Leçons d'algèbre à l'agrégation

Maximilien Dreveton

23 novembre 2016

Résumé

Ce document regroupe des plans de leçons que j'ai tapé durant mon année de préparation à l'agrégation (2014-2015). Ils sont bien évidement imparfaits, relus par personne (et honnêtement c'est à peine si je me suis relu moi même). En particulier, je ne les ai pas retouchés une fois l'agreg passée. Parmi ces plans, certain sont originaux et ne ressemblent en rien aux plan que l'on peut trouver ailleurs, mais la plupart s'inspirent fortement de plan classiques, déjà fait par les génération d'agrégatifs avant moi. Enfin, et cette remarque est importante, certains plans mentionnent des résultats probablement trop difficiles, que je n'aurai jamais osé présenter à l'oral le jour J.

Afin de faciliter la préparation à l'agreg, j'ai voulu être le plus clair possible, et de mettre autant que possible les références où l'on pompe scandaleusement les énoncés des théorèmes et les exemples classiques. Des passages entiers sont des copiés/collés de bouquins, mais c'est assumé, tout le monde faisant pareil afin de se simplifier la tâche le jour de l'épreuve.

J'espère que document pourra servir de base de travail pour de futurs agrégatifs.

TABLE DES MATIÈRES

LEÇON 101

GROUPE OPÉRANT SUR UN ENSEMBLE. EXEMPLES ET APPLICATIONS.

Référence : Perrin, Serre (représentations), H2G2

Développements

- SU(2) SO(3)
- cône nilpotent
- Molien
- Automorphisme de Sn
- (table de caractère de S4)
- (réciprocité quadratique)

I Définitions et premières propriétés

Définition 1. *G un groupe, X un ensemble.* $\rho : G \times X \to X$ *est une action de G sur X si :*
1/ $\rho(e, x) = x \quad \forall x \in X$*, où e est le neutre de G*
2/ $\forall g, h \in G \quad \forall x \in X \ \rho(gh, x) = \rho(g, \rho(h, x))$

Proposition I .1. *Si* $\rho : G \times X \to X$ *est une action de groupe,* $\phi : G \to Bij(X)$ *est un morphisme de groupe.*
Inversement, si $\phi : G \to Bij(X)$ *est un morphisme de groupes, alors est une action de groupe.*

Exemples :
G agit sur lui même par translation, conjugaison.
G agit sur $\mathcal{P}(G)$ par translation (g.S=gS).
G agit sur G/H (H sous groupe de G) par translation : g.xH=gxH
S_n agit sur $\{1, \dots, n\}$ de façon naturelle
$\forall \sigma \in \mathcal{A}_n, < \sigma >$ agit de la même façon sur $\{1, \dots, n\}$.
Dans la suite : G groupe, X ensemble, ρ action de G sur X.

Définition 2. *Orbite, stabilisateur, fix*

Définition 3. *transitive si* $\forall x, y \in X \exists g \in G : \rho(g, x) = y$
fidèle si $Fix(g) = X \Rightarrow g = e$
simple si $\forall x \in X \rho(g, y) = y$

Exemples : transitive et simple implique fidèle
L'action de G sur Orb(x) est transitive.
L'action de G sur G par translation est fidèle.
L'action de G sur G/H avec H distingué n'est pas fidèle.
Pour l'action de G sur G par conjugaison : Orb(g) est appelé classe de conjuguaison ; Stab(g) est appelé centralisateur de g.
L'action de G/Kerϕ sur X est fidèle.
Pour l'action de $< \sigma >$ (où $\sigma \in S_n$) sur $\{1, \dots, n\}$, les orbites correspondent aux supports des cycles dans la décomposition de σ en produit de cycle à support disjoint.
L'action de $\mathcal{A}_n$ sur $\{1, \dots, n\}$ est (n-2) fois transitive.

Définition 4. *Relation d'équivalence :* $x \equiv y \iff \exists g \in G : \rho(g,x) = y \iff y \in Orb(x)$

Remarque : $y \in Orb(x) \iff x \in Orb(y) \iff Orb(x) = Orb(y)$ Donc $X = \cup_{x \in X/\sim} Orb(x)$ (union disjointe). On vient de montrer :

Proposition I .2. *Formule des classes*
Si G et X sont finis, $|X| = \sum_{x \in X/\sim} |Orb(x)|$

Proposition I .3. *Stab(x) est un sous groupe de G pour tout x dans X. De plus :*

$$G/Stab(x) \to Orb(x); gStab(x) \mapsto g.x$$

est bijective.

Rq : cette application n'est pas en général un morphisme de groupe !

Démonstration. Bien défini : si gStab(x)=g'Stab(x), alors $\exists h \in Stab(x)$ tel que $g' = gh$. Donc $g'.x = (gh).x = g.(h.x) = g.x$ car h est dans Stab(x).
Surjectif : par construction.
Injectif : si g.x = g'.x, alors $g^{-1}g \in Stab(x)$. □

Corollaire I .4. *Si G fini,* $|G| = |Stab(x)||Orb(x)|$

Application : $C_n^p = \frac{n!}{p!(n-p)!}$

Proposition I .5. *Formule de Burnside*
Si G et X sont finis, alors :
$|/\sim| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$

II Comprendre G

II .1 Action de G sur lui même

Action par translation à gauche

Théorème II .1. *Cayley*

Démonstration. Action par translation à gauche □

Remarque : S_n isomorphe à un sous groupe de $GL_n(K)$ donc G aussi.
Considérons l'action de G sur G/H (H sous groupe de G) par translation à gauche.

Proposition II .2. $Ker\phi = \cap_{g \in G} gHg^{-1}$

Application : G groupe infini, H sous groupe de G d'indice fini, alors G n'est pas simple.

Action par conjuguaison

Définition 5. *Le centre de G, noté Z(G) est l'ensemble* $\{g \in G \forall h \in G gh = hg\}$

Rq : G abélien ssi G=Z(G) ; Z(G) est un sous groupe de G.

Proposition II .3. *L'équation des classes devient, pour l'acion par conjugaison :*

$$|G| = |Z(G)| + \sum_{g/|Orb(g)| \geq 2} |Orb(g)|$$

Application : Si G est un p-groupe, alors $|Z(G) = 0[p]$, donc $Z(G) \neq e$.
Tout groupe d'ordre p^2 est abélien.

II .2 Représentations linéaires

[Serre]
G groupe fini, de neutre 1, V un $\mathbb{C}$ espace vectoriel de dimension finie.

Définition 6. *Une représentation linéaire de G dans V est un morphisme ρ de G dans GL(V).*
On appelle degré de la représentation la dimension de V.

Définition 7. *On dit que ρ et ρ' sont deux représentations semblables s'il existe un isomorphisme linéaire $\tau : V \to V'$ tq :*

$$\tau \circ \rho(s) = \rho'(s) \circ \tau \quad \forall s \in G$$

Si R_s et R'_s sont les matrices représenant ρ et ρ', la condition s'écrit aussi : $R'_s = TR_sT^{-1}$ avec T inversible.
On identifie deux telles représentations ; elles ont le même degré.

Définition 8. *Soit W sev de V, invariant par G, cad $x \in W \Rightarrow \rho(s)(x) \in W \ \forall s \in G$.*
La restriction de ρ^W à W est un isomorphisme de W dans lui même : on dit que W est une sous représentation de V.

Théorème II .4. *ρ représentation de G dans V et W sev de V stable par G. Alors, il existe un supplémentaire W^0 de W dans V qui est stable par G.*

Démonstration. Par moyennisation. □

Définition 9. *ρ est dite irréductible ou simple si V n'est pas réduit à 0 et si aucun sev de V n'est stable par G (à part 0 et V).*

Théorème II .5. *(Maschke)*
Toute représentation est somme directe de représentations irréductibles.

Démonstration. Par récurrence sur la dim(V), en utilisant le thm précédent. □

Définition 10.

$$\forall s \in G \quad \xi_\rho(s) := Tr(\rho_s)$$

est appelé le caractère de la représentation ρ.

Proposition II .6. *Un caractère est constant sur les classes de conjugaison : c'est un exemple particulier de fonction centrale. Par ailleurs, $\xi(1) = n$ où n est le degré de la représentation associée.*

Lemme II .7. *Lemme de Schur*
Soit $\rho^1 : G \to GL(V_1)$ et $\rho^2 : G \to GL(V_2)$ deux représentations irréductibles de G, et f linéaire de V_1 dans V_2 telle que $\rho^2(s) \circ f = f \circ \rho^1(s) \ \forall s \in G$. Alors :
1/ Si ρ^1 et ρ^2 ne sont pas isomorphes, on a f=0.
2/ Si $V_1 = V_2$, $\rho^1 = \rho^2$, f est une homothétie (ie un multiple scalaire de 1).

Théorème II .8. *Si ξ est le caractère d'une représentation irréductible, on a $(\xi|\xi) = 1$.*
Si ξ et ξ' sont des caractères de deux représentations irréductibles non isomorphes, on a $(\xi|\xi') = 0$.

Théorème II .9. *Soit V représentation de G, de caractère ϕ, et supposons*

$$V = W_1 \oplus \cdots \oplus W_k$$

Alors si W est une représentation irréductible de caractère ξ, le nombre des W_i isomorphes à W est égal au produit scalaire $(\phi|\xi) =< \phi, \xi >$

Corollaire II .10. *Le nombre des W_i isomorphes à W ne dépend pas de la décomposition choisie.*

Corollaire II .11. *Deux représentations de même caractère sont isomorphes.*

Le critère suivant d'irréductibilité est très commode en pratique :

Théorème II .12. *Si ψ est le caractère d'une représentation V, $(\phi|\phi)$ est un entier positif, et on a $(\phi|\phi) = 1$ si et seulement si V est irréductible.*

Exemple :

III Comprendre X

III .1 Des isomorphismes induits par actions de groupes

III .2 Algèbre linéaire

[H2G2]
équivalence (théorème du rang)
conjugaison : récupérer des réduction classiques (Jordan) par l'action de $GL_n(C)$ d'abord sur $D_n(C)$, $T_n(C)$ puis $M_n(C)$. (On n'est absolument pas en train de copier coller H2G2).

III .3 Algèbre bilinéaire

[H2G2]

Action par congruence. Dans R, thm de Sylvester. Stab($I_{p,q}$)=O(p,q). On retrouve les groupes orthogonaux, donner quelques propriétés sur eux.

LEÇON 102

GROUPES DES NOMBRES COMPLEXES DE MODULE 1. SOUS-GROUPES DES RACINES DE L'UNITÉ. APPLICATIONS.

Références : Vidonne, Groupe circulaire, rotations et quaternions (pour le première partie)
Rudin, Gozard (analyse)
Demazure, Perrin, Peyré (algèbre)

Rapport 2008 : Les polynômes cyclotomiques (programme 2009) trouveront naturellement leur place dans cette leçon. Leur irréductibilité doit être maîtrisée.

Rapport 2009 : Les propriétés des polynômes cyclotomiques doivent être énoncées. Leur irréductibilité sur Z doit être maîtrisée. Il est tout à fait possible de parler d'exponentielle complexe, de théorème du relèvement ou de séries de Fourier tout en veillant à rester dans le contexte de la leçon.

Rapport 2015 : Cette leçon est encore abordée de façon élémentaire sans réellement expliquer où et comment les nombres complexes de modules 1 et les racines de l'unité apparaissent dans divers domaines des ma- thématiques (polynômes cyclotomiques, spectre de matrices remarquables, théorie des représentations). Il ne faut pas non plus oublier la partie "groupe" de la leçon : on pourra s'intéresser au relèvement du groupe unité au groupe additif des réels et aux propriétés qui en résultent (par exemple l'alternative "sous-groupes denses versus sous-groupes monogènes"). On pourra aussi s'intéresser aux groupes des nombres complexes de $\mathbb{Q}[i]$, et les racines de l'unité qui y appartiennent.

Préliminaires et notation

On suppose construit le corps des complexes. La fonction valeur absolue est un morphisme de groupe de $\mathbb{C}^*$ dans $\mathbb{R}_+^*$, son noyau est noté $\mathbb{U}$.

I Exponentielle, fonctions trigonométrique. Lien avec la géométrie planaire

I .1 Fondations de la trigonométrie

$$\exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

Proposition I .1. *Premières propriétés*
(i) exp(z+z')= exp(z) exp(z')
(ii) exp est continûement différentiable en 0, et est égale à sa propre dérivée.
(iii) exp ne s'annule jamais : elle est localement étale (th inversion locale).

Proposition I .2. *exp est un morphisme de groupe de* $(\mathbb{C}, +)$ *dans* $(\mathbb{C}^*, \times)$*, surjectif (*$\exp(\mathbb{C}) = \mathbb{C}^*$*) mais non injectif.*

Preuve I .3. $\exp(\mathbb{C})$ *est un sous groupe ouvert de* $\mathbb{C}^*$*, et* $\mathbb{C}^*$ *est connexe.*

Proposition I .4. *Étude de* $\ker \exp$
$\ker \exp$ *est un sous groupe non trivial de* $i\mathbb{R}$*, fermé. Il est donc de la forme* $ib\mathbb{Z}$*, où* $b = \inf\{x > 0, \exp(ix) = O\}$.

Preuve I .5. *ker exp fermé comme image réciproque d'un fermé par une application continue.*

On a $\exp(z)^* = \exp(z^*)$. *Donc* $\exp(z)$*=1 implique* $\exp(z + z*) = 1$, *mais* $z + z* \in \mathbb{R}$ *donc est égal à 0, et* $z \in i\mathbb{R}$. *Don ker exp est un sous groupe de* $i\mathbb{R}$, *non trivial car par surjectivité de exp, il exista a tel que* $exp(a) = -1$, *et donc 2a est dans ker exp, et a non nul. ker exp* $\neq i\mathbb{R}$ *car sinon* $exp(\mathbb{C}) \in \mathbb{R}$.

Définition 11. *Définition de* π *:*

$$\ker \exp = 2\pi\mathbb{Z}$$

Définition 12. *Formules d'Euler :*

$$\exp(ix) = cos(x) + isin(x)$$
$$\cos(z) = \frac{\exp(ix) + \exp(-ix)}{2}$$
$$\sin(z) = \frac{\exp(ix) - \exp(-ix)}{2i}$$

cos *est paire,* sin *est impaire ;* cos *et* sin *sont* 2π *périodiques, et on a* $\sin(x + \pi/2) = \cos(x)$.

Proposition I .6. *Forumules de Moivre, polynômes de Tchebichev, noyau de Dirichlet.*
$(\exp(ix))^n = \cos(nx) + i\sin(nx)$
$\cos^n(x) = P_n(\cos x)$
$\sum_{k=-}^{N} \cos(kx) = ...$

Proposition I .7. *Soit* $\rho : (\mathbb{R}, +) \to (\mathbb{C}^*, x)$ *un morphisme de groupe continu. Alors il existe* $a \in \mathbb{C}$ *tel que* $\forall x \in \mathbb{R}, \rho(x) = \exp(ax)$.

Preuve I .8. *Th relèvement des applications continues, il existe une unique* ρ *telle que :*
(i) $\rho(0) = 0$
(ii) $\forall x \in \mathbb{R}, \rho(x) = \exp(\rho(x))$.
etc

Proposition I .9. *exp :* $\mathbb{R} \to \mathbb{U}$ *est un morphisme surjectif, non injectif, de noyau* $2\pi\mathbb{Z}$.
Donc $\mathbb{U}$ *isomorphe à* $\mathbb{R}/2\pi\mathbb{Z}$

Proposition I .10. *Tout morphisme continu de* $(\mathbb{R}, +)$ *dans* $(\mathbb{U}, \times)$ *est de la forme* $t \to \exp(it)$

I .2 Angles et rotations planes

On rappelle : $SO(2) = \{\phi \in O(2) : det(\phi) = 1\}$
On note E le plan vectoriel de $\mathbb{R}^2$ muni du produit scalaire usuel. La sphère unité de E est notée $\mathbb{S}^1$
On note $\mathbb{U} = \{u \in \mathbb{C} : |u| = 1\}$. On identifie le plan complexe à $\mathbb{R}^2$, donc $\mathbb{U}$ est la même chose que la sphère unité $\mathbb{S}^1$ de $\mathbb{R}^2$.

Théorème I .11. *So(2) agit transitivement et simplement sur* $\mathbb{U}$, *c'est-à-dire :*

$$\forall u, v \in \mathbb{U}, \exists!\ f \in SO(2) \text{ tq } f(u) = v$$

.

Preuve I .12. *SO(2) agit transitivement : notons* τ *la symétrie d'axe* $D = \mathbb{R}(u + v)$ *et* τ' *la symétrie d'axe* $\mathbb{R}v$. *Alors* $\tau' * \tau \in SO(2)$ *et* $\tau' * \tau(u) = v$.
SO(2) agit simplement : supposons qu'il existe f et g telles que f(u)=g(u). Alors l'application $g^{-1} * f \in SO(2)$ *fixe point par point la droite* $\mathbb{R}u$, *donc* $g^{-1} * f = id$.
(On utilise le fait que si $f \in SO(2)$ *fixe une droite D point par point, f=id.)*

Définition 13. *L'espace E est dit orienté lorsque l'on a choisi une base orthonormée de référence* $\beta = (e_1, e_2)$. *Une base orthonormée* $\beta' = (e'_1, e'_2)$ *de E est dite orientée dans le sens direct lorsqu'il existe* $f \in SO(2)$ *telle que* $f(e_i) = e'_i$ *pour i=1,2. Autrement dit, lorsque* $\det f = \det_{beta} \beta' = 1$. *Plus généralement, une base quelconque* β'' *est dite directed ou orientée dans le même sens que* β *lorsque* $\det_{beta} \beta'' > 0$.

