître les limites du calcul exact, même si le cadre mathématique nécessaire est non exigible et hors programme, et introduire sur $\mathbf{R}$ ou $\mathbf{C}$ une ou plusieurs méthodes itératives, dont on démontre la convergence. On peut citer les méthodes de la puissance, puissance inverse et QR pour la recherche d'éléments propres. Les notions de norme matricielle, de rayon spectral doivent être maîtrisées. Le lien avec la convergence des suites du type $X_{n+1} = AX_n$ doit être connu et illustré. On peut aussi s'intéresser à la localisation des valeurs propres. Pour aller plus loin, on peut aborder la problématique du conditionnement en distinguant le problème général et le cas particulier des matrices auto-adjointes, s'intéresser aux liens qui peuvent aussi être faits avec la théorie des représentations et la transformée de Fourier rapide, ainsi qu'au comportement de la suite des itérées de matrices stochastiques ou plus généralement de matrices à coefficients positifs, au moins dans des cas particuliers.

I. Valeurs propres, localisation

I.1. Éléments propres

Référence : Mansuy-Mmeimé

- Notions liés aux éléments propres : valeur propre, vecteur propre, spectre, sous-espaces propres
- Proposition polynôme caractéristique, conséquence : au plus n valeurs propres
- Exemple : matrice compagnon, correspondance valeurs propres racines d'un polynôme.
- Lien avec les polynômes annulateurs, exemple : valeurs propres des endomorphismes d'un groupe fini de $\mathrm{GL}_n(\mathbf{C})$.

I.2. Rayon spectral

- Définition du rayon spectral
- La majoration rayon-spectral norme
- Théorème de Householder
- Conséquence : formule de Gelfand
- application : critère de convergence vers 0 des puissances d'une matrice
- application : contrôle de l'exponentielle
- Remarque : on peut obtenir des résultats plus précis avec la décomposition caractéristique.

I.3. Localisation des valeurs propres

- Premier théorème de Gershgorin
- Exemple des matrices stochastiques
- Application : critère d'arrêt
- Deuxième théorème de Gershgorin

II. Spectre des endomorphismes auto-adjoints

II.1. Théorème spectral

- Rappels matrices auto-adjointes
- Lemme de stabilité
- Les endomorphismes auto-adjoints sont les seules endomorphismes diagonalisables en base orthonormée à valeurs propres réelles.

II.2. Formulation variationnelle des valeurs propres

Référence : Oraux-XENS algèbre 3.

- Théorème du min-max de Courant-Fisher avec cas particulier norme 2.
- Conséquence : théorème d'entrelacement de Cauchy
- Application : Critère de Cholesky
- Conséquence : inégalités de Weyl
- Application : voir item ?

II.3. Décomposition en valeurs singulières

- Définition des valeurs singulières
- Théorème de décomposition en valeurs singulières
- Conséquence : problème d'approximation par des matrices de rang fixé.

III. Calcul numérique des valeurs propres

III.1. Méthodes de calcul des valeurs propres

Référence : Ciarlet et Amodei-Deudieu

Proposition 24. *Méthode de la puissance*
Soit $A \in \mathscr{M}_d(\mathbf{C})$ avec une valeur propre dominante $|\lambda_1| > |\lambda_2| \geqslant \cdots \geqslant |\lambda_s|$. Pour x_0 tel que $\pi_{E_{\lambda_1}}(x_0) \neq 0$ il existe $v \in E_{\lambda_1}$ tel que la suite $x_{k+1} = \frac{Ax_k}{\|Ax_k\|}$ vérifie :

$$\left(\frac{|\lambda_1|}{\lambda_1}\right)^k x_k \to v$$

où v est un vecteur propre associé à la valeur propre λ_1. On peut de plus préciser la vitesse de convergence :

1. Si la valeur propre est simple avec λ_2 de multiplicité m alors $O\left(k^{m-1}\frac{|\lambda_2|^k}{|\lambda_1|^k}\right)$,
2. Si la valeur propre est dégénérée alors $O\left(\frac{1}{k}\right)$.

- Méthode QR voir Ciarlet.

III.2. Sensibilité des valeurs propres

Référence : Ciarlet et Amodei-Deudieu

1. Définition : distance de Hausdorff
2. Théorème de Helsner
3. Théorème de Bauer-Fike
4. Cas particulier des matrices auto-adjointes

III.3. Sur la continuité des valeurs propres

- Continuité topologique des valeurs propres
- Attention au problème de paramétrisation des valeurs propres avec $A(z) = \begin{pmatrix} 0 & 1 \\ z & 0 \end{pmatrix}$ sur D_1.
- Cas des matrices à spectre simple, régularité supplémentaire :

Proposition 30. Soit A une matrice à spectre simple. Il existe un voisinage $\mathscr{V}$ de A et un C^∞-difféomorphisme $\phi : \mathscr{V} \to \mathscr{W} \subset \mathbf{C}^d$ tel que pour tout $B \in \mathscr{V}$, le spectre B avec multiplicité soit $\phi_i(B)$ avec $1 \leqslant i \leqslant d$.

155 : Exponentielle de matrices. Applications.

Bien que ce ne soit pas une leçon d'analyse, il faut savoir justifier précisément la convergence de la série exponentielle. Les questions de surjectivité ou d'injectivité doivent être abordées en distinguant les cas réel et complexe. Il est souhaitable de connaître l'image par exponentielle de certains sous-ensembles de matrices (ensemble des matrices symétriques, hermitiennes, ou antisymétriques). La décomposition de Dunford multiplicative (décomposition de Jordan) de $\exp(A)$ trouve toute son utilité dans cette leçon. L'exponentielle en lien avec la décomposition polaire peut s'avérer utile dans l'étude de sous-groupes du groupe linéaire. L'étude du logarithme (quand il est défini) peut être menée dans cette leçon. Les applications aux équations différentielles méritent d'être présentées sans toutefois constituer l'essentiel de la leçon. On pourra par exemple faire le lien entre réduction et comportement asymptotique, mais le jury déconseille aux candidates et candidats de proposer ce thème dans un développement de cette leçon, sauf à avoir bien compris comment les apports algébriques permettent ici de simplifier les conclusions analytiques. Pour aller plus loin, les candidates et candidats peuvent s'aventurer vers les sous-groupes à un paramètre du groupe linéaire (on peut alors voir si ces sous-groupes constituent des sous-variétés fermées de $\mathrm{GL}_{n,p}(\mathbf{R}^q)$) ou vers les algèbres de Lie.

Plan

I. Définition de l'exponentielle de matrice

I.1. Développement en série entière

- Définition de l'exponentielle de matrice par la série entière en proposition.
- Exemple en dimension 2, lien avec les nombres complexes et même transformations hyperboliques
- Exemple des matrices diagonales
- Exemple des matrices nilpotentes
- Propriétés élémentaires : transposée, spectre, $\exp(P^{-1}AP) = P^{-1}\exp(A)P$ et $\exp(A+B) = \exp(A)\exp(B)$ lorsque A et B commutent. Contre exemple dans le cas général ?

I.2. Caractérisation différentielle

- Lemme différentielle en 0 de l'exponentielle de matrice.
- Caractérisation fondamentale : $t \mapsto \mathrm{e}^{tA}$ est l'unique solution du système différentielle matricielle $M'(t) = AM(t)$.

- Exemple du Gourdon
- Application formule de Glauber : si A et B commutent avec $[A,B]$ alors $\mathrm{e}^{A+B} = \mathrm{e}^{A}\mathrm{e}^{B}\mathrm{e}^{-\frac{1}{2}[A,B]}$.

I.3. Calcul de l'exponentielle de matrice

- Rappel décomposition caractéristique
- Calcul de l'exponentielle de matrice par la décomposition caractéristique selon le Gourdon. Exemple.
- Application : contrôle de e^{tA}, stabilité des systèmes linéaires et non linéaires.
- Pour la partie nilpotente il peut être avantageux de la mettre sous forme de Jordan.

Remarque 1. Autres points de vues :

1. polynôme interpolateur
2. formule de Cauchy $\exp(A) = \int_\Gamma \exp(z)(zI - A)^{-1}\mathrm{d}z$

II. Image de l'exponentielle de matrice

II.1. Surjectivité de l'exponentielle

- Surjectivité de l'exponentielle de matrice
- Application : théorème de Floquet
- Logarithme matricielle
- Cas des matrices réelles
- Remarque : on peut utiliser la décomposition de Dunford et le logarithme matricielle pour une preuve alternative

II.2. Autres transformations remarquables

Des anti-symétriques aux matrices de rotations.

- Matrices anti-symétriques et matrices de rotations
- Cas particulier de la dimension 2 lien avec représentation du cercle par l'exponentielle
- Dimension 3 avec formule de Rodrigue (Gourdon), voir Griffone

Des matrices symétriques aux matrices symétriques plus plus.