A partir de là, on fixe une base (e_1, e_2) orthonormée de E, et on note M(f) la matrice associée à $f \in O(2)$ dans cette base.

Proposition I .13. *L'application*

$$\begin{array}{rccc} \rho : & \mathbb{U} & \to & SO(2,\mathbb{R}) = \{M(f) : f \in SO(2)\} \\ & \exp(i\theta) & \to & R(\theta) = \begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix} \end{array}$$

est un isomorphisme topologique de groupe. En particulier, $SO(2, \mathbb{R})$ *est commutatif, connexe et compact.*

Remarque : On peut aussi écrire ρ comme :

$$\begin{array}{rccc} \rho : & \mathbb{U} & \to & SO(2,\mathbb{R}) \\ & a + ib & \to & \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{array}$$

I .3 Angles orientés de vecteurs

Soit $\mathcal{A}$ l'ensemble des couples de vecteurs unitaires de $\mathbb{R}^2$. On définit sur $\mathbb{A}$ la relation d'équivalence suivante :
$(u,v) \equiv (u',v') \iff \exists R_\theta \in SO(2,\mathbb{R}) \text{ tq } R_\theta(u) = u' \text{et} R_\theta(v) = v'$
$\mathbb{A}/\equiv$ est l'ensemble des angles orientés de vecteurs.

Proposition I .14. *L'application de $\mathbb{A}/\equiv$ dans $SO(2,\mathbb{R})$ qui à un représentant (u,v) associe $R_\theta \in SO(2,\mathbb{R})$ tq $R_\theta(u) = v$ est bien définie et est une bijection.*

Proposition I .15. *Relation de Chasles*
$\forall u,v,w \in \mathbb{S}^1, (u,v) + (v,w) = (u,w)$

Preuve I .16. *Notons f (resp. g) la roation correspondante à (u,v) (resp à (v,w)). Alors f(u)=v et g(v)=w, donc g*f(u)=v.*

Proposition I .17. *L'isomorphisme $\mathbb{R}/2\pi\mathbb{Z} \to SO(2,\mathbb{R})$*
permet de définir une mesure des angles orientés de vecteurs.

Preuve I .18. $A <-> SO(2) <-> SO(2,\mathbb{R}) <-> \mathbb{U}$

L'isomorphisme entre SO(2) et SO(2,$\mathbb{R}$) dépend de l'orientation de E, c'est à dire du choix d'une base orthonormée de référence. Comme $\begin{array}{ccc}\mathbb{R} & \to & \mathbb{U} \\ \theta & \to & \exp(i\theta)\end{array}$ est un morphisme de groupe surjectif dont le noyau est $2\pi\mathbb{Z}$; on a l'isomorphisme :

$\begin{array}{ccc}\mathbb{R}/2\pi\mathbb{Z} & \to & \mathbb{U} \\ \theta & \to & \exp(i\theta)\end{array}$ A chaque angle correspond donc un nombre réel défini à 2π près. Ce nombre s'appelle la mesure de cet angle.

Dans la pratique, dès que l'on a défini une orientation sur E, alors A/≡, SO(2) et $\mathbb{R}/2\pi\mathbb{Z}$ deviennent des ensembles indiscernables en tant que groupes. On parle alors indifféremment d'une rotation, d'un angle ou de sa mesure.

II Racines de l'unité. Sous groupe des racines n-ième de l'unité

Dans toute la suite, n désigne un entier naturel non nul.

II .1 Sous groupe $\mathbb{U}_n$

Définition 14. *L'application $\begin{array}{ccc}\mathbb{U} & \to & \mathbb{U} \\ z & \to & z^n\end{array}$ est un morphisme. Son noyau est un sous groupe de $\mathbb{U}$, que l'on note U_n, c'est l'ensemble des racines n-ième de l'unité.*

Corollaire II .1. *Les racines n-ièmes de l'unité sont donc les solutions de l'équation $z^n - 1 = 0$. Autrement dit, $X^n - 1 = \prod_{\xi \in \mathbb{U}_n}(X - \xi)$*

Proposition II .2. $\begin{array}{ccc}\mathbb{Z}/n\mathbb{Z} & \to & \mathbb{U}_n \\ k & \to & \exp(2i\pi k/n)\end{array}$ *est un isomorphisme de groupe.*

Corollaire II .3. $\mathbb{U}_n$ *est cyclique de cardinal n.*

Proposition II .4. $\mathbb{U}_n$ *est le seul sous groupe de cardinal n de $\mathbb{C}^\times$*

Applications Les sous groupes finis de $SO(2,\mathbb{R})$ sont cycliques.
Les sous groupes finis de $O(2,\mathbb{R})$ sont cycliques ou diédraux.

Définition 15. *Le générateur de $\mathbb{U}_n$ est*

$$\mathbb{U}_n^\times = \{\exp(2i\pi k/n), pgcd(k,n) = 1\}$$

. En particulier, $|\mathbb{U}_n^\times| = \phi(n)$. On appelle racines primitives de l'unité les éléments de $\mathbb{U}_n^\times$.

Proposition II .5. $\mathbb{U}_d \in \mathbb{U}_n \iff d|n$.

Application $\mathbb{U}_n = \bigcup_{d|n} \mathbb{U}_d$

Corollaire II .6. $\phi(n) = \sum_{d|n} \phi(d)$

Proposition II .7. *Un sous groupe de $\mathbb{U}$ est soit dense dans $\mathbb{U}$, soit fini, auquel cas il est de la forme $\mathbb{U}_n$ (pour un certain n).*

II .2 Polynômes cyclotomiques

Définitions Demazure, p.215

Définition 16. *Soit n un entier positif. On appelle n-ième polynôme cyclotomique, noté $\Phi_n(X) = \prod_\xi (X - \xi)$ où ξ parcourt les racines n-ième primitives de l'unité dans $\mathbb{C}$.*

Autrement dit, $\Phi_n(X) = \prod_{n \in (\mathbb{Z}/n\mathbb{Z})^*} (X - \exp(2\pi i k/n))$
De plus, on a : $X^n - 1 = \prod_{n \in (\mathbb{Z}/n\mathbb{Z})} (X - \exp(2\pi i k/n))$ par définition du groupe $\mathbb{U}_n$.

Proposition II .8. *(i) Φ_n est un polynôme unitaire à coefficients entiers de degré $\phi(n)$ où ϕ est l'indicatrice d'Euler.*
(ii) Le polynôme $X^n - 1$ est le produit des $\Phi_d(X)$ pour tous les diviseurs d de n.

Théorème II .9. *Wedderburn*
Tout corps fini est commutatif.

Irréductibilité sur Q

Lemme II .10. *Soient k un corps, f et g deux polynômes irréductibles non nuls de $k[X]$, A un anneau contenant k, d'élément unité 1_k et z un élément de A tel que f(z)=g(z)=0. Si f est irréductible dans $k[X]$, alors il divise g.*

Lemme II .11. *(Lemme de Gauss) Soient f et g deux polynômes unitaires de $\mathbb{Q}[X]$ tels que fg soit à coefficients entiers. Alors f et g sont à coefficients entiers.*

Théorème II .12. *Gauss*
Pour tout entier $n > 0$, le polynôme $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$.

III Applications

III .1 Représentation de groupes finis

III .2 Transformée de Fourier discrète

Demazure p.99
Motivations : multiplier des grands nombres entre eux ; échantillonner un signal.

Racines principales de l'unité renforce la notion de racine primitive de l'unité
Soit A un anneau, n un entier > 0 et ω racine n-ième de l'unité dans A. On a équivalence :
(i) Pour tout entier i $0 < i < n$, $1 - w^i$ n'est pas diviseur de zéro dans A
(ii) Pour tout couple d'entiers i et j non congrus modulo n, l'élément $w^i - w^j$ n'est pas diviseur de zéro dans A.
On dit alors que A est une racine principale n-ième de l'unité. En particulier, w^i est différent de 1 pour $0 < i < n$, et w est une racine principale de l'unité.
Inversement, si A est intègre, toute racine primitive de l'unité est principale. Sur $\mathbb{C}$, $\exp(2\pi i/n)$ est racine principale n-ième.

Proposition III .1. *Soit w racine principale n-ième de l'unité dans A.*
a) On a dans A[X] : $X^n - 1_A = \prod_{i=0}^{n-1}(X - w^i)$
b) L'élément $n1_A$ n'est pas diviseur de zéro dans A et on a : $n1_A = \prod_{i=1}^{n-1}(1 - w^i)$

Définition de la TF Soit w une racine principale n-ième de l'unité dans A, et E l'ensemble des applications de $\mathbb{Z}/n\mathbb{Z}$ dans A.
On appelle transformations de Fourier les applications

$$\mathcal{F} : E \to E \qquad \bar{\mathcal{F}} : E \to E$$

définies, pour $j = 0, \dots, n-1$ par :

$$(\mathcal{F}a)_j = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} w^{ij} a_i \qquad (\bar{\mathcal{F}}a)_j = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} w^{-ij} a_i$$

$$(\mathcal{F}a)_j = \sum_{i=0}^{n-1} w^{ij} a_i \qquad (\bar{\mathcal{F}}a)_j = \sum_{i=0}^{n-1} w^{-ij} a_i$$

On a

$$\mathcal{F}(a+b) = \mathcal{F}(a) + \mathcal{F}(b) \qquad \bar{\mathcal{F}}(a+b) = \bar{\mathcal{F}}(a) + \bar{\mathcal{F}}(b)$$

Proposition III .2. *On a $\mathcal{F}(a * b) = \mathcal{F}(a).\mathcal{F}(b)$ et $\bar{\mathcal{F}}(a * b) = \bar{\mathcal{F}}(a).\bar{\mathcal{F}}(b)$*

Proposition III .3. *On a $\mathcal{F}(\bar{\mathcal{F}}a) = na$ et $\bar{\mathcal{F}}(\mathcal{F}a) = na$*

FFT Principe : Supposons n pair, alors n=2n'. $w^{n'}$ est une racine carré principale de l'unité, donc égale à -1_A. De même, $w' = w^2$ est une racine principale n-ième de l'unité dans A. Notons $\mathcal{F}'$ la transformation de Fourier correspondante.

$(\mathcal{F}'b) = \sum_{i=0}^{n'-1} w'^{ij} b_i \qquad j = 0, \dots, n'-1.$

On décompose la famille a en deux parties

$$a_i^{pair} = a_{2i}, \qquad a_i^{impair} = a_{2i+1}, \qquad i = 0, \dots, n'-1$$

Que l'on peut écrire :

$$P_a(X) = P_{a^{pair}}(X^2) + XP_{a^{impair}}(X^2)$$

D'où :

$$(\mathcal{F}a)_j = \sum_{i=O}^{n'-1} w^{2ij} a_{2i} + \sum_{i=0}^{n'-1} \omega^{2i+1} j a_{2i+1}$$

On a de plus :

$$w^{2ij} = w'^{ij} \qquad w^{2i(n'+j)=w'^{ij}}$$
$$w^{(2i+1)j} = w^j w'^{ij} \qquad w^{(2i+1)(n'+j)} = -w^j w'^{ij}$$

Par conséquent :

$$(Fa)_j = (F'a^{pair})_j + w^j (F'a^{impair})_j$$
$$(Fa)_{n'+j} = (F'a^{pair})_j - w^j (F'a^{impair})_j$$

Ainsi, le calcul de la TF à n point Fa se ramène au calcul des deux TF a $n' = n/2$ points Fa^{pair} et Fa^{impair}.

III .3 Tests et critères de primalité

Introduction et critère de Lehmer

Pour savoir si un nombre n est premier ou non, la méthode brute consistant à diviser par tous les nombres inférieurs pour voir s'ils divisent n est particulièrement inefficace. Mais heureusement d'autres critères existent.

Soit n un entier positif. Si n est premier, il existe une racine primitive (n-1)-ième de l'unité dans $\mathbb{Z}/n\mathbb{Z}$. Inversement, s'il existe une racine primitive (n-1)-ième de l'unité a dans $\mathbb{Z}/n\mathbb{Z}$, alors $(\mathbb{Z}/n\mathbb{Z})^*$ est d'ordre n-1, donc $\mathbb{Z}/n\mathbb{Z}$ est un corps est n est premier.

Calculer toutes les puissances de a modulo n prend du temps. Mais en supposant connue à l'avance la décomposition en facteurs premiers de n-1, cela devient plus simple. C'est par exemple le cas lorsque l'on s'interesse aux nombres de Fermat ($n = 2^s + 1$) ou de Mersenne ($n = 2^s - 1$).

Proposition III .4. *Critère de Lehmer*
Soit $n > 1$ un entier impair tel que l'on connaisse tous les facteurs premiers de n-1. Alors
(i) n est premier
(ii) il existe un entier a tel que $a^{n-1} \equiv 1[modn]$ et $a^{(n-1)/q} \not\equiv 1[modn]$ pour tout facteur premier q de n-1.

Preuve III .5. *(i) implique (ii) : prendre pour a une racine primitive (n-1)ième de l'unité.*

Algorithme AKS (Agrawal, Kayal et Saxena, 2002)

Demazure p. 134 (énoncé) et 228 (preuve).

Théorème III .6. *Soit n un entier positif. Soit r un entier > 1 premier à n, choisi de telle façon que l'ordre de la classe de n dans le groupe multiplicatif $(\mathbb{Z}/r\mathbb{Z})^*$ (qui a $\phi(r)$ éléments) soit $> \log(n)^2$. Posons $s = \sqrt{(\phi(r))} log(n)$. Supposons que pour tout entier a avec $1 \leq a \leq s$ on ait :*

$$(X + a)^n = X^n + a \quad [mod(n, X^r - 1)]$$

Alors, ou bien n possède un facteur premier inférieur à s, ou bien n est une puissance d'un nombre premier.

Proposition III .7. *Basé sur le théorème précédent, on propose l'algorithme suivant :*
1/ Éliminer le cas où n est une puissance m^k avec $k \geq 2$.
2/ Essayer les entiers 2,3,... successivement jusqu'à trouver un r qui convienne ; puis calculer s
3/ Éliminer le cas où n a un facteur premier inférieur à s
4/ Tester la congruence pour a=1,...,s et conclure.

III .4 Codes correcteurs, codes cycliques, codes BCH

LEÇON 103

EXEMPLES ET APPLICATIONS DES NOTIONS DE SOUS-GROUPE DISTINGUÉ ET DE GROUPE QUOTIENT.

Référence : Perrin, Ulmer, Spzirglas

Choses à dire durant la présentation Motivations : Notion de groupe distingué et quotient est une notion naturelle. Le cercle R/Z fournit un premier exemple de groupe quotient, qui formalise la notion et les calculs d'angles.

Deux sous groupes particuliers (centre et dérivé) tiennent compte du défaut de commutativité de G.

Utilité : dévissage (Dn), regarder les objets à travers leurs propriétés communes (espaces de Lebesgue en analyse, osef du pp) ; mettre en évidence les propriétés de certains objets, souvent algébriques ou géométriques (groupes d'isométries).

Construction : par exemple via le noyau d'un morphisme

Manipulation : théorèmes d'isomorphisme

I Sous groupes distingués et groupe quotien

I .1 Classes à gauche

Définition 17. *$gH := \{gh, h \in H\}$est appelé classe à gauche de H dans G. On note G/H l'ensemble des classes à guache.*

relation d'équivalence :

$$gR_Hg' \iff g^{-1}g' \in H \iff gH = g'H$$

Les classes d'équivalence, qui forment une partition de G, sont les classes à gauche.

Lemme I .1. *Les classes à gauches associées au groupe H sont en bijection avec H.*

Démonstration.

$$m_g : H \to gH; x \to gx$$

est injective car g inversible, et surjective par définition de gH. Donc la classe gH est en bijection avec H, et ce pour tout g dans G. □

Définition 18. *Si G/H est de cardinal fini, son cardinal est appelé indice de H dans G, noté $[G : H]$*

Théorème I .2. *Lagrange*

$$|G| = |H|.[G : H]$$

Démonstration. G est la réunion disjointe des classes d'équivalence pour la relation R_H, qui sont en nombre fini [G :H]. par le lemme, chacune des classes est de même cardinal $|H|$. □

Corollaire I .3. *Un groupe G de cardinal premier n'a pas de sous groupes différent de G et de $\{1\}$*

I .2 Sous groupes distingués

[Perrin p11, Spzirglas P.230]

Définition 19. *H sous groupe distingué si* $\forall g \in G \forall g \in H \quad ghg^{-1} \in H$.