- Homéomorphisme $S_n \to S_n^{++}$
- application : racine carrée d'une matrice symétrique
- Remarque : on peut en déduire la décomposition polaire

II.3. Diagonalisation de l'exponentielle

- Rappel décomposition de Dunford
- Décomposition de Dunford l'exponentielle
- Proposition : caractérisation diagonalisibilité exponentielle

III. Groupes de Lie matricielles

III.1. Présentation

- Une définition
- Quelques exemples : $\mathrm{SL}_n(\mathbf{R})$, $\mathrm{SO}_n(\mathbf{R})$, $\mathrm{O}_n(\mathbf{R})$.

III.2. Espace tangent

- Identité d'Euler : $(I + A/n)^n \to \mathrm{e}^{A}$
- Lien avec l'exponentielle pour un sous-groupe fermé

III.3. Théorème de Cartan Von-Neumann

- Lemme de Trotter-Kato
- Théorème de Cartan Von-Neumann

156 : Endomorphismes trigonalisables. Endomorphismes nilpotents.

Il est indispensable de connaître les polynômes caractéristiques et minimaux d'un endomorphisme nilpotent et de savoir justifier son caractère trigonalisable. Il est bon de savoir expliquer pourquoi l'application induite par un endomorphisme trigonalisable (respectivement nilpotent) sur un sous-espace stable est encore trigonalisable (respectivement nilpotent). L'utilisation des noyaux itérés est fondamentale dans cette leçon, par exemple pour déterminer si deux matrices nilpotentes sont semblables. Il est intéressant de présenter des conditions suffisantes de trigonalisation simultanée ; l'étude des endomorphismes cycliques a toute sa place dans cette leçon. L'étude des nilpotents en dimension 2 débouche naturellement sur des problèmes de quadriques et l'étude sur un corps fini donne lieu à de jolis problèmes de dénombrement. Pour aller plus loin, les candidates et candidats peuvent aussi présenter la décomposition de Jordan ou la décomposition de Frobenius, ou des caractérisations topologiques des endomorphismes nilpotents, ou encore des propriétés topologiques de l'ensemble des endomorphismes nilpotents.

I. Trigonalisation

I.1. Matrices triangulaires

- Définition des matrices triangulaires
- Propriété = diagonale valeurs propres
- Corollaire : inversibilité avec inverse diagonale

I.2. Endomorphismes trigonalisables

Définition 1. Les assertions suivantes sont équivalentes :

1. la matrice de u dans la base $B = (e_1, \cdots, e_n)$ est triangulaire supérieur
2. u stabilise le drapeau complet (F_k) où $F_k = \text{vect}(e_1, \cdots, e_k)$

Dans ce cas on dit que u est trigonalisable dans la base B.

Proposition 2. Un endomorphisme u est trigonalisable si et seulement si son polynôme caractéristique est scindée. Tout endomorphisme est trigonalisable dans une clotûre algébrique.

- Application : théorème de Cayley-Hamilton
- Application : le commutant d'une matrice de taille n est de dimension supérieur à n. (on a égalité pour les matrices cycliques)
- Critère de trigonalisation simultanée, nécessaire pas suffisant
- Rem : si la famille d'endomorphismes est un sous-groupes de $\text{GL}_n(K)$ on peut déduire que la famille est trigonalisable à partir de sa structure. Ainsi, (Lie-Kolchin) tout sous-groupe connexe résoluble de $\text{GL}_n(\mathbf{C})$ est trigonalisable tandis que tout p-Sylow de $\text{GL}_n(\mathbf{F}_q)$ est trigonalisable.

I.3. Analyse des coefficients sur-diagonaux

- Soit A une matrice complexe. Pour tout $\varepsilon > 0$, il existe un changement de base tel que les coefficients strictement au dessus de la diagonale soit $\leqslant \varepsilon$.
- app : la classe de similitude est fermé si et ssi diagonalisable
- cor : Householder
- app : Gelfand et contrôles matrices

II. Mieux que la trigonalisation : décomposition caractéristique

II.1. Décomposition caractéristique

- Décomposition caractéristique
- Application au contrôle plus fin des puissances et de l'exponentielle

II.2. Décomposition de Dunford

- Énoncé avec méthode de calcul des polynômes intermédiaires
- Exemple de [MM22]
- Application en mode écart à la diagonalisation avec l'exponentielle
- Remarque : méthode de Newton pour Dunford.

II.3. Extension du corps des scalaires

- Corps parfait avec caractérisation
- Décomposition $s+n$
- contre-exemple de Romagny

III. Étude des endomorphismes nilpotents

III.1. Endomorphismes nilpotents

- Ensemble des matrices nilpotentes, structure de cône
- la somme de deux endomorphismes nilpotents qui commutent reste nilpotent, sinon ce n'est pas le cas
- Cardinal du cône nilpotent avec lemme de Fiting
- Conséquence : cardinal de l'ensemble des matrices trigonalisables

III.2. Réduction de Jordan des nilpotents

Référence : [MM22]

- Réduction de Jordan dans le cadre nilpotent
- Représentation des classes de similitudes par les diagrammes de Young
- Application : Caractérisation en petite dimension.

III.3. Forme normale de Jordan

- Forme normale de Jordan
- Application au calcul, on a des formes sympa
- Corollaire : critère semblable
- Application : toute matrice est semblable à sa transposée

157 : Matrices symétriques réelles, matrices hermitiennes.

Le théorème spectral est indispensable dans cette leçon. Une place importante mérite d'être faite au cas particulier des matrices symétriques positives et définies positives ; les candidates et candidats doivent connaître leurs propriétés fondamentales, leur rôle, et la structure de leur ensemble. La notion de signature pourra être présentée en montrant comment elle détermine la classe de congruence d'une matrice symétrique réelle. L'action du groupe linéaire et du groupe orthogonal sur l'espace des matrices symétriques peut donner un cadre naturel à cette leçon. Le lien avec les formes quadratiques et les formes hermitiennes est incontournable. L'orthogonalisation simultanée est un résultat important de cette leçon. Il faut en connaître les applications géométriques aux quadriques. Les candidates et candidats maîtrisant ces notions pourront illustrer la leçon en évoquant le cas des matrices de covariance de vecteurs aléatoires et discuter les conditions en assurant le caractère inversible, la décomposition de Cholesky, qui a de nombreuses applications pour le calcul scientifique (en lien avec la résolution de systèmes linéaires ou de problèmes de moindres carrés) ou en probabilités (construction d'un vecteur gaussien de matrice de covariance donnée à partir d'un vecteur gaussien de matrice de covariance identité), ou la décomposition en valeurs singulières d'une matrice (particulièrement importante pour le traitement massif de données).

I. Matrices symétriques, hermitiennes et représentation

I.1. Matrices auto-adjointes

- Définition des matrices symétriques hermitiennes qu'on regroupe sous le terme auto-adjointe. Définition matrices auto-adjointes positives et définies positives.
- Propriétés d'ensembles : S_n est un s.e.v, S_n^+ (resp. S_n^{++}) est un cône positif fermé (resp. ouvert) dans S_n. Presque pareil pour les matrices hermitiennes bien $\mathbf{R}$-sev mais pas $\mathbf{C}$-sev.

I.2. Endomorphismes auto-adjoints

- adjoint d'un endomorphisme sur un espace euclidien ou hermitien
- Définition des opérateurs auto-adjoints
- Caractérisation des opérateurs auto-adjoints

I.3. Formes quadratiques

- Définition des formes quadratique, définie, positive
- Forme polaire associée
- Représentation matricielle des formes quadratiques
- Rem : Lien avec la partie précédente

II. Réduction des endomorphismes auto-adjoints

II.1. Diagonalisation en base orthonormée

Lemme 10. (Gourdon) Soit u un endomorphisme normal. Si F est u-stable, $F^\perp$ également.

Proposition 11. Soit E un espace euclidien ou hermitien. Un endomorphisme u de E est diagonalisable en base orthonormée si et seulement si son polynôme caractéristique est scindée et u commute avec son adjoint. En particulier les endomorphismes auto-adjoints sont diagonalisables en base orthonormée à spectre réelle. Ce sont exactement ces endomorphismes.

Corollaire 12. Soit A une matrice auto-adjointe. Il existe une matrice $P \in \mathrm{O}_n(\mathbf{R})$ ou $\mathrm{U}_n(\mathbf{R})$ tel que $P^{-1}AP$ soit diagonale.

II.2. Formulation variationnelle des valeurs propres

Si u est un endomorphisme auto-adjoint on note $\lambda_1(u) \leqslant \cdots \leqslant \lambda_n(u)$ ses valeurs propres rangés par ordre croissant.

Proposition 13. *Principe du min-max de Courant-Fisher* (Oraux X-ENS)
Soit u un endomorphisme auto-adjoint. On a :

$$\lambda_k(u) = \min_{F \in \mathscr{F}_k} \max_{\substack{x \in F \\ \|x\|=1}} \langle u(x) \,|\, x \rangle = \max_{F \in \mathscr{F}_{n-k+1}} \min_{\substack{x \in F \\ \|x\|=1}} \langle u(x) \,|\, x \rangle$$

où $\mathscr{F}_k$ désigne l'ensemble des sous-espaces de dimension k de E. En particulier,

$$\lambda_1 = \min_{\|x\|=1} \langle u(x) \,|\, x \rangle \quad \text{et} \quad \lambda_n = \min_{\|x\|=1} \langle u(x) \,|\, x \rangle.$$

Il en découle que $\rho(u) = \max_{\|x\|=1} |\langle u(x) \,|\, x \rangle|$.

Application 14. *Théorème de perturbation de Weyl* (Oraux X-ENS p144)
Si u et v sont deux endomorphismes auto-adjoints alors :

$$\lambda_{i+j-1}(u+v) \leqslant \lambda_i(u) + \lambda_j(u).$$

En particulier $|\lambda(u) - \lambda(v)| \leqslant \|u - v\|$. Ce résultat montre que les valeurs propres d'une matrice symétrique sont relativement stables par perturbation symétrique.

Corollaire 15. *Théorème d'entrelacement de Cauchy* (Oraux X-ENS p144)
Soit u un endomorphisme auto-adjoint sur un espace E, puis D une droite de E et v l'endomorphisme induit sur le quotient E/D. On a :

$$\lambda_1(u) \leqslant \lambda_1(v) \leqslant \lambda_2(u) \leqslant \cdots \leqslant \lambda_{n-1}(u) \leqslant \lambda_{n-1}(v) \leqslant \lambda_n(u).$$

Application 16. Critère de Sylvester (Oraux X-ENS p144) et (Gourdon p. 260)
Une matrice symétrique est définie positive si et seulement si tous ses mineurs principaux sont > 0. Par exemple la matrice $\left((1+|i-j|)^{-1}\right)_{1 \leqslant i,j \leqslant n}$ est définie positive.

II.3. Décomposition en valeurs singulières

- Théorème de décomposition en valeurs singulières
- Application : problème d'approximation par des matrices de rang fixé
- Théorème : Décomposition polaire
- Conséquence sur la topologie du groupe linéaire : $\mathrm{GL}_n(\mathbf{R})$ est homéomorphe à $\mathrm{O}_n(\mathbf{R}) \times \mathbf{R}^{n(n+1)/2}$ et $\mathrm{O}_n(\mathbf{R})$ est un sous-groupe compact maximal de $\mathrm{GL}_n(\mathbf{R})$ idem cas complexe.

III. Orthogonalisation des formes quadratiques

III.1. Théorème d'inertie de Sylvester

Théorème 21. Soit q une forme quadratique. Il existe une base q-orthogonale de E i.e. dans laquelle la forme quadratique s'exprime sous la forme :

$$q(x_1, \cdots, x_n) = \sum_{i=1}^{n} a_i x_i^2.$$

De plus le nombre s de $a_i > 0$ et t de $a_i < 0$ ne dépend pas de la décomposition choisie. On appelle le couple (s,t) la signature de q.

Remarque 22.
1. q est positive ssi sa signature est de la forme $(s,0)$ et définie positive si et seulement si sa signature est $(\dim E, 0)$.
2. On peut modifier la base de sorte que les coefficients a_i valent $-1, 0$ ou 1.

Application 23. *Classification affine des coniques*
Soit $\mathscr{P}$ un plan affine puis $\mathscr{C}$ une conique propre définie par l'équation f. On note q la partie quadratique de f et Q l'homogénéisé de f. Il existe un repère affine dans lequel f à pour équation :

1. $x^2 + y^2 = 1$ si $\mathrm{sgn}(q) = (2,0)$ et $\mathrm{sgn}(Q) = (3,0)$
2. $x^2 - y^2 = 1$ si $\mathrm{sgn}(q) = (1,1)$ et $\mathrm{sgn}(Q) = (2,1)$ ou $(1,2)$
3. $y^2 = 2px$ si $\mathrm{sgn}(q) = (1,0)$ et $\mathrm{sgn}(Q) =$

Corollaire 24. Soit A une matrice auto-adjointe. Il existe une matrice $P \in \mathrm{GL}_n(\mathbf{K})$ tel que $P^\top AP$ soit diagonale à coefficients dans $\{-1,0,1\}$.

Remarque 25. Il existe un algorithme (algorithme de Gauss) permettant d'effectuer la réduction précédente avec asymptotiquement $\frac{n^3}{3}$ et $\frac{2n^3}{3}$ opérations élémentaires.

III.2. Décomposition de Cholesky

Théorème 26. Si A est une matrice auto-adjointe définie positive il existe une matrice triangulaire inférieur L de diagonale positive tel que $A = L^*L$.

Remarque 27. Il existe un algorithme permettant d'effectuer la réduction précédente avec asymptotiquement $\frac{n^3}{2}$ opérations.

Application 28. Cette méthode permet de simuler efficacement un vecteur gaussien (plus rapidement) qu'avec la méthode de Gauss. Pour simuler un vecteur gaussien de moyenne $\mu \in \mathbf{R}^n$ et de matrice de covariance $\Sigma \in \mathrm{S}_n^{++}(\mathbf{R})$ on calcule $\Sigma = L^\top L$ la décomposition de Cholesky de Σ puis on si X est un vecteur gaussien standard, $L^\top(X - \mu)$ est un vecteur gaussien $\mathscr{N}(\mu, \Sigma)$.

III.3. Théorème spectral

Théorème 29. On reprend les hypothèses du ? et on suppose E munie d'une structure euclidienne ou hermitienne. Alors on peut construire la base q-orthogonal de sorte que les vecteurs soient également orthogonaux au sens de la structure euclidienne ou hermitienne de E.

Remarque 30. On peut de plus choisir entre prescrire les coefficients a_i comme précédemment ou normaliser les vecteurs de la base.

Application 31. *Classification euclidienne des coniques*
Soit $\mathscr{P}$ un plan euclidien puis $\mathscr{C}$ une conique propre définie par l'équation f. Il existe un repère affine dans lequel f à pour équation :

1. $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$
2. $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$
3. $y^2 = 2px$

Corollaire 32. Soit A une matrice auto-adjointe. Il existe une matrice P orthogonal ou unitaire tel que $P^\top AP$ soit diagonale. En particulier la signature de A correspond à son nombre de valeurs strictement positives et son nombre de valeurs propres strictement négatives.

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

Dans cette leçon, le caractère euclidien de l'espace est essentiel pour que l'endomorphisme soit remarquable. Le théorème spectral pour les auto-adjoints et la réduction des endomorphismes orthogonaux sont des résultats incontournables. Le jury met les candidates et candidats en garde sur le fait que le lemme des noyaux ou la décomposition de Dunford ne sont pas des développements adaptés à cette leçon. En revanche, l'utilisation du fait que l'orthogonal d'un sous-espace stable par un endomorphisme est stable par l'adjoint doit être mis en valeur. De même la réduction d'endomorphismes normaux peut être évoquée. L'étude des projections orthogonales (en lien avec le calcul de distances), des rotations, des réflexions, des renversements, etc. fournit des exemples dignes d'intérêt. Une illustration pertinente peut s'appuyer sur la description de problèmes de moindres carrés en faisant ressortir le rôle de l'hypothèse de rang plein de A sur le caractère inversible de $A^\top A$.

Plan

I. Endomorphismes normaux

I.1. Adjoint d'un endomorphisme et endomorphismes normaux

Rappels. Adjoint d'un endomorphisme. Définition des endomorphismes normaux.

I.2. Diagonalisation en base orthonormée

Lemme 1. (Gourdon) Soit u un endomorphisme normal. Si F est u-stable, $F^\perp$ également.

Proposition 2. Soit E un espace euclidien ou hermitien. Un endomorphisme u de E est diagonalisable en base orthonormée si et seulement si son polynôme caractéristique est scindée et u commute avec son adjoint.

Corollaire 3. Si M est une matrice normale alors M est diagonalisable sur $\mathbf{C}$.

I.3. Réduction des endomorphismes normaux sur R

Lemme 4. Unitairement semblable entraine orthogonalement semblable

Théorème 5. Réduction des normaux (Gourdon).

Exemples : matrices antisymétrique, isométries

II. Endomorphismes auto-adjoint

II.1. Endomorphismes auto-adjoint et matrices symétriques

II.2. Réduction des endomorphismes auto-adjoints

II.3. Formulation variationnelle des valeurs propres

Si u est un endomorphisme auto-adjoint on note $\lambda_1(u) \leqslant \cdots \leqslant \lambda_n(u)$ ses valeurs propres rangés par ordre croissant.