Ex : G abélien, tout sous groupe est distingué.
Réciproque fausse, par exemple A_4 ou H_8.
Rq : f morphisme de G dans G', son noyau est un sous groupe distingué de G
Si H distingué dans G, le quotient G/H est un groupe et on a un morphisme surjectif de G sur G/H, ed noyau H.

Théorème I .4. *H distingué dans G. Il existe une unique structure de groupe sur le quotient G/H telle que la projection :*

$$\pi_H : G \to G/H; g \to gH$$

soit un morphisme surjectif.

Démonstration. Soient gH et g'H deux éléments du quotient G/H. On définit leur produit par :

$$gH.g'H = gg'H$$

Comme H distingué dans G, on vérifie que la définition ne dépend pas du choix des représentants g et g'. Puis que la classe H est neutre pour cette loi, qui est associative. Enfin, si $g \in G$, la classe gH admet comme inverse $g^{-1}H$. Cette loi de groupe sur G/H est par définition la seule qui fasse de π_H un morphisme de groupe. □

Remarque : π_H est par définition surjectif, de noyau H, et on a :

$$G/Ker\pi_H = Im\pi_H$$

Définition 20. *Suite exacte.*

Théorème I .5. *Factorisation*
$\phi : G \to G'$ *morphisme. ALors* $Ker\phi$ *est un sous groupe distingué de G et* ϕ *induit un isomorphisme :*

$$G/ker\phi \approx Im\phi$$

Proposition I .6. *H d'indice 2 dans G, alors H distingué dans G.*

Démonstration. SOus groupe H de G est strict et le complémentaire de H dans G est non vide. Soit g élément de ce complémentaire. On a la partition :

$$G = H \cup gH$$

On vérifie que G/H est en bijection avec H/G (classes à droite) par l'application $xH \to Hx$. Il existe une unique classe à droite non triviale. Comme $g \notin H$, cette classe est Hg et on a aussi la partition :

$$G = H \cup Hg$$

Donc gH=Hg. Si $g \in H$, la dernière égalité est triviale. □

I .3 Centre, commutateurs et groupe dérivé

Définition 21.

$$Z(G) := [a \in G : \forall g \in G ag = ga]$$

Exemple : Si G abélien, Z(G)=G.
$Z(S_n) = \{1\}$
$Z(H_8) = \{1, -1\}$
Z(GLn)=...

Définition 22. *groupe dérivé de G, D(G) est le groupe engendré par les commutateurs.*

Proposition I .7. *D(G) est distingué dans G.*

Définition 23. $G^{ab} = G/D(G)$. *Plus grand quotient abélien de G.* $D(G)$ *ss groupe de H* $\iff$ *H distingué dans G et G/H abélien*

Exemple : G abélien, on a $D(G) = \{1\}$
$D(S_3) = \{1, \sigma, \sigma^2\}$
$D(H_8) = \{1, -1\}$
$D(A_5) = A_5)$

I .4 Thm d'isomorphimes

[Szpirglas p.231]

II Groupes simples, groupes résolubles

II .1 Simplicité

Définition 24.

Z/pZ simple ssi p premier
Application : G simple, tout morphisme non trivial de G dans X est injectif !

Théorème II .1. *A_n simple pour $n \geq 5$.*

II .2 Groupes résolubles

Définition 25. ...

Théorème II .2. *Lie Kolchin*

III Dévissage de groupes

IV Motivations

G groupe, H ss groupe de G, $\pi : G \to G/H$

Proposition IV .1. *π est un morphisme de groupe ssi la relation d'équivalence : $g_1 \sim g_2 \iff g_1 g_2^{-1} \in H$ est compatible avec la loi de groupe de G.*
Si $g_1 \sim g_2$ et $g_3 \sim g_4$ alors $g_1 g_3 \sim g_2 g_4$.

Définition 26. *H sous groupe distingué si $\forall g \in G \forall g \in H \quad ghg^{-1} \in H$.*

Proposition IV .2. *π est un morphisme ssi H sous groupe distingué.*
Si G est commutatif, H est toujours distingué.

Ex : Z/nZ ; A_3 distingué dans S_3 <(12345)> pas distingué dans S_5.
Tout sous groupe de H_8 est distingué même si H_8 n'est pas abélien. (idemnpour A_4).

V Comment les construit-on ?

Proposition V .1. *H sous groupe distingué de G ssi H noyau d'un morphisme de G dans G'*

Appli : Si G simple, tout morphisme non trivial de G dans G' est injectif.
Ex : A_n est simple pour $n \geq 5$.

Proposition V .2. *Tout sous groupe d'indice 2 est distingué.*

Ex : A_n distingué dans S_n ;
<i> distingué dans H_8.
$Ker(\det_{|O_3}) := SO_3(R)$ distingué das $O_3(R)$.

Proposition V .3. *Int(G) distingué dans Aut(G).*

Ex : Int(S_6)
Int(G)=Id si G commutatif.

Proposition V .4. *G groupe, H sous groupe. Normalisateur de H est le plus grand sous groupe de G dans lequel H est distingué, noté $N_G(H)$.*

Ex :

V .1 Les sous groupes caractéristiques

Définition 27. *H sous groupe caractéristique si stable par automorphismes de G.*

Proposition V .5. *Si H caractéristique, il est distingué.*

Définition 28. *groupe dérivé de G, D(G) est le groupe engendré par les commutateurs.*

Définition 29. $G^{ab} = G/D(G)$. *Plus grand quotient abélien de G.* $D(G)$ *ss groupe de H* $\iff$ *H distingué dans G et G/H abélien*

Appli : G résoluble ssi il existe une suite ...

Théorème V .6. *Lie Kolchin*

VI Manipuler les groupes distingués et quotients : thm d'isomorphismes

VI .1 Premier théorème

Théorème VI .1. *G groupe,* ϕ *morphisme de G dans G'. Alors* $G/Ker\phi \sim Im\phi$
En particulier si G est fini : $|G| = |Ker\phi||Im\phi|$

Ex : $Int(G) \approx G/Z(G)$

VI .2 Deuxième théorème

Théorème VI .2. *G groupe, H et K deux sous groupes de G avec* $K \subset N_G(H)$. *Alors HK=KH est un sous groupe de G, et H distingué dans HK distingué dans G,* $K \cap H$ *distingué dans G et :* $KH/H \approx K/K \cap H$

Appli : Sylow

VI .3 Troisième théorème

Théorème VI .3. *G groupe, K et H deux sous groupes distingués de G tels que* $H \subset K$. *Alors :*

$$G/H/K/H \approx G/K$$

VII A quoi servent-ils ?

Passer au quotient permet de rendre les choses intrinsèques en ne considérant que les objets au travers de leurs propriétés communes.
Ex : Les espaces de Lebesgue en analyse. Quotienté par la relation d'équivalence " égalité p.p ".
Rendre la structure d'un groupe plus explicite en la décomposant. Ex : D_n.
Modéliser plus facilement certaines propriétés ou étendre un groupe. Ex : PSLn(R)
Mettre en évidence les propriétés de certains objets, souvent algébriques ou géométriques. (groupes d'isométries).

LEÇON 104

GROUPES FINIS. EXEMPLES ET APPLICATIONS.

Référence : Calais, Combes, Perrin, Szpirglas.
Dvt : S4 isométries du cube
Cardinal cône nilpotent
Automorphismes Sn

I Généralités

I .1 Définitions

[Calais, chap 1]
G est dit fini s'il n'a qu'un nombre fini d'éléments. Le cardinal de G est appellé l'ordre du groupe, noté $|G|$.
Exemple : Z/nZ d'ordre n, S_n d'ordre n !.

Définition 30. *L'ordre d'un élément est l'ordre du groupe engendré par cet élément. Peut être fini ou infini.*

Exemple : le neutre est d'ordre 1. Dans S_3 les transpo sont d'ordre 3, les 3-cycles d'ordre 3.

I .2 Lagrange et indice

[Combes chap 1]

Définition 31. *Le carinal commun aux ensemble G/H et H G s'appelle l'indice de H dans G, noté* $[G : H]$. *Si H est réduit au neutre, alors* $[G : H] = |G|$.

Théorème I .1. *de Lagrange*
G groupe fini, K et H deux sous groupes de G tels que $K \subset H$. *On a*

$$[G : K] = [G : H][H : K]$$

Corollaire I .2. *G fini. L'ordre o(a) de tout élément a de G divise* $|G|$.

Applications : U_n racine nième de l'unité ; alors $U_n \cap U_m = U_d$ où d=pgcd(m,n).

I .3 Actions de groupes et conséquences

Définition 32. *action de G sur X*

Définition 33. *stabilisateur, orbite, fixateur*

Proposition I .3. *bijection entre Orb(x) et G(x)/Stab(x)*

Action de G sur lui même par translation à gauche. Csq : Cayley
H sous groupe de G, alors G agit sur G/H par translation.

Théorème I .4. *Equations aux classes*

Théorème I .5. *Formule de Burnside*

II Groupes finis abéliens

II .1 Groupes cycliques

Proposition II .1. *Un groupe cyclique est abélien. SI G cyclique d'ordre n, alors G isomorphe à Z/nZ.*

Ex : U_n isomorphe à Z/nZ

Proposition II .2. *Un groupe d'ordre p premier est cyclique.*

Proposition II .3. *Perrin p.24 Générateurs de (Z/nZ,+)*

Proposition II .4. *Aut(Z/nZ) isomorphe à* $(Z/nZ)^*$

Théorème II .5. *Théorème Chinois (perrin p.25)*

Application : formule pour l'indicatrice d'Euler

II .2 Décomposition des groupes finis abéliens

Théorème II .6. *Théorème de structure*

III Autres groupes finis

III .1 Le groupe symétrique

[Szp] Motivation : th de Cayley.
Décomposition en cycle à support disjoints, générateurs de S_n, morphisme signature, def de A_n

Proposition III .1. A_n *simple pour* $n \geq 5$.

Csq : $D(S_n) = A_n$

Proposition III .2. *Un sous groupe d'ordre n de* S_n *est isomorphe à* S_{n-1}

III .2 Le groupe diédral

[Caplais chap3]

Définition 34. D_n *:=groupe des isométries du plan conservant un polygône régulier à n côté.*

Proposition III .3. $|D_n| = 2n$

Proposition III .4. *Générateurs de* D_n *: une rotation + une symétrie.*

Proposition III .5. D_n *non abélien pour* $n > 2$.

III .3 Le groupe des quaternions

Proposition III .6. $Z(H_8) = \{+/-1\}$
Les sous groupes de H_8 *sont ...*

IV Représentations linéaires de groupes finis

LEÇON 105

GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI. APPLICATIONS.

Référence : Perrin, Szpirglas, Gourdon, Ramis-Deschamps-Odoux, Ulmer (Théorie des groupes)
Dvt : Automorphismes de S_n et isométries de S_4

I Groupe des permutations

I .1 Définition

Définition 35. *X un ensemble, on note S(X) le groupe des bijections de X muni de la composition. On appelle permutation un élément de S(X).*

Proposition I .1. *Si X est en bijection avec Y, alors* $S(X) \approx S(Y)$

Définition 36. *On note* $S_n = S(\{1, \dots, n\})$ *le groupe symétrique à n éléments.*

Proposition I .2. *On a* $|S_n| = n!$

I .2 Propriété et structure de S_n : orbites et cycles

[ULM]

Définition 37. *Soit* $\sigma \in S_n$*. Le support de* σ *est l'ensemble* $Supp(\sigma) := \{i \in \mathbb{N}^* \sigma(i) \neq i\}$

Proposition I .3. *Les permutations à support disjoints commutent*

Définition 38. *cycles de longueur l ; transpositions*

Théorème I .4. *Décomposition en produits de cycles à support disjoint.*

Proposition I .5. *Si* $n \geq 3$*, on a* $Z(S_n) = \{id\}$

Définition 39. *Orbite de k sous* $\sigma \in S_n$

Définition 40. *p cycle ; 2-cycle = transpo.*

I .3 Générateurs de S_n

Théorème I .6. *Toute permutation* $\sigma \in S_n$ *s'écrit comme produit de cycles à supports disjoints, de façon unique à permutation près des cycles.*

Proposition I .7. *Soit* $\sigma \in S_n$*. Son ordre est le ppcm des ordres des cycles rentrant dans la décomposition.*

Proposition I .8. *Les ensembles suivants engendrent* S_n *:*
Les transpo (i,j) $1 \leq i, j \leq n$
Les transpo (1,i)
Les transpo (i-1,i)
La transpo (1,2) et le cycle $(1, \dots, n)$.

Formules utiles :
$(i_1, i_2, \dots, i_l) = (i_1, i_2)(i_2, i_3) \dots (i_{l-1}, i_l)$
(i,j)=(1,i)(1,j)(1,i)
Exo : $\sigma = (3,1,5,2) = (3,2)(3,5)(3,1) = (1,3)(1,2)(1,5)$

II Structure algébrique

II .1 Le groupe alterné

Théorème II .1. *Il existe un unique morphisme de groupe non trivial de S_n dans $\mathbb{C}^*$. On l'appelle morphisme signature, à valeur dans $\{-1, 1\}$, noté ϵ. Il prend la valeur -1 sur toutes les transpositions.*

Rq : pour calculer la signature de $\sigma \in S_n$, on décompose σ en cycle et on remarque $\epsilon(i_1 \dots_i r) = (-1)^{r-1}$

Définition 41. *On appelle groupe alterné, noté AZ_n, le noyau de la signature dans S_n. C'est un sous groupe distingué de S_n, d'indice 2.*

Rq : A_n distingué dans S_n, en tant que noyau du morphisme signature, ou en tant que sous groupe d'indice 2.

Proposition II .2. *Pour $n \geq 3$, les 3-cycles sont dans A_n et l'engendrent. Si $n \geq 5$, ils sont de plus conjugués dans A_n.*

Démonstration. □

Proposition II .3. *A_n est le seul sous groupe d'indice 2 dans S_n.*

Démonstration. Idée : □

III Structure de A_n et S_n

Théorème III .1. *Si $n \neq 4$, A_n est simple.*

Corollaire III .2. *Si $n \geq 5$, les groupes dérivés de A_n et S_n sont :*

$$D(A_n) = A_n \quad D(S_n) = A_n$$

Rq : Dans A_4, on a $D(1_4) = V_4$!

Corollaire III .3. *Si $n \neq 4$, les seuls sous groupes distingués de S_n sont $\{Id\}$, A_n et S_n.*

Corollaire III .4. *Tout sous groupe d'indice n de S_n est isomorphe à S_{n-1}.*

Théorème III .5. *Pour $n \neq 6$, tout automorphisme de S_n est un automorphisme intérieur. Si de plus $n \geq 3$:*

$$Aut(S_n) \equiv Int(S_n) \equiv S_n$$

Corollaire III .6. *Soit ϕ un automorphisme de S_n qui transforme les transpositions en transpositions. Alors ϕ est un automorphisme intérieur.*

Proposition III .7. *On a $Aut(S_6) \neq Int(S_6)$*

IV Application

IV .1 Action de groupes, théorème de Cayley

Théorème IV .1. *Cayley*

IV .2 Réalisation géométrique de S_n et A_n

IV .3 Formes multilinéaires alternées

[Gou p.134]

Définition 42. *K corps, E Kev,*

Proposition IV .2. *ϕ alternée ssi $\forall \sigma \in S_n \forall (x_1, \dots, x_n) \in E^n \quad \phi(x - \sigma(1), \dots, x_{\sigma(n)}) = \epsilon(\sigma)\phi(x_1, \dots, x_n)$*

Théorème IV .3. *L'ensemble des formes n linéaires alternées sur E est un Kev de dimension 1. De plus, si B est une base de E, on a :*

$$\phi(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \epsilon(\sigma \prod_i x_{\sigma(i)})$$

Définition 43. *$\det_B$ est l'unique forme n linéaire alternée telle que $det_B(B) = 1$*

IV .4 Polynômes symétriques

[RDO p.200] A anneau commutatif

Proposition IV .4. *L'application $S_n \times A[X_1, \dots, X_n] \to A[X_1, \dots, X_n]; (\sigma, P) \to \sigma(P)$ où est une action de groupe*

Définition 44. $P \in A[X_1, \dots, X_n]$ *est dit symétrique si* $\forall \sigma \in S_n, \sigma(P) = P$
est dite alternée si $\forall \sigma \in A_n, \sigma(P) = P$. *(osef ?)*

Ex : $\prod_{1 \leq i < j \leq n}(X_j - X_i)$ est alterné mais pas symétrique.

Définition 45. *Les n polynômes* $\Sigma_p := \sum_{1 \leq i_1 < \dots < i_p \leq n} X_{i_1} \dots X_{i_p}$ *sont symétriques et appelés polynômes symétriques élémentaires.*

Proposition IV .5. $P := \prod_{i=1}^{n}(Y - X_i) \in A[X_1, \dots, X_n]$. *Alors on a* $P = Y^n + \sum_{p=1}^{n}(-1)^n \Sigma_p Y^{n-p}$

Rq : On retrouve les relations coeff racines.