Proposition 6. *Principe du min-max de Courant-Fisher* (Oraux X-ENS)
Soit u un endomorphisme auto-adjoint. On a :

$$\lambda_k(u) = \min_{F\in\mathscr{F}_k} \max_{\substack{x\in F\\ \|x\|=1}} \langle u(x)\,|\,x\rangle = \max_{F\in\mathscr{F}_{n-k+1}} \min_{\substack{x\in F\\ \|x\|=1}} \langle u(x)\,|\,x\rangle$$

où $\mathscr{F}_k$ désigne l'ensemble des sous-espaces de dimension k de E. En particulier,

$$\lambda_1 = \min_{\|x\|=1} \langle u(x)\,|\,x\rangle \quad \text{et} \quad \lambda_n = \min_{\|x\|=1} \langle u(x)\,|\,x\rangle.$$

Il en découle que $\rho(u) = \max_{\|x\|=1} |\langle u(x)\,|\,x\rangle$.

Application 7. *Théorème de perturbation de Weyl* (Oraux X-ENS p144)
Si u et v sont deux endomorphismes auto-adjoints alors :

$$\lambda_{i+j-1}(u+v) \leqslant \lambda_i(u) + \lambda_j(u).$$

En particulier $|\lambda(u) - \lambda(v)| \leqslant \|u - v\|$. Ce résultat montre que les valeurs propres d'une matrice symétrique sont relativement stables par perturbation symétrique.

Corollaire 8. *Théorème d'entrelacement de Cauchy* (Oraux X-ENS p144)
Soit u un endomorphisme auto-adjoint sur un espace E, puis D une droite de E et v l'endomorphisme induit sur le quotient E/D. On a :

$$\lambda_1(u) \leqslant \lambda_1(v) \leqslant \lambda_2(u) \leqslant \cdots \leqslant \lambda_{n-1}(u) \leqslant \lambda_{n-1}(v) \leqslant \lambda_n(u).$$

III. Isométries

III.1. Isométries et matrices orthogonales

- Exemple en dimension 2 (Griffone)

III.2. Réduction des isométries

- Théorème de réduction
- Classification des isométries en dimension 3 (Griffone, Audin)

III.3. Groupes des isométries

- Générateurs
- Groupe dérivée, centre
- Simplicité
- Cas remarquables par les quaternions

IV. Décomposition euclidienne d'une transformation linéaire

IV.1. Décomposition en valeurs singulières

- SVD
- Conséquence 1 : approximation par des matrices de rang fixé
- Conséquence 2 : problème des moindres carrés

IV.2. Décomposition polaire

- Décomposition polaire version homéomorphisme
- Conséquence 1 : $\mathrm{O}_n(\mathbf{R})$ groupe compact maximal
- Conséquence 2 : $\mathrm{GL}_n(\mathbf{R})$ homéomorphe à $\mathrm{O}_n(\mathbf{R}) \times \mathbf{R}^{\frac{n(n+1)}{2}}$.

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

Il est important de bien placer la thématique de la dualité dans cette leçon ; celle-ci permet de mettre en évidence des correspondances entre un morphisme et son morphisme transposé, entre un sous-espace et son orthogonal (canonique), entre les noyaux et les images ou entre les sommes et les intersections. Bon nombre de résultats d'algèbre linéaire se voient dédoublés par cette correspondance. Les liens entre base duale et fonctions de coordonnées doivent être parfaitement connus. Le passage d'une base à sa base duale ou antéduale, ainsi que les formules de changement de base, doivent être maîtrisés. On pourra s'intéresser aux cas spécifiques où l'isomorphisme entre l'espace et son dual est canonique (cas euclidien, cas des matrices). Savoir calculer la dimension d'une intersection d'hyperplans via la dualité est important dans cette leçon. L'utilisation des opérations élémentaires sur les lignes et les colonnes permet d'obtenir les équations d'un sous-espace vectoriel ou d'exhiber une base d'une intersection d'hyperplans. Le lien avec la résolution des systèmes linéaires doit être fait. Cette leçon peut être traitée sous différents aspects : géométrique, algébrique, topologique ou analytique. Il faut que les développements proposés soient en lien direct avec la leçon. Enfin rappeler que la différentielle d'une fonction à valeurs réelles est une forme linéaire semble incontournable. Pour des candidates et candidats ayant une pratique de ces notions, il est possible d'illustrer la leçon avec un point de vue probabiliste, en rappelant que la loi d'un vecteur aléatoire X est déterminée par les lois unidimensionnelles $X \cdot u$ pour tout vecteur u.

Plan

I. Dualité

I.1. Formes linéaires

Définition 1 (Grifone ou Gourdon)**.** Une forme linéaire sur E est une application linéaire $f : E \to K$. On note E^* l'ensemble des formes linéaires sur E, c'est un K-espace vectoriel appelé espace dual de E.

Exemples :

- coordonnées pour K^n, sera généraliser par les bases duales dans la section suivante ;
- dérivation dans $K_n[X]$;
- l'intégration sur $\mathbf{K}_n[X]$ pour $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$.

Proposition 2. Les assertions suivantes sont équivalentes :
- H est un sous-espace vectoriel de E de dimension $n-1$;
- H est le noyau d'une forme linéaire sur E.

On dit alors que H est un hyperplan de E.

Exemple 3. En dimension 3 un hyperplan est un plan vectoriel et peut se définir par une équation de la forme $ax+by=0$.

I.2. Bases dual et antédual

Définition 4 (Gourdon)**.** Étant donnée $(e_1,\cdots,e_n)$ une base de E on définit pour tout $i\in\{1,\cdots,n\}$ la forme linéaire e_i^* par $e_i^*(e_j)=\delta_{i,j}$.

Proposition 5 (Gourdon)**.** Avec les notations précédentes $(e_1^*,\cdots,e_n^*)$ est une base de E appelée base duale de $(e_1,\cdots,e_n)$ et on a pour toute forme linéaire f ;

$$f(x)=\sum_{i=1}^{n} e_i^*(x)e_i.$$

Ainsi, E est isomorphisme à son dual E^* donc en particulier $\dim E=\dim E^*$. Toutefois cette isomorphisme n'est pas canonique.

Exemple 6. La base dual de $(X-a)^k$ est $f_k : P\mapsto \frac{P^{(k)}(a)}{k!}$ on a ainsi la formule de Taylor :

$$P=\sum_{k=1}^{n}\frac{P^{(k)}(a)}{k!}(X-a)^k.$$

Proposition 7. L'application $x\mapsto\tilde{x}$ où l'on note $\tilde{x} : f\in E^*\mapsto f(x)\in K$ définit un isomorphisme canonique entre E et le dual de son dual E^{**} dit bidual.

Corollaire 8 (Gourdon)**.** Soit $(f_1,\cdots,f_n)$ une base de E^*. Il existe une unique famille de vecteurs $(e_1,\cdots,e_n)$ tel que $(f_1,\cdots,f_n)$ soit la base duale de $(e_1,\cdots,e_n)$. On dit que $(e_1,\cdots,e_n)$ est la base antéduale de $(f_1,\cdots,f_n)$.

Exemple 9 (Gourdon ±)**.** Soient $(a_0,\cdots,a_n)$ des points distincts de K. Les formes linéaires $f_k : P\in K_n[X]\mapsto P(a_k)$ forme une base de $K_n[X]^*$ dont la base antéduale est donnée par les polynômes interpolateurs de Lagrange

$$L_k=\prod_{l\neq k}\frac{X-a_l}{a_k-a_l}.$$

app : sur $\mathbf{R}$ il existe des scalaires $\lambda_0,\cdots,\lambda_i$ tels que $\int_{-1}^{1}P(t)\mathrm{d}t=\sum_{i=0}^{n}\lambda_i P(a_i)$ pour tout $P\in\mathbf{R}_n[X]$ les λ_i correspond aux $\int_{-1}^{1}P_i(t)\mathrm{d}t$. Ce résultat est à la base des méthodes d'intégrations numériques.

Changement de base, calcul de la base antéduale....

I.3. Dualité dans un espace munie d'une forme bilinéaire

Soit E un K-espace vectoriel de dimension finie munie d'une forme bilinéaire $\varphi : E\times E\to K$.

Proposition 10. L'application Φ qui au vecteur x associe la forme linéaire $y\mapsto\varphi(x,y)$ définie une application linéaire de E dans E^*. Cette application est bijective si et seulement si φ est non dégénérée c'est à dire que pour tout $x\in E$, il existe un vecteur y tel que $\varphi(x,y)\neq 0$. Dans ce cas, pour tout forme linéaire f il existe un unique $x\in E$ tel que $f(y)=\varphi(x,y)$.