Définition 46. *On appelle poids du monôme* $X_1^{l_1} \dots X_n^{l_n}$ *l'entier* $\sum_{k=1}^{n}$??. *Le poids d'un polynôme est le maximum des poids de ses monômes.*

Soit P polynôme symétrique. P a le même degré paetiel par rapport à chaque indéterminée, que l'on appelle alors l'ordre de P, noté w(P).

Théorème IV .6. *Théorème de structure des polynômes symétriques*

Soit P un polynôme symétrique de $A[X_1, \dots, X_n]$ *de degré p et d'ordre w. Il existe un unique polynôme Q de* $A[X_1, \dots, X_n]$ *tel que* $P(X_1, \dots, X_n) = Q(\Sigma_1, \dots, \Sigma_n)$, *Q est de poids p et degré w.*

IV .5 Groupes d'isométries de polyèdre

[Spz p.422-424]

LEÇON 106

GROUPE LINÉAIRE D'UN ESPACE VECTORIEL DE DIMENSION FINIE E, SOUS-GROUPES DE GL(E). APPLICATIONS.

Références Perrin, Szpirglas, H2G2, Serre

Développements

— Lie-Kolchin

— O(p,q)

— Molien

Rapport jury (2015) Cette leçon est souvent présentée comme un catalogue de résultats épars et zoologiques sur GL(E). Il serait bien que les candidats unifient la présentation de la leçon en faisant correspondre les sous-groupes du groupe linéaire avec les stabilisateurs de certaines actions naturelles (sur des formes quadratiques, symplectiques, sur des drapeaux, sur une décomposition en somme directe, etc.).

À quoi peuvent servir des générateurs du groupe GL(E) ? Qu'apporte la topologie dans cette leçon ? Il est préférable de se poser ces questions avant de les découvrir le jour de l'oral. Certains candidats affirment que $GL_n(K)$ est dense (et ouvert) dans $M_n(K)$. Il est judicieux de préciser les hypothèses nécessaires sur le corps K ainsi que la topologie sur $M_n(K)$.

La présentation du pivot de Gauss et de ses applications se justifient pleinement.

Il faut aussi savoir réaliser S_n dans $GL_n(K)$ et faire le lien entre signature et déterminant. Dans le même ordre d'idée, la théorie des représentations permet d'illustrer, dans les leçons plus robustes, l'omnipotence de $GL_n(C)$ et de son sous-groupe unitaire.

Motivation / speech à l'oral

I Le groupe linéaire

[Perrin, Szp pour compléter]

I .1 Définitions

Définition 47. *GL(E) ; isomorphisme (non canonique, besoin de fixer une base) avec $GL_n(K)$.*

Définition 48. *déterminant.*
Ker det = SL(E).

I .2 Générateurs

Définition 49. *transvections, dilatations*

I .3 Centre, groupe dérivé

I .4 Cas des corps finis : cardinaux, isomorphismes

II Actions du groupe linéaire

[H2G2]

II .1 Par équivalence

Énoncer le théorème du rang.

II .2 Par conjuguaison

II .3 Par congruence

Introduire la relation de congruence et son lien avec la réduction des f.q. Enoncer Sylvester dans R (éventuellement dans C et Fq), pour introduire le Stabilisateur de $I_{(p,q)}$, cad O(p,q). Recaser avec joie ledit développement. (pas mentionner les résultats de compacité ou connexité de O(p,q) ici, puisqu'on en parle qu'après dans la leçon).

II .4 Action sur les couples de sev en somme directe

Application : cardinal du cône nilpotent. (en mettant lemme de Fitting en remarque).

II .5 Action sur les polynômes

G sous groupe de $GL_n(C)$. Recaser Molien.

III Topologie

III .1 Densité

On s'amuse avec la matrice $diag(\epsilon, \epsilon^2, \dots, \epsilon^n)$.

Donner pas mal d'exemple, le plus classique étant la densité de $D_n(C)$ dans $M_n(C)$, avec pour conséquence quasi immédiate Cayley Hamitlon. On donne le contre exemple dans R, avec sous groupe des rotations 2x2. Enfin matrice trianguarisables denses. Le plus frappant étant surement :

Théorème III .1. *Pour tout $\epsilon > 0$, il existe $||.||$ une norme matricielle telle que :*

$$\rho(B) \leq ||B|| + \epsilon$$

Autrement dit, $\rho(B) = \inf ||B||$, l'inf étant pris sur les normes matricielles.

Application : définition du logarithme matriciel pour toutes les matrices ayant un rayon spectral plus petit strictement que 1.

Remarque : on a toujours $||B|| \leq \rho(B)$

Démonstration. cf Serre. □

III .2 Compacité

Proposition III .2. *$O(n)$ est compact. Corollaire : O(p,q) l'est ssi pq=0.*

Théorème III .3. *Décomposition polaire*

Appli : rayon spectral égal à norme 2 (faire pour matrices inversible puis densité de GLn(C) dans Mn(C).

Proposition III .4. *exp : $S_n \to S_n^{++}$ homéomorphisme.*

Démonstration. Utilise la décomposition polaire. Pas complètement dans le cadre de la leçon, mais on utilise ce résultat dans la suite. □

III .3 Connexité

Proposition III .5. *$GL_n(C)$ est connexe.*
$GL_n(R)$ a deux composantes connexes : GL_n^+ et GL_n^-.

Proposition III .6. *O_n a deux composantes connexes : SO_n et l'autre.*
U_n est connexe.

Démonstration. Pour O_n : union disjointe de SO_n et l'autre. SO_n connexe par arc car on met sous forme normale (diagonale de 1 et de rotations, éventuellement d'angle π (ie on regroupe les -1 2 par 2 ; il y en a un nombre pair car le det vaut 1)). Puis on fait un chemin reliant cette matrice à l'identité.
Puis $O_n^- = MSO_n$ pour n'importe quelle matrice M dans O_n^-.
Pour U_n : on a par décomposition polaire $GL_n(C)$ homéomorphe à $U_n \times H_n^{++}$ et $GL_n(C)$ est connexe. □

Proposition III .7. *O(p,q) a 2 composantes connexes si pq=0, 4 sinon.*
U(p,q) est connexe.

Démonstration. Voir Serre.
Vient du fait que O(p) et O(q) ont 2 composantes connexes sauf dans les cas dégénérés pq=0.
U(p,q) est connexe car U(p) et U(q) le sont toujours.

□

LEÇON 107

REPRÉSENTATIONS ET CARACTÈRES D'UN GROUPE FINI SUR UN C-ESPACE VECTORIEL.

Référence : Serre, RWM

I Représentations linéaires

[Serre]

I .1 Définition, pemiers exemples

G groupe fini, de neutre 1, V un $\mathbb{C}$ espace vectoriel de dimension finie.

Définition 50. *Une représentation linéaire de G dans V est un morphisme ρ de G dans GL(V).*
On appelle degré de la représentation la dimension de V.

Exemple : représentation degré 1 ; G étant fini, $\rho(s)$ est racine de l'unité.
représentation régulière (degré = $|G|$).
représentation par permutation : G agit sur X : pour tout s de G, on a $x \to sx$ est permutation de X, avec

$$1x = x \quad s(tx) = (st)x \; s, t \in G, x \in X$$

Définition 51. *On dit que ρ et ρ' sont deux représentations semblables s'il existe un isomorphisme linéaire $\tau : V \to V'$ tq :*

$$\tau \circ \rho(s) = \rho'(s) \circ \tau \quad \forall s \in G$$

Si R_s et R'_s sont les matrices représentant ρ et ρ', la condition s'écrit aussi : $R'_s = TR_sT^{-1}$ avec T inversible.
On identifie deux telles représentations ; elles ont le même degré.

I .2 Sous représentations

Définition 52. *Soit W sev de V, invariant par G, cad $x \in W \Rightarrow \rho(s)(x) \in W \; \forall s \in G$.*
La restriction de ρ^W à W est un isomorphisme de W dans lui même : on dit que W est une sous représentation de V.

Théorème I .1. *ρ représentation de G dans V et W sev de V stable par G. Alors, il existe un supplémentaire W^0 de W dans V qui est stable par G.*

Démonstration. Par moyennisation. □

I .3 Représentations irréductibles

Définition 53. *ρ est dite irréductible ou simple si V n'est pas réduit à 0 et si aucun sev de V n'est stable par G (à part 0 et V).*

Théorème I .2. *(Maschke)*
Toute représentation est somme directe de représentations irréductibles.

Démonstration. Par récurrence sur la dim(V), en utilisant le thm précédent. □

II Théorie des caractères

Définition 54.

$$\forall s \in G \quad \chi_\rho(s) := Tr(\rho_s)$$

est appelé le caractère de la représentation ρ.

Proposition II .1. *Un caractère est constant sur les classes de conjugaison : c'est un exemple particulier de fonction centrale. Par ailleurs, $\chi(1) = n$ où n est le degré de la représentation associée.*

Lemme II .2. *Lemme de Schur*

Soit $\rho^1 : G \to GL(V_1)$ et $\rho^2 : G \to GL(V_2)$ deux représentations irréductibles de G, et f linéaire de V_1 dans V_2 telle que $\rho^2(s) \circ f = f \circ \rho^1(s)$ $\forall s \in G$. Alors :

1/ Si ρ^1 et ρ^2 ne sont pas isomorphes, on a f=0.

2/ Si $V_1 = V_2, \rho^1 = \rho^2$, f est une homothétie (ie un multiple scalaire de 1).

Théorème II .3. *Si χ est le caractère d'une représentation irréductible, on a $(\chi|\chi) = 1$.*

Si χ et χ' sont des caractères de deux représentations irréductibles non isomorphes, on a $(\chi|\chi') = 0$.

Théorème II .4. *Soit V représentation de G, de caractère ϕ, et supposons*

$$V = W_1 \oplus \cdots \oplus W_k$$

Alors si W est une représentation irréductible de caractère χ, le nombre des W_i isomorphes à W est égal au produit scalaire $(\phi|\chi) =< \phi, \chi >$

Corollaire II .5. *Le nombre des W_i isomorphes à W ne dépend pas de la décomposition choisie.*

Corollaire II .6. *Deux représentations de même caractère sont isomorphes.*

Le critère suivant d'irréductibilité est très commode en pratique :

Théorème II .7. *Si ϕ est le caractère d'une représentation V, $(\phi|\phi)$ est un entier positif, et on a $(\phi|\phi) = 1$ si et seulement si V est irréductible.*

LEÇON 108

EXEMPLES DE PARTIES GÉNÉRATRICES D'UN GROUPE. APPLICATIONS.

Référence : Szpirglas, Perrin
Motivations
Applications - Connaître les générateurs d'un groupe permet de mieux connaitre sa structure -Prouver la surjectivité de morphismes -Montrer qu'un groupe est simple (An, SO(3)) -On peut vérifier une propriété seulement sur les générateurs et ça se transmet au groupe entier

Définitions et notations

G groupe, A partie de A, $< A >$ intersection de tous les sous groupes contenant A.
On dit que A engendre G si $< A >$=G

I Groupes abéliens de type fini

I .1 Groupe cycliques

Définition 55.

Proposition I .1.

II Groupes non abéliens finis

II .1 Groupes diédraux

II .2 Groupe symétrique

III Groupe linéaire

[Szpirglas]

III .1 Gl(E) et SL(E)

Définition 56. *Groupe linéaire = ensemble des K automorphismes de E, noté GL(E).*
Le noyau du déterminant est appelé groupe spécial linéaire, noté SL(e).

Définition 57. *Dilatation d'hyperplan H, de droite D de rapport λ = élément u de GLn(K) vérifiant H=Ker(u-Id) et D=Ker(u-λ Id), avec $\lambda \neq 1$.*

Réflexion = dilatation de rapport -1.

Proposition III .1. *Deux dilatations sont conjuguées ssi elles ont même rapport.*

Démonstration. Si elles sont conjuguées, elles ont même det donc même rapport. Réciproquement, si elles ont même rapport, elles sont représentées par la même matrice donc sont conjuguées. □

Définition 58. *Transvection = élément de SLn(K) différent de l'identité fixant un hyperplan.*

Théorème III .2. *SLn(K) est engendré par les transvections.*
GLn(K) est engendré par les dilatations et les transvections.

III .2 Groupe orthogonal

Définition 59. *O(q)*

Proposition III .3. $u \in O(q) \Rightarrow det(u) = +/-1$.

Définition 60. *SO(q)*

Définition 61. *symétries : éléments de GL(E) (pas identité) tq* $u^2 = Id$.
symétries orthogonales = symétrie appartenant à O(q).

Théorème III .4. *Cartan*
O(q) est engendré par les réflexions orthogonales.

Théorème III .5. *Cartan-Dieudonné*
Tout élément de O(q) est produit d'au plus n réflexions orthogonales.

Définition 62. *Renversement orthogonal = renversement appartenant à O(q). C'est donc une sym ortho tq* $dim(E^-) = 2$.

Corollaire III .6. $n \geq 3$. *Alors tout élément de So(q) s'écrit comme produit d'au plus n renversements.*

LEÇON 110

CARACTÈRES D'UN GROUPE ABÉLIEN FINI ET TRANSFORMÉE DE FOURIER DISCRÈTE. APPLICATIONS.

Références Colmez, Peyré, Demazure (pour FFT)

Développements

— FFT (Peyré, Demazure)

— Structure groupes abéliens finis (Colmez, Artin pour unicité ?)

Rapport jury (2015) Il s'agit d'une nouvelle leçon qui n'a pas encore trouvé l'affection des candidats.

Pourtant, le sujet et abordable, par exemple : le théorème de structure des groupes abéliens finis, qui a bien entendu une place de choix dans cette leçon. On pourra en profiter pour montrer l'utilisation de la dualité dans ce contexte. Comme application, la cyclicité du groupe multiplicatif d'un corps fini est tout à fait adaptée. D'ailleurs, des exemples de caractères, additifs, ou multiplicatifs dans le cadre des corps finis, sont les bienvenus. Pour les candidats chevronnés, les sommes de Gauss permettent de constater toute l'efficacité de ces objets.

L'algèbre du groupe est un objet intéressant, surtout sur le corps des complexes, où il peut être muni d'une forme hermitienne. On peut l'introduire comme une algèbre de fonctions, munie d'un produit de convolution, mais il est aussi agréable de la voir comme une algèbre qui prolonge la multiplication du groupe.

La transformée de Fourier discrète pourra être vue comme son analogue analytique, avec ses formules d'inversion, sa formule de Plancherel, mais dans une version affranchie des problèmes de convergence, incontournables en analyse de Fourier.

On pourra y introduire la transformée de Fourier rapide sur un groupe abélien d'ordre 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.

Motivation / speech à l'oral

I Caractères d'un groupe abélien fini ; structure du groupe dual

But : étude algébrique des fonctions $f : G \to \mathbb{C}$ où G groupe abélien fini. On peut se donner tous les f(g) où g parcourt G, mais on n'exploite alors pas la structure de groupe de G.

I .1 Dual d'un groupe fini

Définition 63. *Caractère : morphisme de G dans $(C^*, \times)$. On note $\hat{G}$ l'ensemble des caractères de G, appelé groupe dual.*

Définition 64. *multiplication des caractères : $\chi_1\chi_2 : x \mapsto \chi_1(x)\chi_2(x)$ Donc $\hat{G}$ muni de cette loi est un groupe.*

Proposition I .1. *$|G| = n$. Alors $\chi \in \hat{G}$ est à valeur dans $\mathbb{U}_n$.*
En particulier, $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$
$\hat{G}$ est un groupe fini.

Définition 65. *Espace des fonctions de G dans $\mathbb{C}$: $\mathbb{C}[G]$. C'est un ev que l'on muni du produit hermitien :*

$$\forall (f,h) \in \mathbb{C}[G], \quad < f, g >:= \frac{1}{|G|} \sum_{g \in G} f(g)\overline{h(g)}$$

Norme : $||f||_2^2 =< f, f >$.

Proposition I .2. *Invariance par translation du produit scalaire (ici translation c'est multiplication :* $x \mapsto f(xy)$ *translation de y).*

Proposition I .3. $(\delta_g)_{g\in G}$ *donne une base de* $\mathbb{C}[G]$. *En particulier,* $C[G]$ *est un ev de dimension n.*

Rq : On dit que G se plonge de façon canonique dans $C[G]$ par $g \mapsto \delta_g$.

Démonstration. Orthonormées et fonctions non nulles donc libre.
Génératrice car : $f = \sum_{g\in G} f(g)\delta_g$ □

Problème : cette base n'est pas pratique pour les calculs (combinaison linéaire, ok, produit, produit de convolution moins ok).

On va montrer que la famille des caractères, formées d'éléments de $\hat{G}$ est une base agréable de $C[G]$ (simple à utiliser et calculs facilités).

I .2 Orthogonalité des caractères

Cas d'un groupe cyclique

Proposition I .4. $G =< g >$ *groupe cyclique d'ordre n, w racine primitive n ieme de l'unité. Les éléments de* $\hat{G}$ *sont de la forme :*

$$\chi_j : g^k \in G \mapsto (w^j)^k \in \mathbb{C}^*$$

En particulier G et $\hat{G}$ *sont isomorphes (pas canonique).*

Proposition I .5. *G cyclique.* $\hat{G}$ *forme une base orthonormale de C[G] :*

$$< \chi_p, \chi_q >= \delta_{pq}$$

Cas général

Lemme I .6.

$$\chi \in \hat{G} \quad \sum_{g\in G} \chi(g) = |G| si \chi = 1, 0 \; sinon$$

Démonstration. Si $\chi = 1$ c'est direct. Sinon, soit t dans G tel que $\chi(t) \neq 0$. On a alors :

$$\chi(t)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(tg) = \sum_{h\in G} chi(h)$$

Donc :

$$(\chi(t)-1)\sum_g \chi(g) = 0 \quad \sum_g \chi(t) = 0$$

□

Remarque : il existe bien un caractère non trivial. Dans Lidl et Niederreiter, c'est fait via le thm de prolongement des caractères. On prend $h = g_1 g_2^{-1} \neq 1_G$ et $H =< h >$; H cyclique donc on a un caractère non trivial sur H, que l'on peut prolonger à G.

Corollaire I .7.

$$|G| = |\hat{G}|$$

Démonstration. $|\hat{G}| = \sum_{g\in G}\sum_{\chi\in\hat{G}}\chi(g) = \sum \chi \in \hat{G}\sum_{g\in G}\chi(g) = |G|$ □

Proposition I .8.

$$\forall \chi_1 \neq \chi_2 \in \hat{G} \quad < \chi_1, \chi_2 >= 0$$

Démonstration. $\chi := \chi_1\overline{\chi_2} = \chi_1\chi_2^{-1}$ (car χ_i sont de module 1).

$$< \chi_1, \chi_2 >= \frac{1}{|G|}\sum_g \chi(g)$$

On conclut avec le lemme précédent. □

Corollaire I .9. $\hat{G}$ *est une base orthonormale de C[G].*

Démonstration. $\hat{G}$ libre en tant que famille orthonormale. G et $\hat{G}$ ont même cardinal, qui est la dimension de $C[G]$ en tant que C-ev : c'est une base. □

Proposition I .10.

$$\sum_{\chi\in\hat{G}} \chi(g)\chi(\hat{h}) = |G|\delta_{gh}$$

Démonstration. Lemme d'avant à $\hat{G}$ (groupe fini abélien). □

I .3 Structure du groupe dual ; groupe bidual ; lien avec la structure des groupes abéliens

(titre à raccourcir le jour de l'oral)

Définition 66. *Bidual.*

Proposition I .11. *Isomorphisme de groupe (canonique) entre G et son bidual.*

Faire le lien en algèbre linéaire (en dimension finie) : E et E^* isomorphe, mais on choisit au préalable une base. Par contre, E isomorphe à son bidual canoniquement.

Tout s'écroule en dimension infinie (que ce soit ev ou groupe abélien : dual du tore $\mathbb{R}/2\pi\mathbb{Z}$ est isomorphe à $\mathbb{Z}$).

Définition 67. *Exposant d'un groupe (ppcm des ordres). Cas particulier groupe abélien : exposant est atteint, c'est le maximum des ordres. Contre exemple dans S_3 d'ordre 6, sans éléments d'ordre 6.*

Lemme I .12. *G et $\hat{G}$ ont même exposant.*

Théorème I .13. *Théorème de structure des groupes abéliens finis.*

II Structure d'algèbre sur le groupe dual ; transformée de Fourier

II .1 Transformée de Fourier

Définition 68. *Coeff de Fourier de $f \in \mathbb{C}[G]$:*

$$\forall\chi\in\hat{G} \quad c_f(\chi) :=< f,\chi >$$

$$c : f \in C[G] \mapsto c_f \in C[\hat{G}]$$

Définition 69. *Transformée de Fourier*

$$\mathcal{F} : f \in \mathbb{C}[G] \mapsto \hat{f} \in C[\hat{G}]$$

où

$$\forall\chi\in\hat{G} \quad \hat{f}(\chi) := |G|c_f(\overline{\chi}) = \sum_x f(x)\chi(x)$$

Proposition II .1. *Formule d'inversion de Fourier. $f \in C[G]$:*

$$f = \sum_{\chi\in\hat{G}} c_f(\chi)\chi = \frac{1}{|G|}\sum_{\chi\in\hat{G}} \hat{f}(\chi)\chi^{-1}$$

Démonstration. Car $\hat{G}$ base orthonormale de C[G], donc on décompose f dans cette base. □

Proposition II .2. *c et $\mathcal{F}$ sont des isomorphismes d'espaces vectoriels de C[G] dans $C[\hat{G}]$.*

Démonstration. Injectif : via formule d'inversion si $c_f = 0$ alors f=0.

G et $\hat{G}$ ont même cardinal, donc les ev C[G] et $C[\hat{G}]$ ont même dimension donc surjectif. □

Proposition II .3. *Formule de Plancherel*

Démonstration. Décomposer f et g par formule d'inversion puis :

$$\sum_s f(s)\overline{g(s)} = |G| < f,g >= |G| \sum_{\chi_1,\chi_2\in\hat{G}} c_f(\chi_1)\overline{c_g(\chi_2)} < \chi_1,\chi_2 >$$

Conclure par orthogonalité des caractères. □

II .2 Produit de convolution

Définition 70. $f_1, f_2 \in C[G]$

$$f_1 * f_2(g) := \sum_{h,k \in G : hk=g} f_1(h) f_2(k) = \sum h \in G f_1(h) f_2(h^{-1}g)$$

Proposition II .4. $\chi \in \hat{G}$.

$$\mathcal{F}_\chi : f \in C[G] \to \hat{f}(\chi) \in \mathbb{C}$$

est un morphisme d'algèbre.

Remarque : c'est l'unique façon d'étendre le morphisme de groupe χ en morphisme d'algèbre.

Démonstration. Unicité : osef.

$$\forall g \in G \quad \mathcal{F}_\chi(\delta_g) = \sum_x \delta_g(x)\chi(x) = \chi(g)$$

□

Théorème II .5. *Convolution et TF. f,g* $\in C[G]$*, on a :*

$$\hat{f * g} = \hat{f}\hat{g}$$

$$c_{f*g} = |G| c_f c_g$$

Donc $\mathcal{F}$ *est un isomorphisme d'algèbre de* $(C[G], *)$ *dans* $(C[\hat{G}], .)$.

II .3

III Applications

III .1 FFT

On recase gentiment le développement

III .2 Caractères sur un corps finis

Sur $(\mathbb{F}_q^*, \times)$ F_q cyclique donc c'est assez easy. (modulo il faut pouvoir récupérer un générateur de F_q....).

Sur $(\mathbb{F}_q, +)$

Définition 71. *Trace de* F_q *sur* F_p *avec* $q = p^n$ *:*

$$Tr(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$$

$$\chi_1(c) = \exp(i2\pi Tr(c)/p) \quad \forall c \in \mathbb{F}_q$$

Théorème III .1. $b \in F_q$*, la fonction* $\chi_b(c) = \chi_1(bc)$ *est un caractère additif de* F_q*, et tous les caractères additifs de* F_q *sont obtenus de cette façon.*

Démonstration. Montrer que c'est bien un caractère.
Puis $\frac{\chi_a(c)}{\chi_b(c)} = \frac{\chi_1(ac)}{\chi_1(bc)} = \chi_1((a-b)c) \neq 1$ si $a \neq b$. □

III .3 Somme de Gauss

Un peu dur mais stylé.

III .4 Formule sommatoire de Poisson

Vraiment stylé pck on fait bien le lien avec TF en analyse et la formule du même nom. Mais un peu hard.

IV Vrac

IV .1 Rappels : représentations et caractères

Définition 72. *représentation*

Définition 73. *Caractère χ_V de V définit par $\chi_V(g) = Tr(\rho_V(g))$.*

Proposition IV .1. *χ_V est une fonction centrale (constante sur les classes de conjugaisons).*

Proposition IV .2. *G fini, les valeurs propres de $\rho_V(g)$ sont des racines de l'unité. Comme les vp de $\rho_V(g^{-1} = \rho_V(g)^{-1})$ sont les inverses de celles de $\rho_V(g)$, et trace est la somme des vp, on en déduis que $\chi_V(d^{-1}) = \overline{\chi_V(g)}$.*

Caractères linéaires Ce sont les morphismes de GL(V) dans $\mathbb{C}^*$.

Théorème IV .3. *G abélien. Toute représentation irréductible de g est de dimension 1.*

Corollaire IV .4. *G abélien. toute fonction de G dans $\mathbb{C}$ est CL de caractères linéaires.*

IV .2 Cas particulier dans un groupe abélien

G groupe abélien fini.

Définition 74. *Groupe dual $\hat{G}$ des caractères linéaires de G.*

Proposition IV .5. *$\hat{G}$ est un groupe pour la multiplication des caractères linéaires : $\xi_1\xi_2(x) := \xi_1(x)\xi_2(x)$.*

Proposition IV .6. *$\hat{G} \subset \mathbb{U}_n$ où $n = |G|$.*

Rq : $\hat{G}$ est fini.

Définition 75. *$\mathbb{C}[G]$ l'ensemble des fonctions de G dans C : espace vectoriel, avec produit hermitien*

$$< f, g >= \frac{1}{|G|} \sum_{x \in G} \overline{f(x)g(x)}$$

Proposition IV .7. *Les Dirac forment une base de $\mathbb{C}[G]$*

IV .3 Sructure du groupe dual (et bidual)

Lemme IV .8. *G et $\hat{G}$ ont même exposant*

LEÇON 120

ANNEAUX Z/NZ. APPLICATIONS.

Références Perrin, Gourdon, Szpirglas, Combes, Demazure

Développements

— Théorèmes des deux carrés

— Irréductibilité polynômes cyclotomiques

— Réciprocité quadratique

Rapport jury (2015) Cette leçon, souvent choisie par les candidats, demande toutefois une préparation minutieuse.

Tout d'abord, n n'est pas forcément un nombre premier. Il serait bon de connaître les sous-groupes de Z/nZ et, plus généralement, les morphismes de groupes de Z/nZ dans Z/mZ.

Il est nécessaire de bien maîtriser le lemme chinois et sa réciproque. Et pour les candidats plus étoffés, connaître une généralisation du lemme chinois lorsque deux éléments ne sont pas premiers entre eux, faisant apparaître le pgcd et le ppcm de ces éléments.

Il faut bien sûr savoir appliquer le lemme chinois à l'étude du groupe des inversibles, et ainsi, retrouver la multiplicativité de l'indicatrice d'Euler. Toujours dans le cadre du lemme chinois, il est bon de distinguer clairement les propriétés de groupes additifs et d'anneaux, de connaître les automorphismes, les nilpotents, les idempotents...

Enfin, les candidats sont invités à rendre hommage à Gauss en présentant quelques applications arithmétiques des anneaux Z/nZ, telles que l'étude de quelques équations diophantiennes bien choisies. De même, les applications cryptographiques telles que l'algorithme RSA sont naturelles dans cette leçon.

Motivation / speech à l'oral Anneaux qui arrivent naturellement en arithmétique quand on veut résoudre des équations modulo n. Les calculs dans Z/nZ se passent plutôt bien, puisque l'on a un anneau commutatif. Il est intéressant de s'attarder sur les inversibles, et leur cardinal. Le cas particulier n premier donne une structure de corps, avec un groupe des inversible cyclique. Un passage chez les polynômes donne des critères d'irréductibilité bien pratique.

Récapitulatif : 3 idées principales : Z/nZ, $(Z/nZ)^*$ et Fp.

En fait ces cas sont fondamentaux car :

1/ thm structure groupe abéliens finis ; 2/ racines n-ième de l'unité et cyclotomie ; 3/ corps fini : sous corps est un Fp où p est la caractéristique (nécessairement premier car pZ est le noyau du morphisme $n \mapsto n1_K$ donc par passage au quotient l'anneau Z/pZ isomorphe à $\phi(Z/nZ)$, sous anneau de K donc intègre).

Remarque : éventuellement sucrer la 3ème partie, mettre réduction modulo p et cyclotomie dans la 2nde partie si le plan est déséquilibré.

I Structures de groupe Z/nZ. Premières applications

I .1 Le groupe $(Z/nZ, +)$

Def, abélien, cyclique, tout groupe cyclique à n élément est isomorphe à Z/nZ, exemple important : racines nième de l'unité (que l'on retrouvera dans la suite).

Sous groupe de Z/nZ : les Z/dZ avec d diviseur de n ; il y en a $\phi(n)$ par def de ϕ ;

I .2 Le groupe multiplicatif $((Z/nZ)^*, \times)$

ordre des éléments, thm Euler : $a^{\phi(n)} = 1[n]$
Racines primitives de l'unité. Récupérer $\sum \phi(d) = n$ la somme allant sur les diviseurs d de n.

I .3 Structure des groupes abéliens finis

Introduire quelques notions de groupe dual d'un groupe abélien fini quand même. Recaser le dvt, mais un peu limite ?

II Structure d'anneau (Z/nZ,+,x), voire plus

II .1 Anneau

abélien, corps ssi p premier ssi Z/pZ intègre
Lemme chinois :

$$pgcd(m,n) = 1 \iff Z/(mnZ) \approx Z/nZ \times Z/mZ$$

généralisation à un produit.

Remarque : si pgdc(m,n)=d $\neq 1$, alors $(a,b) \in Z/nZ \times Z/mZ$ alors $(mn(a,b)) = (0,0)$ donc (a,b) est d'ordre mn/d : donc il n'y a pas d'éléments d'ordre mn.

II .2 Cas particulier p premier

On a un corps ! Trop cool.
Thm Wilson, Fermat, morphisme de Frobenius

III Polynômes

III .1 Irréductibilité

Eisenstein, réduction modulo p (ok car on a mentionné Fp juste avant...). Exemples.

III .2 Cyclotomie

Racines de l'unité, polynômes cyclotomiques, irréductibilité dans Z et Q.

IV Corps fini

Mettre les trucs classiques. Attention au hors sujet quand même. Mais bon ça doit passer.

Bien insister sur la caractéristique, qui donne $q = p^n$, sur le fait que K^* est cyclique, donc engendré par α, et comme par magie on a $F_q = K = F_p(\alpha)$ c'est pile dans la leçon.

Parler du rôle des polynômes cyclotomiques, et de leur (non) irréductibilité dans Fp.

IV .1

IV .2

IV .3

LEÇON 121

NOMBRES PREMIERS. APPLICATIONS.

Références Combes, Demazure Ukmer

Développements

— Théorèmes des deux carrés

— Irréductibilité polynômes cyclotomiques

— Réciprocité quadratique

Rapport jury (2015) Il s'agit d'une leçon pouvant être abordée à divers niveaux.

Il y a tant à dire sur la question que le candidat devra fatalement faire des choix. Attention toutefois à celui des développements, ils doivent être pertinents ; l'apparition d'un nombre premier n'est pas suffisant !

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 est un résultat historique important, qu'il faudrait citer. Sa démonstration n'est bien sûr pas exigible au niveau de l'agrégation.

Quelques résultats sur les corps finis et leur géométrie sont les bienvenus, ainsi que des applications en cryptographie.

Motivation / speech à l'oral Autre idée pour le plan : faire carrément une partie entière sur la cyclotomie. En particulier, étudier les polynômes cyclotomiques dans F_p et montrer qu'ils permettent de bien réaliser F_q comme corps de rupture et corps engendré par une racine primitive (racine d'un "bon" polynôme cyclotomique).

I Rôle fondemental des nombres premiers

I .1 Le théorème fondemental de l'arithmétique

Définition 76. *p est un nombre premier si ces seuls diviseurs sont 1 et p.*

Théorème I .1. *p premier et p divise ab alors p divise a ou b.*

Théorème I .2. *Théorème fondemental de l'arithmétique : tout entier $n > 1$ s'écrit de façon unique (à l'ordre des éléments près) comme produits de puissance de nombres premiers.*

Proposition I .3. *Pour connaître les nombres premiers, on peut faire le crible d'Eratosthène.*

Théorème I .4. *Il existe une infinité de nombre premiers.*

I .2 Arithmétique modulaire et primalité

Définition 77. *Fonction d'Euler*

Théorème I .5. *Petit théorème de Fermat*

p nombre premier et a entier non divisible par p. Alorss $a^{p-1} \equiv 1[p]$. De plus, pour a quelconque, $a^p \equiv a[p]$.

Remarque : réciproque fausse (p=561=3x11x17). Néanmoins, on utilise ce test en pratique (test de Fermat). On tire a au hasard, si $a^{n-1} \not\equiv 1[n]$, on dit que n est pseudo premier en base a. On le fait pour plein de bases. Les nombres de Caramichael sont pseudo premiers dans toutes les bases sans être premiers...

Théorème I .6. *Théorème d'Euler*

Application : dernier chiffre de 3^{345}.

Théorème I .7. *Théorème de Wilson*

I .3 Groupe et fonction indicatrice d'Euler

I .4 Répartition des nombres premiers

Théorème I .8. *Théorème des nombres premiers*

$$\pi(x) \sim \frac{x}{ln(x)}$$

Démonstration. Admise. □

Mais il existe des trous arbitrairement grands.