Exemple 11 (Gourdon ±)**.** Sur $\mathcal{M}_n(K)$ l'application $(A,B)\mapsto\mathrm{Tr}(AB)$ est une forme bilinéaire non dégénérée donc pour toute forme linéaire f sur $\mathcal{M}_n(K)$ il existe $A\in\mathcal{M}_n(K)$ tel que $f(X)=\mathrm{Tr}(AX)$.
app : tout hyperplan de $\mathcal{M}_n(K)$ contient une matrice inversible.

II. Orthogonalité

II.1. Annulateur d'un sous-espace

Définition 12. Annulateur à gauche et à droites et propriétés.

Proposition 13. Dimension

Corollaire 14. Définition d'un sous-espace par des équations, interprétation géométrique.

Exemple 15. Comment trouver les équations d'un sous-espace

Application 16. Test d'appartenance à un sous-espace etc...

II.2. Cas d'un espace munie d'une forme bilinéaire

Lemme 17. Avec les notations précédentes on a $A^{\perp} = \overline{f}(A)^{\circ}$.

Proposition 18 (Grifone)**.** Soit F un sous-espace de E. Alors,

- $\dim F^{\perp_q} = \dim E - \dim F + \dim(F \cap N(q))$;
- $F^{\perp\perp} = F + N(q)$.

où $N(q)$ est le noyau de q définit comme le noyau de l'application linéaire $\overline{f}$. Lorsque $N(q) = \{0\}$ on dit que q est non dégénérée.

Application 19. Si q est une forme quadratique non dégénérée et F est un sous-espace tel que $q_{|F} = 0$ (on dit que F est totalement isotrope) alors $\dim(F) \leqslant \frac{\dim(E)}{2}$. Cet argument est un point clé de la preuve du résultat suivant : (théorème de Flanders).

Corollaire 20 (Grifone)**.** Un sous-espace F de E est supplémentaire avec son orthogonal si et seulement $F \cap F^{\perp} = \{0\}$, on dit alors que F est anisotrope.

Application 21. Si x est un vecteur non isotrope alors $\langle x \rangle \oplus \langle x \rangle^{\perp} = E$.

II.3. Bases orthogonales

Définition 22. Vecteurs orthogonaux.

Théorème 23. Existence de bases orthogonales

Corollaire 24. Théorème d'inertie de Sylvester.

Proposition 25. Plus sur la matrice de passage

III. Transposition

III.1. Application transposée

- Définition, interprétation matricielle
- Échange noyau/image, applications ?

III.2. Sous-espaces stables

- Lemme de stabilité
- Application : trigonalisation, même trigonalisation en base orthonormée dans le cas d'un espace munie d'un produit scalaire
- Application : diagonalisation des endomorphismes auto-adjoint

III.3. Réduction de Frobenius

- Le lemme fondamental
- Réduction, calcul par la méthode de Smith
- Application : une matrice est toujours semblable à sa transposée
- Autres applications...

161 : Espaces vectoriels et espaces affines euclidiens : distances, isométries.

Les généralités sur les espaces euclidiens et affines sont supposées connues. La leçon reste contenue dans le cadre des espaces de dimension finie. La notion de distance est abordée dans le cadre de la norme euclidienne : les projections orthogonales doivent être mentionnées. Les déterminants de Gram et des inégalités du type des inégalités d'Hadamard ont toute leur place dans cette leçon. La classification des isométries en dimension 2 et 3 est exigible. En dimension 3, il faut savoir classifier les rotations et connaître les liens avec la réduction. On peut aussi penser aux isométries laissant stables certains objets en dimension 2 et 3. Il faut savoir justifier qu'une isométrie est affine, pouvoir donner des générateurs du groupe des isométries affines et savoir composer des isométries affines. Les groupes de similitudes peuvent également être abordés. Pour aller plus loin, les candidates et candidats peuvent évoquer l'interprétation de l'écart-type comme une distance, et présenter la matrice de covariance comme un exemple pertinent de matrice de Gram. Ainsi, les déterminants de Gram permettent de calculer l'erreur commise dans le cadre de prédictions affines.

Plan

I. Distance dans un espace affine euclidien

Préliminaires

Définition 1. Espace affine euclidien

Proposition 2. Formule de Pythagore

I.1. Projection orthogonal

Théorème 3 (Perso)**.** Soient $\mathscr{F}$ un sous-espace affine de $\mathscr{E}$ et A un point de $\mathscr{E}$. La distance de H à $\mathscr{F}$ est atteinte en un unique point H appelée projeté orthogonal de A sur H ; c'est l'unique point de $\mathscr{F}$ tel que $\overrightarrow{AH} \perp F$.

Proposition 4. Si $(O, A_1, \cdots, A_n)$ est un repère affine orthonormée de $\mathscr{E}$ tel que $(O, A_1, \cdots, A_p)$ soit un repère affine orthonormée de $\mathscr{F}$ alors,

$$\overrightarrow{OH} = \sum_{i=1}^{n} \langle \overrightarrow{OA}, \overrightarrow{OA_i} \rangle \overrightarrow{OA_i}, \qquad d(A, \mathscr{F}) = \sum_{i=p+1}^{n} (\overrightarrow{OA} \cdot \overrightarrow{OA_i}) \overrightarrow{OA_i}.$$

Exemple 5. Si f est une application affine non nulle de $\mathscr{E}$ dans $\mathbf{R}$, la distance de A à l'hyperplan $H = f^{-1}(0)$ est $\frac{|f(A)|}{\|\vec{f}\|}$.

Proposition 6. Formule de Gram

Exemple 7. Minimisation de $\int_{\mathbf{R}}(1+a_1x+\cdots+a_nx^n)^2\mathrm{e}^{-x}\mathrm{d}x$ ou autre.

I.2. Lien avec le volume

Proposition 8.

Interprétation géométrique de la formule de Gram.

Proposition 9. Inégalité de Hadamard.

Application 10. Calcul de déterminant sur $\mathbf{Z}$.

II. Réduction des isométries

Préliminaires

Définition 11. Isométrie, isométrie direct et indirect.

Proposition 12. Une isométrie est une application affine.

II.1. Réduction des isométries

Lemme 13. Décomposition canonique des isométries.

Théorème 14. Classification des isométries vectoriels

Application 15. Classification des isométries en dimension 2

Application 16. Classification des isométries en dimension 3

II.2. Représentation des rotations par les quaternions

III. Étude du groupe des isométries

Préliminaire

Définition 17.

Proposition 18. Premier dévissage avec le déterminant. Produit semi-direct

Exemple 19. Pour $n = 2$...

III.1. Structure du groupe des isométries

Proposition 20. Centre.

Définition 21. Groupe projectif orthogonal

Lemme 22. Générateurs et conjugaison

Théorème 23. Simplicité

III.2. Sous-groupes finis de $\mathrm{SO}(3,\mathbf{R})$

Pas au point encore.

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

Dans cette leçon, les techniques liées au simple pivot de Gauss constituent l'essentiel des attendus. Il est impératif de faire le lien avec la notion de système échelonné (dont on donnera une définition précise et correcte) et de situer l'ensemble dans le contexte de l'algèbre linéaire, sans oublier la dualité. Un point de vue opératoire doit accompagner l'étude théorique et l'intérêt algorithmique des méthodes présentées doit être expliqué, éventuellement en l'illustrant par des exemples simples (où l'on attend parfois une résolution explicite). Parmi les conséquence théoriques, les candidates et candidats peuvent notamment donner des systèmes de générateurs de $\mathrm{GL}_n(\mathbf{K}$ et $\mathrm{SL}_n(K)$. Ils est aussi pertinent de présenter les relations de dépendance linéaire sur les colonnes d'une matrice échelonnée qui permettent de décrire simplement les orbites de l'action à gauche de $\mathrm{GL}_n(K)$ sur $\mathscr{M}_n(K)$ donnée par $(P,A) \mapsto PA$. Pour aller plus loin, les candidates et candidats peuvent exploiter les propriétés des systèmes d'équations linéaires pour définir la dimension des espaces vectoriels et obtenir une description de l'intersection de deux sous-espaces vectoriels donnés par des systèmes générateurs, ou d'une somme de deux sous-espaces vectoriels donnés par des équations. De même, des discussions sur la résolution de systèmes sur $\mathbf{Z}$ et la forme normale de Hermite peuvent trouver leur place dans cette leçon. Enfin, il est possible de présenter les décompostions LU et de Choleski, en évaluant le coût de ces méthodes ou encore d'étudier la résolution de l'équation normale associée aux problèmes des moindres carrés et la détermination de la solution de norme minimale par la méthode de décomposition en valeurs singulières.