II Polynômes et nombre premiers

II .1 Résidus quadratiques

Motivation : solutions de $ax^2 + bx + c \equiv 0[p]$.
Recaser loi réciprocité quadratique.

II .2 Factorisation de polynômes à coefficients entiers

Proposition II .1. *Critère d'irréductibilité d'Eisenstein. Réduction modulo p.*

Théorème II .2. *Théorème chinois : A anneau principal, m et n dans A tq pgcd(m,n)=1. Alors*

$$A/mnA \approx A/mA \times A/nA$$

II .3 Polynômes cyclotomiques

Irréductibilité dans Q et Z (développement).

III Corps finis

III .1 Un cas particulier d'anneau : Z/pZ

C'est en fait le corps F_p. Z/nZ intègre ssi n premier.

III .2 Propriétés de bases sur les corps finis

Prop de base : caractéristique, si K corps fini on a $[K : F_p]$ = n donc $card(K) = p^n =: q$. Et K^* est cyclique.

III .3 Réalisation des corps fini

Comme corps de décomposition de $X^q - X$ Mais on peut aussi le réaliser comme un $F_p(\alpha)$, par exemple avec α générateur de K^*.

LEÇON 122

ANNEAUX PRINCIPAUX. EXEMPLES ET APPLICATIONS.

Référence : Perrin, Combes, Szpirglas, Objectif Agreg
Remarque : éventuellement rajouter de la théorie des corps pour recaser dvt corps de rupture ?
Et parler d'anneaux noethériens ? (avec applications ! ! !)

Notations : A anneau commutatif, I idéal.

I Notion de principalité

I .1 Idéaux d'un anneau ; Anneaux principaux

Définition 78. *Idéal principal s'il est engendré par un élément.*

Définition 79. *I est premier ssi l'anneau A/I est intègre.*
I maximal si $I \neq A$ et I maximal pour l'inclusion, cad : si J idéal de A contenant I, et $J \neq A$, alors J=I.

Proposition I .1. *I premier* $\iff$ $(ab \in I \Rightarrow a \in I$ *ou* $b \in I)$
I maximal $\iff$ *A/I corps.*

Exemple : nZ premier ssi n=0 ou n premier.
Les idéaux maximaux de Z sont les pZ, ou p premier.

Corollaire I .2. *Tout idéal maximal est premier.*

Réciproque fausse, par ex (X) idéal de k[X,Y] premier non maximal.

Définition 80. *Un anneau est principal si tout idéal est engendré par un élément.*

Exemple : Z (idéaux de la forme nZ)

I .2 Cas particulier important : les anneaux euclidiens

Définition 81. *A euclidien si A intègre et muni d'un stathme euclidien.*

Théorème I .3. *euclidien implique principal*

Réciproque fausse : $Z[\frac{1+i\sqrt{19}}{2}]$

Lemme I .4. *Division euclidienne dans A[X], A anneau commutatif.*

Corollaire I .5. *k corps, k[X] euclidien (donc principal)*

Contre exemple : $< 2, X + 1 >$ n'est pas principal dans Z[X].

I .3 Premières applications

Application En algèbre linéaire

Définition 82. *polynôme minimal d'un endomorphisme.*

Proposition I .6. *u diago ssi π_u scindé à racine simple sur K. (à mettre plus loin ?)*

Proposition I .7. *Lemme des noyaux.*

Application en théorie des corps

Définition 83. *Def pol minimal d'un élément algébrique.*

Proposition I .8. *Construction de corps par adjonction d'éléments.*
Si P irred (non nul) de k[X], principal, alors (P) est maximal, donc k[X]/(P) est un corps.

recasage développement ?

L'anneau Z[i] des entiers de Gauss recasage développement

II Arithmétique

II .1 Pgcd et ppcm

Définition 84. *pgcd ppcm dans anneau principal.*

Solutions d'équations diophantiennes

Proposition II .1. *Soient a,b $\in \mathbb{Z}$, pas tous les deux nuls, et $d = pgcd(a,b)$ leur pgcd. Pour $c \in \mathbb{Z}$, l'équation ax+by = c a une solution si et seulement si d divise c. Si (x_0, y_0) est une solution particulière, les autres solutions sont tous les couples de la forme $(x_0 - kb_0, y_0 + ka_0)$, où k décrit $\mathbb{Z}$, $a = da_0$ et $b = db_0$.*

Démonstration. Découle de Bézout + linéarité de l'équation □

Algorithme d'Euclide et complexité cf Demazure

Proposition II .2. *pgcd(u,v)=pgcd(u,qv) où q est le quotient dans la division euclidienne de u par v.*

Algorithme :

II .2 Anneau factoriels

Vraiment indispensable ?

II .3 Théorème chinois

[Combes]
Exemple : mettre un exemple de calculs (Szpirglas)
Application : π_u scindé à racines simple implique u diagonalisable. [Objectif Agreg]

LEÇON 123

CORPS FINIS. APPLICATION

Référence : Demazure, Gozot, Perrin.
Developpement : loi réciprocité quadratique [H2G2]
théorème des deux carrés [Perrin]

I Construction des corps finis

I .1 Premières observations à la main

Proposition I .1. *$F_p = Z/pZ$ p premier est un corps*

Définition 85. *Perrin p.72 On appelle sous corps premier de K le plus petit sous corps de K.*
Soit $\phi : \mathbb{Z} \to K ; n \to n1_K$ morphisme d'anneaux. Son noyau est un idéal de $\mathbb{Z}$, donc soit $\mathbb{Z}$, soit un $p\mathbb{Z}$ ou p premier (car inclu dans K, donc intègre).
p est appelé la caractéristique du corps K.
Si K est fini (ce que nous supposerons dans la suite), car(K)=p premier. (réciproque fausse, considérer $F_p(X)$.

Proposition I .2. *Demazure, p.210 Si K fini, alors $|K| = p^n$ pour un certain n entier*

Démonstration. Isomorphisme d'ev entre $|K|$ et $(Z/pZ)^n$ □

Proposition I .3. *(Demazure ou Perrin) Morphisme de Frobenius. Automorphisme car K fini. Si K est F_p, c'est l'identité.*
$Q \in F_p[X] \iff Q(X^p) = Q(X)$

Théorème I .4. *Wedderburn (éventuellement)*

Exemple de construction explicites Quotientage par polynômes irréductible

Proposition I .5. *Construction par adjonction d'un élément. Soit K un corps et P un polynôme irréductible sur K[X]. Alors K/(P) est un corps.*
Si α racine de P dans une extension, alors K/(P) est isomorphe à $K[\alpha]$.

Démonstration. Utiliser Bézout. □

Proposition I .6. *Soit K un corps. Alors $M_\alpha(K) = \{\begin{pmatrix} a & \alpha b \\ b & a \end{pmatrix}, a, b \in K\}$ est un sous corps de l'anneau non commutatif $M_2(K)$.*

Exemples : $F_3/(X^2+1)$, $F_3/(X^2+X+1)$, $M_{-1}(F_3)$ sont 3 exemples de corps à 9 éléments. Pas évident qu'ils vont être isomorphes !

I .2 Construction formelle

Théorème I .7. *Demazure p.210 K corps fini de caractéristique p, de cardinal $|K| = p^n$.*
$\alpha^{p^n} = \alpha \; \forall \alpha \in K$ et dans K[X] $X^{p^n} - X = \prod_{\alpha \in K}(X - \alpha)$
Le groupe K^* est cyclique, d'ordre $|K| - 1$.
Le nombre d'élément de tout sous corps de K est de la forme p^r ou r divise n.
Inversement, pour tout diviseur r de n, il existe un unique sous corps de K à p^r éléments : c'est l'ensemble des $\alpha \in K$ tels que $\alpha^{p^r} = \alpha$.

Théorème I .8. *(redite du 1er point précédent...) Si K corps à p^n éléments existe, alors $K = \{$racines dans K de $X^{p^n} - X \in \mathbb{Z}/p\mathbb{Z}[X]\}$.*

Démonstration. Inclusion directe par Lagrange à K^* d'ordre q-1.
Inclusion réciproque par cardinaux. □

Théorème I .9. *Gozot p.73 Soit p premier et n entier naturel. $q = p^n$. Alors (i) $F_q := Dec_{F_p}(X^q - X)$ est un corps à q éléments.*
(ii) $X^q - X = \prod_\alpha (X - \alpha)$
(iii) Tous les corps finis à q éléments sont isomorphes à F_q.

Remarque : Il faut faire attention. Tous les corps à q éléments sont isomorphes certes, mais l'isomorphisme n'est pas uniquement déterminé. Sur $\mathbb{F}_4$, si on prend (0,1,α, β) et (0,1,α', β'), on peut considérer l'isomorphisme envoyant α sur α' ou celui envoyant α sur β'.
Lire Demazure.

Proposition I .10. *Treillis des corps finis.*

$$F_{p^n} \subset F_{p^m} \iff n|m$$

I .3 Lien entre les deux constructions

Proposition I .11. *Soit K un corps fini, de caractéristique p et cardinal p^n. Il existe un élément primitif de K sur F_p. Autrement dit, il existe un polynôme irréductible de degré n.*

Autrement dit, on peut toujours voir F_q comme $F/p[X]/(P)$ ou bien $F_p[\alpha]$.

Démonstration. α générateur de K^* (ie une racine primitive de l'unité d'ordre $|K| - 1$). Tout élément non nul de K est une puissance de α, et tout sous anneau contenant α est égal à K. Donc $K = F_p[\alpha]$.
On prend P=polynôme minimal de α. Il est irréductible sur F_p, et de degré n. En effet, $F_p[X]/(P) = F_p[X] = F_q$ corps donc P irred sur $F_p[X]$, de degré n. □

Théorème I .12. *De l'élément primitif pour les corps finis. Gozot p.84*
Soit L extension de degré finie de K, corps fini. Alors L est monogène, cad $\exists \xi \in L / L = K(\xi)$

Démonstration. m=$[L : K] \in \mathbb{N}^*$. L est un K-ev de dimension m, donc isomorphe en tant que K ev à K^m, donc en bijection avec K^m. Donc $card(L) = (card(K))^m$ et L est un corps fini. Par csq, le groupe multiplicatif de L est cyclique. Soit ξ générateur de L^*. p=car(K)=car(L)/ On a $\mathbb{F}_p \subset K \subset L$, et $L = \mathbb{F}_p(\xi)$. Donc $L \subset K(\xi)$. Comme $K(\xi) \subset L$, il y a égalité. □

Proposition I .13. *Soit K un corps fini à q éléments, et m premier avec q. Notons r la classe de q dans le groupe $(Z/mZ)^*$ Alors le polynôme cyclotomique $\phi_m(X)$ se décompose dans K[X] en produit de polynôme unitaires irréductibles de degré r, tous différents.*

Corollaire I .14. *K corps à q éléments, n entier positif premier à q. Pour que $\phi_m(X)$ soit irréductible sur K, il faut et suffit que la classe de q engendre le groupe $(Z/mZ)^*$.*

Corollaire I .15. *Dans $F_p[X]$, ϕ_{p^r-1} est produit de polynômes unitaires irréductibles de degré r, tous différents.*

Définition 86. *Un polynômes irréductible $P \in F_p[X]$ de degré r, est dit primitif s'il divise ϕ_{p^r-1} ou, de manière équivalente, si ses racines sont des racines primitives $(p^r - 1)$ ieme de l'unité.*

Proposition I .16. *Pour tout nombre premier p et tout entier $r > 0$, il existe dans $F_p[X]$ des polynômes irréductibles primitifs de degré r.*

II Etude du groupe cyclique et application

II .1 Application de cyclicité de K^*

On a déjà vu que K^* est cyclique.

Corollaire II .1. *Il existe un polynôme irred de degré donné sur $Fp[X]$.*

Proposition II .2. *Théorème de l'élément primitif*

Facile à démontrer dans le cas des corps finis.

II .2 Etude des carrés

Perrin p.74-75

Définition 87.

$$F_q^2 = \{x \in F_q / \exists y \in F_q x = y^2\}$$

$$F_q^{*2} = F_q^2 \bigcap F_q^*$$

Proposition II .3. *Nombre de carré*
1) Pour p=2, on a $F_q^2 = F_q$
2) Si $p > 2$*, on a* $|F_q^2| = \frac{q+1}{2}$ *et* $|F_q^{*2}| = \frac{q-1}{2}$

Proposition II .4. *Caractérisation des carrés*
On suppose $p > 2$*. Alors :*

$$x \in F_q^{*2} \iff x^{\frac{q-1}{2}} = 1$$

Corollaire II .5. *Il existe une infinité de nombres premiers de la forme 4k+1.*

Démonstration. p diviseur premier de $(n!)^2 + 1$. Alors p impair et $p > n$ (sinon p diviserait n !) Dans F_p, $(n!)^2 + 1 = 0$ donc -1 est un carré donc p=1[4]. □

Proposition II .6. *Dirichlet faible (grosse généralisation du corollaire précédent !)*
Soit $n \geq 1$*. Il exite une infinité de nombres premiers p avec* $p = 1[n]$.

Lemme II .7. *L'équation* $ax^2 + by^2 = 1$ *admet une solution sur* F_q.

Démonstration. Les cardinaux de $\{ax^2, x \in F_q\}$ et $1 - by^2, y \in F_q$ valent $\frac{q+1}{2}$ donc les deux ensembles ne sont pas disjoints. □

Théorème II .8. *Loi de réciprocité quadratique [H2G2]*

II .3 Réduction des formes quadratique sur F_q

Gozard p.94

Proposition II .9. *K corps fini de caractéristique différente de 2. E Kev de dimension n finie.*
1) Q fome quadratique non dégénérée sur E, il existe une base $(f_1, \dots, f_n)$ *de E telle que* $Mat(Q, F) = diag(1, \dots, 1, d)$*, où* $d \in K^*$.
2) Soit Q_1 *et* Q_2 *deux formes quadratiques non dégénérées sur E.* (E, Q_1) *et* (E, Q_2) *sont isomorphes ssi* $\frac{disc(Q_2)}{disc(Q_1)} \in K^2$.

Corollaire II .10. *Soit K corps fini, caractéristique différente de 2. Il y a exactement deux classes d'équivalence dans l'ensemble des matrices de* $M_n(K)$ *symétriques et inversibles pour la relation de congruence.*

III Algèbre linéaire et dualité sur un corps fini

Proposition III .1. $A \in M_n(F_q)$ *diagonalisable* $\iff X^q - X$ *annulateur.*

III .1 Etudes de groupes particuliers

Ref : Perrin, chapitre groupe linéaire

Proposition III .2. *Cardinaux usuels*
$|GL_n(F_q)| = \prod_{i=0}^{n-1}(q^d - q^i)$ *(compter les bases)*
$|SL_n(F_q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})q^{n-1} = N$
$PGL_n(F_q) = |SL_n(F_q)| = N$
$|PSL_n(F_q) = N/d$ *où d=pgcd(n,q-1).*

Proposition III .3 (H2G2 2eme tome p. 217)**.** *Le cardinal du cône nilpotent dans* $M_n(F_q)$ *vaut* $q^{n(n-1)}$.

Proposition III .4. *Perrin p.113*
$GL_2(F_2) = SL_2(F_2) = PSL_2(F_2) = S_3$
$PGL_2(F_3) = S_4$ *et* $PSL_2(F_3) = A_4$
$PGL_2(F_4) = ??$

Proposition III .5. *Il existe un p-Sylow dans* $GL_n(F_q)$ *(matrices triangulaires supérieurs avec des 1 sur la diagonale).*

III .2 Algèbre bilinéaire

déjà mis dans partie 2.3

III .3 Codes correcteurs

Demazure ou RMW.

III .4 Caractères et groupes duaux d'un corps fini

Voir Peyré.

IV Autres trucs

Ref : Lidl Niederreiter, Introduction to finite fields and their applications.

IV .1 Représentation via matrices compagnons

Soit P polynômes irréductible de degré n sur $F_p[X]$, et C_P la matrice compagnon de P. Alors F_q est isomorphes à l'ensemble des polynômes en A de degré inférieur à n. (en fait osef du degré inférieur à n, vu que le polynôme minimal de C_P est de degré n, mais c'est pour en avoir un nombre fini).

Exemple : $h(x) = x^2 + x + 2 \in F_3[X]$

IV .2 Racines de l'unité et polynômes cyclotomiques

Définition 88. *Le corps de décomposition de $X^n - 1$ sur K est appelé nieme corps cyclotomique sur K, et noté $K^{(n)}$.*
Les racines de $X^n - 1$ sont appelées racine nième de l'unité sur K, et le set de ces racines est noté $E^{(n)}$.

Cas particulier si K=Q : on retrouve U_n

Théorème IV .1. *K corps caractéristique p.*
(i) Si p ne divise pas n, alors $E^{(n)}$ est un groupe cyclique d'ordre n pour la multiplication de $K^{(n)}$.
(ii) Si p divise n, $n = mp^e$ avec m,e entiers, tel que m pas divisible par p. Alors $K^{(n)} = K^{(m)}$, $E^{(n)} = E^{(m)}$, et les racines de $X^n - 1$ dans $K^{(n)}$ sont les m éléments de $E^{(m)}$, chacune ont une multiplicité p^e.

Démonstration. (i) n=1 ok
$n \geq 2$ $X^n - 1$ n'a pas de racines multiples, donc $E^{(n)}$ a n éléments. C'est un groupe multiplicatif : si $\eta, \xi \in E^{(n)}$, alors $t(\xi\eta^{-1})^n = \xi^n\eta^{-n} = 1$, donc $\xi\eta^{-1} \in E^{(n)}$. Soit $n = p_1^{e_1} \dots p_t^{e_t}$ une décomposition de n. Alors pour chaque i, $1 \leq i \leq t$, il existe $\alpha_i \in E^{(n)}$ racine de $x^{n/p_i} - 1$, donc $\beta_i = \alpha_i^{n/p_i^{e_i}}$ est do'rdre $p_i^{e_i}$, et donc $E^{(n)}$ est un groupe cyclique de fénérateur $\beta = \beta_1 \dots \beta_t$.
(ii) $x_n - 1 = x_{mp^e} - 1 = (x^m - 1)^{p^e}$ puis partie (i) □

V Vrac

Théorème V .1. *F_q^* est cyclique.*

Démonstration. □

LEÇON 126

EXEMPLES D'ÉQUATION DIOPHANTIENNE.

Rapport du jury 2015 : Il s'agit d'une leçon nouvelle, ou plus exactement d'une renaissance. On y attend les notions de bases servant à aborder les équations de type ax+by = d (identité de Bezout, lemme de Gauss), les systèmes de congruences, mais aussi bien entendu la méthode de descente et l'utilisation de la réduction modulo un nombre premier p. La leçon peut aussi dériver vers la notion de factorialité, illustrée par des équations de type Mordell, Pell-Fermat, et même Fermat (pour n = 2, ou pour les nombres premiers de Sophie Germain).

Notes historiques : Nommées en l'honneur de Diophante, mathématicien grec.

Définition 89. *Une équation Diophantienne est une équation polynômiale*

$$p(x_1, \dots, x_n) = 0$$

à coefficients entiers dont on cherche les solutions entières, ie dans $\mathbb{Z}^n$ ou dans $\mathbb{Q}^n$.

Motivations irrationalité de 2 ; Équation de Fermat

$\frac{26}{65} = \frac{2}{5}$: clairement, on a simplifié par 6. Chercher les fractions où ce genre de simplification grotesque est vérifié revient à résoudre une eq diophantienne. En effet, on veut : $\frac{10x+y}{10y+z} = \frac{x}{z}$ ce qui donne (10 x+y)z = x(10y +z). (rq : on veut en plus x,y,z positifs inférieurs à 10).

Problème de ces équations On peut résoudre les plus simple à la main en étant astucieux, mais (contrairement à des équations sur R ou C) si on change un paramètre et la méthode ne marche plus. On voudrait donc pouvoir classifier les équations en fonction de leur nombre de solutions.

Théorème .1. *Théorème de Matiyasevich (1970, admis)*

Il n'y a pas d'algorithme général permettant de déterminer si une équation en nombre entiers $p(x_1, \dots, x_n) = 0$ a ou non une infinité de solutions dans $\mathbb{Z}^n$.

Remarque : cela résout le 10ème problème de Hilbert. Par contre, si l'on restreint la famille d'équation, la réponse peut devenir positive (ex : équations de Thue (dur), formes quadratiques, ou équation du premier degré sont résolvables algorithmiquement).

Preuve .2. *Idée de la preuve : en gros introduire les nombres diophantiens. Montrer que c'est récursivement énumérable.*

I Equation du premier ordre

I .1 Equation ax+b=c

Proposition I .1. *Soient a,b $\in \mathbb{Z}$, pas tous les deux nuls, et $d = pgcd(a, b)$ leur pgcd. Pour $c \in \mathbb{Z}$, l'équation ax+by = c a une solution si et seulement si d divise c. Si (x_0, y_0) est une solution particulière, les autres solutions sont tous les couples de la forme $(x_0 - kb_0, y_0 + ka_0)$, où k décrit $\mathbb{Z}$, $a = da_0$ et $b = db_0$.*

Démonstration. Découle de Bézout + linéarité de l'équation □

Algorithme d'Euclide et complexité cf Demazure

Proposition I .2. *pgcd(u,v)=pgcd(u,qv) où q est le quotient dans la division euclidienne de u par v.*

Algorithme :

Proposition I .3. *Si l'ago d'Euclide partant de (u,v) (avec $u > v > 0$) s'arrête au bout de n pas, alors on a :*

$$u \geq dF_{n+2} \quad v \geq dF_{n+1}$$

où F_n désigne la suite de Fibonacci (qui part de (0,1)).

Preuve I .4. *Par récurrence.*

Sachant que $F_n = (\phi - \bar{\phi})/\sqrt{5}$, on a dans le pire des cas :

$$n + 1 \leq \frac{\ln(y\sqrt{5} + 1)}{\ln \phi}$$

Le pire peut être atteint si l'on part de deux nombres de Fibonnacci successifs.
Conclusion : algorithme efficace (ln(y) linéaire en le nombre de chiffres de y).

Interprétation matricielle de l'algorithme d'Euclide Sorte de pivot de Gauss, voir plus loin (paragraphe sur équations linéaires)

I .2 Equations $a_1x_1 + \cdots + a_nx_n = c$

Même topo, avec Bezout on a CNS d'existence des solutions. Par linéarité on casse le problème en solution particulière + solution homogène.

Pour vraiment résoudre, il faut se ramener au pb précédent avec deux inconnues seulement. On pose :

$$x_{n-1} = \alpha u + \beta v \quad x_n = \gamma u + \delta v$$

avec $\alpha\delta - \beta\gamma = 1$. On prend

$$\beta = \frac{a_n}{pgcd(a_n, a_{n-1})} \quad \delta \frac{-\alpha_{n-1}}{pgcd(a_n, a_{n-1})}$$

pour bien avoir pgcd$(\delta, \beta) = 1$

L'équation devient

$$a_1x_1 + \ldots a_{n-2}x_{n-2} + (\alpha_{n-1}\alpha + \alpha_k\gamma) = c$$

On a en plus :

$$a_{k-1}\alpha + a_k\gamma = -(pgcd(a_{k-1}, a_k)\alpha\delta) + pgcd(a_{n-1}a_n)\beta\gamma = -pgcd(a_{n-1}, a_n)$$

$$pgcd(a_1, a_2, \ldots a_{n-2}, pgcd(a_{n-1}, a_n)) = pgcd(a_1, \ldots, a_n)$$

On continue le procédé jusqu'à obtenir une équation de degré 2 qu'on sait résoudre, puis on remonte. C'est dégeulasse à faire à la main (et à écrire en latex), mais possible.

La conclusion est que la solution générale d'une équation à n inconnues s'exprime en fonction de n-1 paramètres.

Proposition I .5. *Dénombrement des solutions*

Soient $a_1, \ldots, a_n \in \mathbb{N}^*$ premiers entre eux dans leur ensemble, S_N le nombre de solutions positives ou nulles de l'équation $\sum_{i=1}^{N} a_ix_i = N$. Alors :

(i) S_N est le coefficient de t^N dans la série entière $\frac{1}{\prod_{i=1}^{n}(1-t^{a_i})}$

(ii) lorsque $N - - > \infty$ on a $S_N \equiv \frac{1}{a_1 \ldots a_p} \frac{N^{p-1}}{(p-1)!}$

I .3 Système d'équations diophantiennes linéaire

On pose $A \in M_{m,n}(\mathbb{Z})$ et $B \in \mathbb{Z}^m$ et on étudie AX=B où $X \in mathbbZ^n$.

Idée : on se plonge dans $\mathbb{Q}$: les solutions sont soit l'ensemble vide, soit un sous espace affine de $\mathbb{Q}^n$ de dimension n-rg(A). Mais ça merde pour repasser dans $\mathbb{Z}$ (pas trop compris pourquoi en fait....).

Bêtement, on peut résoudre les équations une par une, ou bien on substitue la première dans la deuxième, etc... Mais ça va être pénible. On propose dans la suite une méthode plus générale.

Solution du système homogène AX=0 Les solutions sont un sous groupe de $\mathbb{Z}^n$, noyau d'un morphisme de Z-module. Via le théorème de la base adaptée, c'est faisable (à parement).

Lemme I .6. *L'ensemble des $X \in \mathbb{Z}^n$ tels que AX=0 est un sous groupe de $\mathbb{Z}^n$, libre de rang n-rg(A) où le rang de A est calculé dans $M_{m,n}(\mathbb{Q})$.*

Solution particulière

Théorème I .7. *Soit M $\in M_{n,m}\mathbb{Z}$. Alors il existe deux matrices inversibles P$\in GL_m(\mathbb{Z})$ et Q$\in GL_n(\mathbb{Z})$ et une matrice (quasi)-diagonale DP$\in M_{n,m}(\mathbb{Z})$ telle que :*

(i) M=PDQ

(ii) D=diag($d_1, \dots d_r, 0, \dots, 0$) avec $d_1|d_2, \dots, d_i|d_{i+1}, \dots$.

De plus, si $M' = P'D'Q'$ est une autre décomposition avec ces deux propriétés, les scalaires d_j et d'_j sont associés. Donc à un inversible près, les d_i sont uniques.

Définition 90. *Les scalaires $d_1, \dots, d_r$ sont appelés les facteurs invariants de M.*

Démonstration. Voir Denis Serre, Matrices p.101

Unicité : faisable

Existence : Par récurrence.

Idée : Le but est de construire M' equivalente à M telle que $m'_{1,1}$ soit divisible par tous les coefficients de M, par exemple égal au pgcd des coeffs de M.

Méthode : Construire une suite de matrices équivalentes $M^{(p)}$ tel que $m_{11}^{(p)}$ divise $m_{11}^{(p-1)}$ et divise un élément de plus de $M^{(p-1)}$. Raisonner pour 4 cas possibles distincts.

Ceci étant fait, on peut réduire M en M' matrice avec que des zéros sur la première ligne et première colonne, sauf en (1,1) (où on a le pgcd des coeff de M). On applique l'HR et c'est plié.

□

On peut voir ça comme une variante de Gauss pour réduire A en matrice diagonale avec des facteurs invariants $Q^{-1}AP = D$ avec D=diag($d_1 \dots d_r, 0, \dots, 0$).

On peut avoir D via opérations élémentaires sur lignes colonnes, et P et Q gardent la trace de ces opérations (cf pivot de Gauss).

Ensuite il suffit de poser $X' = P^{-1}X$ et $B' = Q^{-1}B$ et on a :

$$AX = B \iff DX' = B'$$

I .4 Equations modulaires

Résolvables via lemme chinois, voir Demazure.

II Equations de degré supérieures : méthodes de résolution

II .1 Descente infinie

Définition 91. *Descente infinie : principe de la méthode, inventée par Fermat.*

On considère l'ensemble de $\mathbb{N}$ (supposé non vide, donc avec un plus petit élément) formé des éléments solutions de l'équation Diophantienne. On choisit le plus petit, puis on en exhibe un autre strictement plus petit, aboutissant à une contradiction.

Théorème II .1. *Soit $d \in \mathbb{N}$; on suppose d n'est pas un carré parfait. Alors $\sqrt{d}$ est irrationnel.*

Preuve II .2. *Supposons $\sqrt{d} = \frac{a}{b}$ avec a, b entiers premiers entre eux. Donc $b^2d = a^2$. Comme d n'est pas carré, il existe un nombre premier p et un entier k tel que $d = p^{2k+1}\delta$, avec $p \not| \delta$. Alors $p^{2k+1}|a^2$ donc $p^{k+1}|a$ et on écrit $a = p^{k+1}\alpha$ Donc $b^2\delta = p\alpha^2$. Donc p divise $b^2\delta$ mais ne divise pas δ. Donc $p|b^2$, et par suite $p|b$. Ainsi, $p|a$ et $p|b$, ce qui est en contradiction avec l'hypothèse a et b premier entre eux.*

Remarque : dans la preuve, on suppose un argument de minimalité (pgcd(a,b)=1) pour avoir une contradiction. Si on veut réellement être dans le cas de la descente infinie, on enlève cette hypothèse, et on voit qu'en partant de a, on construit une suite d'entiers positifs strictement décroissante, ce qui est impossible, et on est bien dans le cas de la descente. La preuve avec la minimalité est plus simple, mais l'autre est juste à savoir au cas où le jury pète les couilles.

Corollaire II .3. *Si $d \in \mathbb{N}$ n'est pas un carré parfait, les nombres 1 et $\sqrt{d}$ sont linéairement indépendants sur $\mathbb{Q}$; cad si p,q$\in \mathbb{Q}$ et $p + q\sqrt{d} = 0$, alors p=q=0.*

Exemple : triplet pythagoriciens

Prop : L'aire d'un triangle pythagoricien ne peut pas être un carré.

Application : Équation de Fermat pour n=4.

Exemple : $x^3 + 2y^3 = 4z^3$ n'a pas de solutions non triviales.

Proposition II .4. *Sophie Germain*

Si p nombre premier tel que 2p+1 est premier, alors $\nexists (x, y, z) \in \mathbb{Z}^3$ tels que $xyz \neq 0[p]$ and $x^p + y^p + z^p = 0$

Exemple : $n \in \mathbb{N}, \alpha \in \mathbb{N}, \alpha > n \geq 2 \quad x_1^2 \dots x_n^2 = \alpha x_1 \dots x_n$ n'admet pas de solutions non triviales. (à enlever ? en tout cas de mémoire j'ai pas de référence.... Si on enlève le second membre, c'est le problème de Warning il me semble, et c'est chaud.)

II .2 Changement d'anneau et réduction modulaire

Réduction modulaire Principe : On suppose il existe une solution, et on passe dans $\mathbb{Z}/p\mathbb{Z}$ pour trouver une contradiction. Permet en général de montrer l'inexistence de solutions.

Ex : $x^3 + 5 = 117y^3$ n'a pas de solutions entières (réduction modulo 9)

$x^3 + y^3 + z^3 = 4ou5$ n'ont pas de solutions entières (modulo 9)

Si $p \equiv 3[4]$, p premier, alors $x^2 + y^2 = pc^2$ n'a pas de solutions non triviales (réduction modulo p + descente infinie). Par contre, si $p \equiv 1ou2[4]$, il y en a une infinité !

$2^n - 1$ n'est jamais le carré d'un nombre pour $n \geq 3$

Changement d'anneau On se ramène au problème de trouver les unités dans un anneau du type $\mathbb{Q}[d]$

Théorème II .5. *Théorème des deux carrés*

Preuve II .6. *voir Perrin + Gourdon*

II .3 Méthodes géométriques

Solutions rationnelles On peut chercher à résoudre sur Q pour revenir sur Z. Dans le cas particulier où l'application qui a une solution sur Q associe une solution sur Z est surjective, c'est plié, mais c'est quand même un cas particulier...

Paramétrisation rationnelle

Définition 92. *On considère une équation p(X,Y,Z)=0, om $p \in \mathbb{Z}[X, Y, Z]$ est un polynôme homogène tel que la courbe d'équation p(x,y,1)=0 possède une paramétrage rationnel. On trouve les racines rationnelles de p(x,y,z) à partir de ce paramétrage.*

Exemple : cercle $x^2 + y^2 = 1$ paramétré par $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ permet d'obtenir l'ensemble des triplets pythagoriciens : ce sont les (x,y,z) = $(d(u^2 - v^2), 2duv, d(u^2 + v^2))$ où $d \in \mathbb{N}$ et pgcd(u,v)=1.

Paramétrisation rationnelle On considère f(x,y)=0 d'une conique, et (x_0, y_0) une solution particulière. Alors on trace la droite de pente $t \in \mathbb{Q}$ passant par (x_0, y_0). Le point d'intersection entre cette droite et la conique est alors une autre solution rationnelle.

Proposition II .7. *Toutes les solutions rationnelles sont ainsi obtenues.*

En dimension supérieure, le problème virent du fait qu'il n'y a pas forcément un seul point d'intersection.

Exemple : $x^2 + y^2 = 1$: solution particulière (-1,0) et on considère la droite y=t(x+1) ; le point d'intersection s'obtient en résolvant $x^2 + t^2(x + 1)^2 - 1 = 0$, avec $x \neq -1$, donc $x - 1 + t^2(x + 1) = 0$ cad :

$$x = \frac{1 - t^2}{1 + t^2} \qquad y = \frac{2t}{1 + t^2}$$

En écrivant t=a/b, on obtient les solutions de l'équation $x^2 + y^2 = z^2$ déjà étudié précédemment.

Proposition II .8. *Points entier appartenant à une hyperbole.*

Preuve II .9.

Critique/Limitations de cette méthode :

A partir de points rationnels, pas forcément direct de trouver les points entiers, et tâtonnement garanti.

En degré supérieur : un point rationnel ne suffit pas pour construire d'autres points (une droite coupe la courbe en strictement plus d'un point en général). Y'a des livres entiers sur les courbes elliptiques

LEÇON 140

CORPS DES FRACTIONS RATIONNELLES À UNE INDÉTERMINÉE SUR UN CORPS COMMUTATIF. APPLICATIONS.