Plan

I. Techniques d'échelonnement

def : matrices échelonnés
résolution d'un système d'équation linéaire avec une matrice échelonnée

I.1. Méthode du pivot

Opérations élémentaires sur une matrice
traduction en terme d'opérations par des matrices élémentaires
résultat : à partir de ces opérations élémentaires on peut réduire en une matrice échelonnée
cor : générateurs $\mathrm{GL}_n(K)$ et $\mathrm{SL}_n(K)$
app : connexité par arcs
pro : complexité du pivot $\frac{2n^3}{3} + O(n^2)$.
rem : problème de l'instabilité numérique, remarque orientation Décomposition de Hermite
app : résolution de systèmes diophantiens

I.2. Méthode de Householder

Matrices de Householder
lem : le fameux lemme
résultat : à partir de ces opérations élémentaires on peut réduire en une matrice échelonnée
cor : $\mathrm{O}_n(\mathbf{R})$ est engendré par les réflexions, $\mathrm{SO}_n(\mathbf{R})$ est engendré par les retournements pour $n \geqslant 3$.
pro : complexité Householder
rem : stabilité numérique, matrices de rotations de Givens.

I.3. Décomposition matricielles

Décomposition PLU pour le pivot de Gauss
pro : critère d'existence d'une décomposition LU
cor : matrice définie positive existence et forme → Cholesky
Décomposition QR pour la méthode de Householder
cor : QR + Gauss = Cholesky
algorithme de Crout pour cholesky, opérations et avantages numériques.

Conséquences théoriques et pratiques

Avec Gauss on peut résoudre nombres de problèmes d'algèbre linéaire : est ce qu'une famille est libre, est génératrice, est une base.
Réduction de Gauss donne l'existence d'une base et fournit un algorithme pour la calculer, parler aussi d'Hermite pour les modules libres
Householder donne l'existence d'une base orthogonal et donne un moyen pour la calculer

II. Déterminant

II.1. Définition du déterminant

Définition du déterminant d'une famille de vecteurs
formule de changement de base
def : orientation
rem : interprétation avec les composantes connexes

II.2. Formules de Cramer

Formules de Cramer [Gourdon]
ex : un exemple ?
app : déterminant de Gram
app : points remarquables du triangle
cor : Formule de la comatrice
rem : généralisation de la formule à un anneau
app : Cayley-Hamilton

II.3. Cas de systèmes rectangulaires

def : mineurs [Gourdon]
pro : rang = mineur [Gourdon]

app : rang est semi-continue inférieurement
th : rouché fontené [Gourdon]
ex : un exemple.

III. Résolution d'un système au sens des moindres carrés

III.1. Le problème des moindres carrés

énoncé du problème
équation normale
cas parfait → méthode de Cholesky
méthode QR

III.2. Décomposition en valeurs singulières

Décomposition en valeurs singulières
cor : approximation d'une matrice par des matrices de rang inférieur
app : résolution du problème des moindres carrés de norme minimal
rem : calcul de la svd

III.3. Modèles linéaires gaussiens

en légende...

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

La leçon débute par une étude générale des formes quadratiques, indépendamment du corps. On peut, par exemple, adopter le point de vue de l'action par congruence du groupe linéaire sur l'espace des matrices symétriques, ce qui permet de dégager quelques invariants (rang, discriminant), de s'interroger sur le nombre et la structure des orbites. L'algorithme de Gauss doit être énoncé et pouvoir être mis en œuvre sur une forme quadratique simple. En ajout de la classification sur $\mathbf{R}$, le candidat pourra parler de la classification des formes quadratiques sur le corps des complexes. Il est aussi possible de s'intéresser à la classification sur les corps finis. On peut s'intéresser au groupe orthogonal (générateurs, structure du groupe quand l'espace est de dimension 2). Le lien avec la dualité des espaces vectoriels permet de comprendre le sens de la décomposition de Gauss et de comparer les notions de sous-espace orthogonal, en s'interrogeant sur les conditions pour que que l'orthogonal d'un sous-espace vectoriel en soit un supplémentaire. La notion d'isotropie doit être connue. On pourra rattacher cette notion à la géométrie différentielle. Pour aller plus loin, on peut s'intéresser aux espaces hyperboliques, ou à l'étude de la géométrie d'un $\mathbf{R}$-espace vectoriel muni d'une forme quadratique de signature (p,q) notamment la structure du cône de lumière de l'espace-temps de Minkowski, avec la traduction géométrique de la notion d'orthogonal dans ce cas et des propriétés du groupe $\mathrm{O}(p,q)$.

I. Formes quadratique et orthogonalité

I.1. Formes quadratiques

On se donne E un K-espace vectoriel de dimension finie.

Définition 1 (Grifone)**.** Une forme quadratique sur E est une application $q : E \to K$ si étant donnée une base de E, q est un polynôme homogène de degré 2 en les composantes des vecteurs de la base, cette propriété ne dépendant pas du choix de la base.

Exemple 2. Pfaffien Déterminant sur $\mathscr{M}_2(\mathbf{R})$. Covariance

Proposition 3 (Grifone)**.** Si $\mathrm{car}(K) \neq 2$, à toute forme quadratique q sur E est associé une unique forme bilinéaire symétrique f tel que $q(x) = f(x,x)$ donnée par :

$$f(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)).$$

Inversement si $f : E \times E \to K$ est une forme bilinéaire symétrique, $x \mapsto f(x,x)$ est une forme quadratique sur E.

Exemple 4. Norme et produit scalaire Différentielle seconde

Notation : si f est une forme bilinéaire on notera f_x la forme linéaire $y \mapsto f(x,y)$.

Proposition 5 (Perso)**.** Si f est une forme bilinéaire sur E alors $\overline{f} : x \mapsto f_x$ est une application linéaire de E vers son dual E'. Inversement si $\ell : E \to E'$ est une application linéaire alors il existe une forme bilinéaire f tel que $f_x = \ell_x$, pour tout $x \in E$. [+ écriture en coordonnées].

On a ainsi fait la suite de correspondance :

$$\text{Formes quadratiques} \leftrightarrow \text{formes bilinéaires symétriques} \leftrightarrow \text{applications linéaires } E \to E'.$$

L'un des gain de cette correspondance est de ramener l'étude des formes quadratiques à celles des applications linéaires, cela peut être utile sachant notre bonne connaissance des applications linéaires.

I.2. Orthogonalité

Rappels sur l'orthogonalité en dualité...

Définition 6. Soit q une forme quadratique sur E de forme polaire f. Deux vecteurs $x, y \in E$ sont dits q-orthogonaux lorsque $f(x,y) = 0$ ce que l'on note $x \perp_q y$. Si A est une partie de E on note $A^{\perp_q}$ l'ensemble des vecteurs q-orthogonaux à tout élément de A.

Définir vecteurs isotropes.

Lemme 7. Avec les notations précédentes on a $A^{\perp} = \overline{f}(A)^{\circ}$.

Proposition 8 (Grifone)**.** Soit F un sous-espace de E. Alors,

- $\dim F^{\perp_q} = \dim E - \dim F + \dim(F \cap N(q))$;
- $F^{\perp\perp} = F + N(q)$.

où $N(q)$ est le noyau de q définit comme le noyau de l'application linéaire $\overline{f}$. Lorsque $N(q) = \{0\}$ on dit que q est non dégénérée.

Application 9. Si q est une forme quadratique non dégénérée et F est un sous-espace tel que $q_{|F} = 0$ (on dit que F est totalement isotrope) alors $\dim(F) \leqslant \frac{\dim(E)}{2}$. Cet argument est un point clé de la preuve du résultat suivant : (théorème de Flanders).

Corollaire 10 (Grifone)**.** Un sous-espace F de E est supplémentaire avec son orthogonal si et seulement $F \cap F^{\perp} = \{0\}$, on dit alors que F est anisotrope.

Application 11. Si x est un vecteur non isotrope alors $\langle x \rangle \oplus \langle x \rangle^{\perp} = E$.

I.3. Bases orthogonales

Théorème 12. Famille de représentants des carrés. Existence de base orthogonal

Algorithme de Gauss.

Exemple 13.

Proposition 14. Si q est anisotrope on peut préciser la matrice de changement de base...

Application 15. Décomposition de Choleski avec algorithme de calcul

Théorème 16. Réduction simultanée avec une structure euclidienne.

II. Classification des formes quadratiques

II.1. Équivalence de formes

Définition 17. équivalence

Proposition 18. Interprétation matricielle.

Exemple 19. *Classification sur un corps algébriquement clos*

II.2. Théorème d'inertie de Sylvester

Théorème 20. Classification sur $\mathbf{R}$, signature

Application 21. Optimisation avec différentielle à l'ordre 2

Corollaire 22. Lemme de Morse

Application 23. Méthode de Laplace

II.3. Classification sur un corps fini

Lemme 24. Dénombrement

Théorème 25. Classification

Application 26. Loi de réciprocité quadratique.

III. Le groupe orthogonal associé à une forme quadratique

III.1. Présentation

Définition 27. Définition du groupe orthogonal.

Proposition 28. Représentation matricielle

Exemple 29. Les cas de la dimension 2

Définition 30. Isométries positives et négatives

Proposition 31. Sous-groupe distingué, s'écrit comme un produit semi-direct

Exemple 32. Cas exceptionnel

III.2. Dévissage

On passe dans le cas réel.

Proposition 33. Centre.

Définition 34.

Proposition 35. Cartan Von-Neumann

Corollaire 36. Dérivée.

Théorème 37. Simplicité.

III.3. Représentation par les quaternions

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

Dans cette leçon, la loi d'inertie de Sylvester doit être présentée ainsi que l'orthogonalisation simultanée. L'algorithme de Gauss doit être énoncé et pouvoir être mis en oeuvre sur une forme quadratique simple ; le lien avec la signature doit être clairement énoncé et la signification géométrique des deux entiers r et s composant la signature d'une forme quadratique réelle doit être expliquée. La différentielle seconde d'une fonction de plusieurs variables est une forme quadratique importante qui mérite d'être présentée dans cette leçon. La définition et les propriétés classiques des coniques d'un plan affine euclidien doivent être connues. On peut présenter les liens entre la classification des formes quadratiques et celles des coniques ; de même il est intéressant d'évoquer le lien entre le discriminant de l'équation ax^2+bx+c et la signature de la forme quadratique $ax^2+bxy+cy^2$. La classification des quadriques n'est pas exigible, mais des situations particulières doivent pouvoir être discutées. Pour aller plus loin, les candidates et candidats peuvent aussi aller vers la théorie des représentations et présenter l'indicatrice de Schur-Frobenius qui permet de réaliser une représentation donnée sur le corps des réels.

Plan

I. Formes quadratiques réelles

I.1. Formalisme des formes quadratiques

Définition 1 (Grifone)**.** Une forme quadratique sur E est une application $q : E \to K$ si étant donnée une base de E, q est un polynôme homogène de degré 2 en les composantes des vecteurs de la base, cette propriété ne dépendant pas du choix de la base.

Proposition 2 (Grifone)**.** Si $\mathrm{car}(K) \neq 2$, à toute forme quadratique q sur E est associé une unique forme bilinéaire symétrique f tel que $q(x) = f(x,x)$ donnée par :

$$f(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)).$$

Inversement si $f : E \times E \to K$ est une forme bilinéaire symétrique, $x \mapsto f(x,x)$ est une forme quadratique sur E.

Notation : si f est une forme bilinéaire on notera f_x la forme linéaire $y \mapsto f(x,y)$.

Proposition 3 (Perso)**.** Si f est une forme bilinéaire sur E alors $\overline{f} : x \mapsto f_x$ est une application linéaire de E vers son dual E'. Inversement si $\ell : E \to E'$ est une application linéaire alors il existe une forme bilinéaire f tel que $f_x = \ell_x$, pour tout $x \in E$. [+ écriture en coordonnées].

I.2. Formes quadratiques positives, définies positives et norme

I.3. Théorème d'inertie de Sylvester

[•]

Théorème d'inertie de Sylvester ;

Algorithme de Gauss

App : en calcul différentielle point critique, lemme de Morse et méthode de Laplace

I.4. Plus sur le matrice de passage

[•]

Réduction simultanée

Décomposition de Cholesky, algo de Crout, comparaison avec Gauss, app vecteurs gaussiens et résolutions systèmes linéaires

II. Coniques

II.1. Formalisme algébrique

Lemme 4. Intersection d'un cône et d'un plan.

Définition 5. Définition des coniques [Audin]
conique propre = irréductible.

Remarque 6. Lien entre conique propre et cône.

Proposition 7. Par 5 points passe une conique

Théorème 8. Théorème de Pascal sur les 6 points.

II.2. Classification des coniques

Théorème 9. Classification des coniques [Audin]

Remarque 10. Symétries, centres.

Corollaire 11. Classification affine.

Application 12. Ellispe de Steiner

Proposition 13. Avec les 5 points comment déterminer le type.

II.3. Définition métrique

Proposition 14. Définition par foyers

Corollaire 15. Équation polaire.

Remarque 16. Cas des coniques à centre.

Proposition 17. Définition par directrice.

III. Le groupe orthogonal associé à une forme quadratique

III.1. Présentation

Définition 18. Définition du groupe orthogonal.

Proposition 19. Représentation matricielle.

Théorème 20. Structure de $O(p,q)$.

III.2. Dévissage

Proposition 21. Isométries positives. Sous-groupe distingué, s'écrit comme un produit semi-direct

Exemple 22. Structure en dimension 2.

Proposition 23. Centre.

Définition 24.

Proposition 25. Cartan Von-Neumann

Corollaire 26. Dérivée.

Théorème 27. Simplicité.

III.3. Représentation par les quaternions

190 : Méthodes combinatoires, problèmes de dénombrement

Il est nécessaire de dégager clairement différentes méthodes de dénombrement et de les illustrer d'exemples significatifs. De nombreux domaines des mathématiques sont concernés par des problèmes de dénombrement, cet aspect varié du thème de la leçon doit être mis en avant. L'utilisation de séries génératrices est un outil puissant pour le calcul de certains cardinaux. De plus, il est naturel de calculer des cardinaux classiques et certaines probabilités. Il est important de connaître l'interprétation ensembliste de la somme des coefficients binomiaux et ne pas se contenter d'une justification par le binôme de Newton. L'introduction des corps finis (même en se limitant aux cardinaux premiers) permet de créer un lien avec l'algèbre linéaire. Les actions de groupes peuvent également conduire à des résultats remarquables. Pour aller plus loin, les candidates et candidats peuvent aussi présenter des applications de la formule d'inversion de Möebius ou de la formule de Burnside. Des candidates et candidats ayant un bagage probabiliste pourront explorer le champ des permutations aléatoires, en présentant des algorithmes pour générer la loi uniforme sur le groupe symétrique S_n et analyser certaines propriétés de cette loi uniforme (points fixes, cycles, limite $n \to \infty$).

I. Cardinal d'un ensemble fini

I.1. Définition

Référence : Gourdon

- Définition cardinal par les bijections
- Proposition : injection, surjection et bijection
- Conséquence : principe des tiroirs et applications.

I.2. Dénombrements fondamentaux

Listes et arrangements

Simplement n^p et $(n)_p$ et interprétations

Combinaisons

$\binom{n}{p}$ expression et interprétation, formule de Pascal, généralisation par les coefficients multinomiaux. Remarque combinaison avec remise.

Partitions

$\left\{ \begin{matrix} n \\ p \end{matrix} \right\}$ formule de récurrence, expression à l'aide de la formule du crible, interprétations : surjections, nombres de partitions.

II. Méthodes de dénombrement

II.1. Opérations ensemblistes

Référence : Feller.

- Formule du crible de Poincaré
- Application de la formule du crible : expression de l'indicatrice d'Euler, dérangements revenir sur les partitions [10] (Voir Algèbrie)

10. autres : probabilités que deux nombres soient premiers entre eux

- Généralisation de la formule du crible par Feller, exactement m évènements et au moins m évènements. Application à $\mathscr{L}(C_j)$ (**DEV1**).

II.2. Dénombrement en présence de groupes

- Rappels actions de groupes. Relation orbite-stabilisateur
- Exemple : annagrammes de Mississipi
- Exemple : loi complète des cycles
- Illustration en algèbre linéaire sur un corps fini : dénombrement des diagonalisables, des nilpotents, des trigonalisables

III. Formes standard en dénombrement

III.1. Produit de Cauchy

- Définition produit de Cauchy, propriétés et règles d'inversion.
- Exemple : formule d'inversion de Pascal, application : formule des partitions
- Série génératrice et règles de calculs
- Application : Vandermonde, nombres de Bell
- Proposition : règle de Hadamard, majorations de Cauchy
- Illustration sur les partitions d'un entier : $\limsup p_n^{1/n} = 1$ et mieux $p_n \leqslant \dots$

III.2. Produit de Dirichlet

- Définition et propriétés, règle d'inversion
- Exemple inversion de Mobius
- Application à l'indicatrice d'Euler
- Définition série de Dirichlet et règles de calcul
- Application : ordre moyen indicatrice d'Euler

III.3. Dénombrement des orbites

- Formule de Burnside
- Application au placement des chaises autour d'une table ronde
- Application aux coloriages

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

Le jury souhaite proposer une leçon qui offre une ouverture large autour du thème de la géométrie. Avec cet intitulé, les candidates et candidats sont libres de présenter des résultats et des exemples très variés en lien avec la géométrie. L'objectif n'est pas de couvrir le plus d'aspects possible, mais plutôt d'en proposer certains suffisamment consistants et variés. À partir du moment où ils sont de nature géométrique, tous les éléments du programme peuvent être pertinents. En contrepartie de cette liberté laissée aux candidates et candidats, une difficulté est de structurer la présentation des objets et des notions choisis. Ainsi, plusieurs approches sont possibles pour organiser cette leçon, par exemple : - en regroupant les outils par " famille " : outils matriciels (repérage des points par des matrices colonnes, des transformations par des matrices, rang, réduction, etc.), outils polynomiaux (formes quadratiques, déterminant, résultant, etc.), outils structurels (groupes, corps) ; - ou par niveau d'abstraction/de généralité (nombres réels, complexes, matrices, groupes...) ; - ou par type d'objectifs (identifier des objets géométriques, les mesurer, les classifier, démontrer des résultats en utilisant des transformations géométriques...) Il est aussi possible de se focaliser sur un seul type d'outils (par exemple algèbre linéaire, géométrie affine ou groupes) en détaillant plusieurs applications en géométrie ou sur une question géométrique fouillée à l'aide de diverses techniques (par exemple sur des problèmes impliquant des figures géométriques comme les cercles et triangles, les polygones et polyèdres réguliers, etc.). Des situations " élémentaires ", dans le plan, permettent certainement de mettre en valeur des connaissances et un recul mathématique. Il faut bien éviter l'écueil d'un catalogue fastidieux ou celui qui consisterait à recycler directement le contenu d'une autre leçon avec un vague habillage géométrique. Parmi les nombreux éléments qui peuvent être discutés, on peut indiquer : - les notions de distance, aire, volume. Notamment les propriétés de la matrice de Gram, le lien entre déterminant et aire d'un parallélogramme ou volume d'un parallélépipède, la construction du produit vectoriel et du produit mixte,... peuvent être exploités avec pertinence dans cette leçon. On peut ainsi être amené à étudier l'aire balayée par un arc paramétré du plan, la position d'un point par rapport à un cercle circonscrit à un triangle, etc. Le déterminant de Cayley- Menger permet de mettre en évidence des conditions pour que $n+1$ points de $\mathbf{R}^n$ forment une base affine, ou que $n+2$ points de $\mathbf{R}^n$ soient cocycliques. Dans une autre direction, la division euclidienne dans $\mathbf{Z}$ donne une preuve d'une forme du théorème de la base adaptée, avec pour conséquence le calcul du volume (d'une maille élémentaire) d'un sous réseau de $\mathbf{R}^n$ comme étant le déterminant d'un système générateur dans la base canonique. - l'apport de l'algèbre linéaire à la géométrie. On peut ainsi exploiter le calcul matriciel et les techniques de réduction pour mettre en évidence des informations de nature géométrique (avec les exemples fondamentaux des homothéties, projections, symétries, affinités, rotations, la classification des isométries vectorielles, etc.). On peut être alors amené à présenter le théorème de Cartan-Dieudonné sur la décomposition d'isométries euclidiennes en produit de réflexions ou encore évoquer une (ou des) interprétation(s) géométrique(s) de la décomposition en valeurs singulières. Dans cette même veine, la leçon peut être orientée vers la géométrie affine, en s'adossant à la théorie des espaces vectoriels pour définir certains objets (espaces et sous- espaces affines, applications affines, repères affines, etc), ce qui permet, par exemple, d'établir ainsi certains résultats classiques, comme les théorèmes de Thalès, Pappus, Desargues,... - l'analyse des formes quadratiques permet d'aborder des problèmes géométriques : étude des coniques, quadriques, classification des quadriques de $\mathbf{R}^n$, interprétation géométrique de la signature, application des méthodes de réduction, etc. - la théorie des groupes est un champ naturel pour cette leçon (mais qui n'est cependant pas indispensable) : groupes de transformations (isométries, déplacements, similitudes, translations), composition de transformations, mise en évidence d'invariants fondamentaux (angle, birapport, excentricité d'une conique). Il est possible de se focaliser sur des groupes de transformations préservant une certaine structure géométrique et en distinguant parmi eux les groupes finis (groupes d'isométries classiques), les groupes discrets infinis (avec des translations, groupes de pavages) et, pour aller plus loin, les groupes continus (groupes de Lie). - les techniques de

convexité constituent aussi un champ fructueux : le théorème de séparation par un hyperplan dans $\mathbf{R}^n$ de Hahn-Banach et, en corollaire, le théorème de Helly permettent par exemple d'établir des propriétés intéressantes sur les cordes de convexes compacts. - certains candidates et candidats peuvent trouver intérêt à aborder les questions d'intersection de courbes polynomiales, qui permettent notamment de mettre en oeuvre le théorème de Bezout et des méthodes exploitant la notion de résultant. - un grand nombre de problèmes de géométrie peuvent être traités en exploitant le formalisme des nombres complexes. Il est tout à fait approprié d'évoquer l'étude des inversions et, en particulier, la possibilité de ramener un cercle à une droite et inversement ; la formule de Ptolémée illustre bien l'utilisation de cet outil. On peut parler des suites définies par récurrence par une homographie et leur lien avec la réduction dans $\mathrm{SL}_2(\mathbf{C})$ et aborder la construction de la sphère de Riemann. - les problématiques de la construction à la règle et au compas constituent un autre axe pertinent pour cette leçon, avec le théorème de Wantzel, et peuvent conduire à s'intéresser à des extensions de corps. Comme dans le cas des autres leçons, il est tout à fait bienvenu de chercher à illustrer cette leçon par des exemples issus de l'analyse, des probabilités, de la statistique (par exemple en évoquant l'interprétation géométrique de l'analyse en composantes principales), du calcul formel (par exemple avec les applications du résultant) ou du calcul scientifique (par exemple en présentant des problématiques de géométrie computationnelle, comme le calcul d'enveloppe convexe, les algorithmes de triangulation de Delaunay, les diagrammes de Voronoi...). Les thèmes en lien avec la géométrie projective ou la géométrie algébrique peuvent permettre à certains candidates et candidats de présenter des résultats très avancés. Cette leçon nécessite une préparation très personnelle et réfléchie. Les exemples et les résultats qui y sont présentés ont vocation à inciter les candidates et candidats à enrichir les autres leçons de cette épreuve d'exemples issus de la géométrie.

I. Utilisation de systèmes de coordonnées

I.1. Illustration sur les nombres constructibles

Le tout sur les nombres constructibles, de la définition au théorème de Wantzel au problèmes grecs insolubles et pour terminer les polygones réguliers constructibles. Voir Audin et Perrin.

I.2. Constructions de systèmes adaptées

Constructions de bases q-orthogonales pour une forme quadratique, théorème spectral, classification affine et euclidienne des coniques.

I.3. Réduction des transformations géométriques

Décomposition canonique, théorème de réduction des isométries, exemple en dimension 1 ou 2.

II. Outils algébriques

II.1. Le déterminant

Définition, interprétation en terme de volume, formules de Cramer avec application aux points remarquables du triangle

II.2. Utilisation pour le calcul d'un point à un sous-espace

Matrices de Gram, formule de Gram et exemple facile avec forme linéaire.

II.3. Un autre exemple : le produit vectoriel

Voir Audin.

III. Groupes de transformations

III.1. Définition d'invariants

Exemple groupe des angles (Audin), exemple birapport.

III.2. Recherche d'invariants

Voir Caldero. Par exemple on peut chercher les invariants de l'action de $\mathrm{O}_2(\mathbf{R})$ sur $\mathbf{R}[X_1, X_2, X_3, X_4]$.

III.3. Utilisation de la transitivité

Exemple : les médianes s'intersectent, ellipse de Steiner

IV. Structures algébriques

IV.1. Nombres complexes

Le plan complexe avec interprétation géométrique de la multiplication, isomorphisme $SO_2(\mathbf{R})$ avec la sphère, application au théorème de Napoléon. Caractérisation de l'alignement avec application Ptolémée.

IV.2. Quaternions

Voir Perrin. Isomorphismes remarquables.

Bibliographie

[CG13] P. Caldero and J. Germoni. *Histoires hédonistes de groupes et géométrie - Tome 1*. Calvage et Mounet, 2013.

[Dem97] M. Demazure. *Cours d'algèbre*. Cassini, 1997.

[Gou21] X. Gourdon. *Les maths en tête. Algèbre et probabilités - 3e édition*. Ellipses, 2021.

[Gri24] J. Grifone. *Algèbre linéaire 7ème édition*. Cépaduès, 2024.

[MM22] R. Mansuy and R. Mneimné. *Algèbre linéaire. Réduction des endomorphismes*. Deboeck supérieur, 2022.

[Per96] D. Perrin. *Cours d'algèbre (Agrégation)*. Ellipses, 1996.

[SP99] P. Saux Picart. *Cours de calcul formel - Algorithmes fondamentaux*. Ellipses, 1999.