Références Szpirglas, RDO

Développements

— Degré d'une sous extension monogène de K(X)

— Loi réciprocité quadratique

— Partition entier en parts fixées

Rapport jury (2015) Le bagage théorique est somme toute assez classique, même si parfois, le candidat ne voit pas l'unicité de la décomposition en éléments simples en termes d'indépendance en algèbre linéaire. Ce sont surtout les applications qui sont attendues : séries génératrices (avec la question à la clef : à quelle condition une série formelle est-elle le développement d'une fraction rationnelle), automorphismes de K[X], version algébrique du théorème des résidus, action par homographies. Le théorème de Lüroth n'est pas obligatoire et peut même se révéler un peu dangereux si le candidat n'est pas suffisamment préparé aux questions classiques qui l'attendent sur ce sujet.

Motivation / speech à l'oral

I Construction de K(X)

I .1 Définitions

Définition 93.

Proposition I .1. *Forme irréductible*

Théorème I .2. *Degré d'une extension monogène de K(X)*

Application : K-automorphismes de K(X) sont les homographies.

I .2 Racines, pôle, degré

Proposition I .3. *Zéros, pôles, fonctions rationnelles*

Définition 94. *Degré d'une fonction rationnelle*

I .3 Dérivation

II Décomposition en éléments simples

Motivation : trouver une base, comme $(1, X, X^2, \dots)$ dans le cas des polynômes.

II .1 Partie entière, partie polaire

Théorème II .1. *Décomposition en éléments simples dans K(X)*

Théorème II .2. *Cas particuliers dans C(X)*

$$F(x) = E(X) + \frac{c_{a,n}}{(X-a)^n}$$

Puis dans R(X)

II .2 Décomposition en éléments simples dans C

Théorème II .3. *Fonctions rationnelles et séries entières.*
Toute fonction rationnelle n'admettant pas 0 pour pôle peut être développée en série formelle.

III Applications

III .1 Calcul d'intégrales

III .2 Intégration des fonctions rationnelles

III .3 Série génératrices

Dénombrement équation diophantienne

LEÇON 141

POLYNÔMES IRRÉDUCTIBLES À UNE INDÉTERMINÉE. CORPS DE RUPTURE. EXEMPLES ET APPLICATIONS.

Référence : Perrin, Spzirglas, Demazure

I Polynômes irréductibles

I .1 Rappels et critères d'irréductibilité

Définition 95.

Proposition I .1.

I .2 Critères classiques d'irréductibilité

Contenu pour se ramener dans un corps
réduction modulo p
Eisenstein

I .3 Applications

Polynômes minimaux d'endomorphisme. Lemme des noyau. u diago ssi π_u scindé à racines simples.
Polynôme minimal d'éléments algébriques sur un corps.

I .4 Polynômes cyclotomiques

définition, irréductibilité. Exemples.

II Extension de corps

II .1 Corps de rupture

Def, thm, exemples ; appli construction corps par adjonction de racines.

II .2 Corps de décomposition

Def, thm, exemples. Unicité corps finis.

II .3 Lien entre les deux constructions : corps cyclotomiques

[Demazure] Prop, appli construction corps adaptées aux calculs.

Proposition II .1. *Soit K un corps fini, de caractéristique p et cardinal p^n. Il existe un élément primitif de K sur F_p. Autrement dit, il existe un polynôme irréductible de degré n.*

Autrement dit, on peut toujours voir F_q comme $F_p[X]/(P)$ ou bien $F_p[\alpha]$.

Démonstration. α générateur de K^* (ie une racine primitive de l'unité d'ordre $|K|-1$). Tout élément non nul de K est une puissance de α, et tout sous anneau contenant α est égal à K. Donc $K = F_p[\alpha]$.

On prend P=polynôme minimal de α. Il est irréductible sur F_p (par définition !), et de degré n. En effet, $F_p[X]/(P) = F_p[\alpha] = F_q$ corps donc P irred sur $F_p[X]$, de degré n.

Remarque : on peut aussi montrer que $(1, \alpha, \dots, \alpha^{n-1})$ est une F_p base de F_q. □

Théorème II .2. *De l'élément primitif pour les corps finis. Gozot p.84*
Soit L extension de degré finie de K, corps fini. Alors L est monogène, cad $\exists \xi \in L / L = K(\xi)$

Démonstration. m=$[L : K] \in \mathbb{N}^*$. L est un K-ev de dimension m, donc isomorphe en tant que K ev à K^m, donc en bijection avec K^m. Donc $card(L) = (card(K))^m$ et L est un corps fini. Par csq, le groupe multiplicatif de L est cyclique. Soit ξ générateur de L^*. p=car(K)=car(L)/ On a $\mathbb{F}_p \subset K \subset L$, et $L = \mathbb{F}_p(\xi)$. Donc $L \subset K(\xi)$. Comme $K(\xi) \subset L$, il y a égalité. □

Proposition II .3. *Soit K un corps fini à q éléments, et m premier avec q. Notons r la classe de q dans le groupe* $(Z/mZ)^*$ *Alors le polynôme cyclotomique* $\phi_m(X)$ *se décompose dans K[X] en produit de polynôme unitaires irréductibles de degré r, tous différents.*

Corollaire II .4. *K corps à q éléments, n entier positif premier à q. Pour que* $\phi_m(X)$ *soit irréductible sur K, il faut et suffit que la classe de q engendre le groupe* $(Z/mZ)^*$.

Corollaire II .5. *Dans* $F_p[X]$, ϕ_{p^r-1} *est produit de polynômes unitaires irréductibles de degré r, tous différents.*

Définition 96. *Un polynômes irréductible* $P \in F_p[X]$ *de degré r, est dit primitif s'il divise* ϕ_{p^r-1} *ou, de manière équivalente, si ses racines sont des racines primitives* $(p^r - 1)$ *ieme de l'unité.*

Proposition II .6. *Pour tout nombre premier p et tout entire* $r > 0$*, il existe dans* $F_p[X]$ *des polynômes irréductibles primitifs de degré r.*

LEÇON 142

ALGÈBRE DES POLYNÔMES À PLUSIEURS INDÉTERMINÉES. APPLICATIONS.

Références Szpirglas, RDO, Perrin

Développements

- Kronecker
- Bezout
- Degré d'une extension monogène de K(X)
- Molien

Rapport jury (2015) La leçon ne doit pas se concentrer exclusivement sur les aspects formels ou uniquement sur les polynômes symétriques. Les aspects arithmétiques ne doivent pas être négligés. Il faut savoir montrer l'irréductibilité d'un polynôme à plusieurs indéterminées en travaillant sur un anneau de type A[X], où A est factoriel. Le théorème fondamental sur la structure de l'algèbre des polynômes symétriques est vrai sur Z. L'algorithme peut être présenté sur un exemple. Les applications aux quadriques, aux relations racines coefficients ne doivent pas être délaissées : on peut faire par exemple agir le groupe GLn(R) sur les polynômes à n indéterminées de degré inférieur à 2.

Motivation / speech à l'oral

I L'algèbre $A[X_1, \dots, X_n]$

I .1 Définition, premières propriétés

Szp

Définition 97. *$A[X_1][X_2]$ et $A[X_2][X_1]$ sont canoniquement isomorphes, on note $A[X_1, X_2]$.*

Définition 98. *On itère par récurence pour définir $A[X_1, \dots, X_n]$.*

Exemple ; déterminant d'une matrice, polynôme caractéristique.

Proposition I .1. *Soit A factoriel. Alors A[X] est factoriel*

Théorème I .2. *A factoriel.*
$P \in A[X]$ irréductible $\iff$ P primitif (contenu égal à 1) et P irréductible dans $K_A[X]$.

Proposition I .3. *A factoriel alors $A[X_1, \dots, X_n]$ aussi. A noetherien, alors $A[X_1, \dots, X_n]$ aussi.*

Proposition I .4. *K corps, $K[X_1, X_2]$ n'est pas principal. Gauss subsiste, mais pas Bézout.*

I .2 Degré et polynôme homogène

Définition 99. *Dégré partiel, degré total*

Proposition I .5.

$$\deg(PQ) \leq degPdegQ \quad \textit{égalité si A intègre}$$
$$deg(P+Q) \leq max\{degP, degQ\}$$

Définition 100. *Polynômes homogène*

Théorème I .6. *Molien.*

II Polynômes symétriques, relations coefficients racines

II .1 Polynômes symétriques

[copié collé Spzirglas]

Définition 101. *Def pol symétrique.*

II .2 Relations coeff racines

Proposition II .1. *Relation coeff racines*

Théorème II .2. *Théorème de structure des polynômes symétriques.*

Théorème II .3. *Indépendance des polynôme symétriques élémentaires.*

II .3 Sommes de Newton

Appli : polynôme interpolateur de Newton.

III Elimination

III .1 Résultant

Résultant. Copié collé Szp page 564.
Recasage développement Kronecker.
Insister sur le fait que pour $A, B \in \mathbb{Z}[X]$ on a l'existence de U,V tels que UA+VB = Res(A,B).

III .2 Application arithmétique

III .3 Application géométrique

Définition 102. *Courbe algébrique plane*

$$V(A) = \{(x,y) \in C^2 : A(x,y) = 0\}$$

Si A réductible $A = A_1A_2$ alors $V(A) = V(A_1) \cup V(A_2)$. On dit que V(A) est irréductible si A l'est.

Définition 103. *Sous variété algébrique de $\mathbb{C}^n$*

$$V(I) = \{(x_1, \dots, x_n) \in \mathbb{C}^n : \forall P \in I, P(x_1, \dots, x_n) = 0\}$$

Si I principal, I=(P), on note V(I)=V(P).
Une courbe affine plane est une sous variété algébrique de $\mathbb{C}^2$.

Proposition III .1. *A pol non constant de $\mathbb{C}[X,Y]$. Alors V(AZ) est infini, plus précisément $card(V(A)) = card(\mathbb{R}) = card(\mathbb{C})$.*

Théorème III .2. *Bézout, 1779*
A, B irréductibles de $\mathbb{C}[X,Y]$ et non proportionnels. Alors $V(A) \cap V(B)$ est formé d'un nombre fini de points, éventuellement nul. Soit $R_X(A,B) \in \mathbb{C}[X]$ et $R_Y(A,B) \in \mathbb{C}[Y]$. Les coordonnées des points d'intersection vérifient $R_Y(A,B)(x) = 0$ et $R_X(A,B)(y) = 0$

LEÇON 144

RACINES D'UN POLYNÔME. FONCTIONS SYMÉTRIQUES ÉLÉMENTAIRES. EXEMPLES ET APPLICATIONS.

Références Szpirglas, Gourdon, Perrin, (RWM)

Développements

- Kronecker
- Gersgorin
- Corps rupture/décomposition

Rapport jury (2015) Il s'agit d'une leçon au spectre assez vaste. On peut y traiter de méthodes de résolutions, de théorie des corps (voire théorie de Galois si affinités), de topologie (continuité des racines) ou même de formes quadratiques. Il peut être pertinent d'introduire la notion de polynôme scindé, de citer le théorème de d'Alembert-Gauss et des applications des racines (valeurs propres, etc.). On pourra parler des applications de la réduction au calcul d'approximations de racines. Notons le lien solide entre la recherche des racines d'un polynôme et la réduction des matrices. Les valeurs propres de la matrice compagnon d'un polynôme permet d'entretenir ce lien. Les problèmes de localisation des valeurs propres, comme les disques de Gershgorin, sont tout à fait appropriés à ce contexte.

Motivation / speech à l'oral

I Racines d'un polynôme

I .1 Définitions, premières propriétés

Copié collé Gourdon.

Définition 104. *a racine si P(a)=0*

Proposition I .1. *a racine ssi X-a divise P*

Définition 105. *Racine d'ordre h*

Csq : P degré n a au plus n racines. Faux si pas sur un corps commutatif.

Proposition I .2. *K corps infini, tel que* $\forall x \in K \quad P(x) = 0$. *Alors P=0. faux si K fini.*

Définition 106. *Polynômes scindés, irréductible*

I .2 Dérivation et racines

Copié collé Szpirglas Lien racine multiple et polynômé dérivé ; pgcd(P,P') divise P.

Proposition I .3. $P \in \mathbb{Q}[X]$ *irréductible. Alors P n'a que des racines simple dans* $\mathbb{C}$.

Démonstration. P et P' sont premiers entre eux dans Q donc dans C aussi (prendre une relation de Bezout). □

I .3 Adjonction de racines

[Perrin ou RWM]

Définition 107. *Corps de rupture*

Théorème I .4. *Existence et unicité à isomorphisme près du corps de rupture.*

Définition 108. *Corps de décomposition*

Théorème I .5. *Existence et unicité à isomorphisme près du corps de décomposition.*

Mettre des exemples.

Définition 109. *Corps algébriquement clos.*

Théorème I .6. *C est algébriquement clos*

Corollaire I .7. *Polynômes irréductibles de $C[X]$ sont les polynômes X-a. Ceux de R[X] sont les X-a et les polynômes de degré 2 avec discriminant scrictement négatif.*

II Utilisation des racines

II .1 Relation coefficients racines

[Szp p.559 copié collé]
Def polynômes symétriques, relations coeff racines, thm de structure.

II .2 Elimination

Résultant. Copié collé Szp page 564.
Recasage développement Kronecker.

II .3 Algèbre linéaire

Polynôme minimal, caractéristique. Gersgorin

II .4 Interpolation de Lagrange

Eventuellement, s'il reste de la place.
Application : calcul de l'exponentielle matricielle.

LEÇON 151

DIMENSION D'UN ESPACE VECTORIEL (ON SE LIMITERA AU CAS DE LA DIMENSION FINIE). RANG. EXEMPLES ET APPLICATIONS.

Références Grifone, Gourdon, H2G2

Développements

— Frobenius

— Luroth

Rapport jury (2015) Dans cette leçon, il est important de bien connaître les théorèmes fondateurs de la théorie des espaces vectoriels de dimension finie en ayant une idée de leurs preuves. Ces théorèmes semblent simples car ils ont été très souvent pratiqués, mais leur preuve demande un soin particulier, ce qui rend la leçon plus difficile qu'on ne le croit. Des questions élémentaires comme "un sous-espace vectoriel d'un espace vectoriel de dimension finie, est-il aussi de dimension finie ?" peuvent dérouter un candidat. Les diverses caractérisations du rang trouvent bien leur place ainsi que, pour les candidats plus chevronnés, l'utilisation du degré d'une extension dans la théorie des corps. r

Motivation / speech à l'oral

I Bases et dimension

I .1 Familles génératrices, familles libres

Définition 110. $(v_i)_{i\in I}$ *est dite génératrice si* $Vect((v_i)_{i\in I}) = E$

exemple : dans R^2 les vecteurs de base. Dans $R[X]$ les monômes X^k.

Définition 111. *famille libre, liée.*

Proposition I .1. *Toute sur famille d'une famille génératrice est génératrice. Tout sous famille d'une famille libre reste libre.*

Définition 112. *Base = famille libre génératrice.*

I .2 Dimension d'un ev

Lemme I .2. $(e_1, \dots, e_n)$ *génératrice de E et* $(f_1, \dots, f_{n+1})$ *famille de E.*
Alors $(f_1, \dots, f_{n+1})$ *est liée.*

Démonstration. Récurrence sur n.
n=1 OK.
$n \Rightarrow n+1$: On décompose les f_i dans la base e_i :

$$\forall i \in \{1, \dots, n+1\} \quad f_i = \sum_{j=1}^{n} \alpha_i^j e_j$$

Si toues les α_i^n sont nuls, alors HR à $(e_1, \dots, e_{n-1})$ et $(f_1, \dots, f_n)$.
Sinon on pose $\tilde{f_i} = f_i - \frac{\alpha_i^n}{\alpha_{n+1}^n} f_{n+1}$ et on se ramène à l'HR. □

Corollaire I .3. *Soit E un ev admettant une base de cardinal fini. Alors toutes les bases de E ont le même cardinal, et on appelle dimension de E le cardinal commun.*

Rq : il vient aussi que si dimE=n, alors toute famille de plus de n vecteurs est liée, et toute famille de moins de n vecteurs n'est pas génératrice.

Théorème I .4. *Théorème de la base incomplète.*
E dimension finie. L famille libre et G famille génératrice, alors il existe une base B telle que $L \subset B \subset G$

Application : L'idéal des polynômes annulateur d'un endomorphisme est engendré par un élément.

I .3 Sous espace vectoriel de dimension finie

Proposition I .5. *F sev de E, dim E finie. Alors : F est de dimension finie et* $dimF \leq dimE$. *Egalité ssi F+E.*

Démonstration. Par l'absurde, si F pas de dimension finie, alors on prend un vecteur et on le complète en une famille libre à deux vecteurs (possible car sinon dimE ≤ 2). On continue jusqu'à ce que le cardinal de cette famille dépasse n=dimE. Contradiction (on a une famille libre de E de cardinal supérieur à la dimension).

Par le même raisonnement, on voit que dimF$\leq$ dimE.

Enfin, si on a égalité des dimensions, on a une base de F qui a dimE éléments, mais qui est en fait aussi une base de E, donc engendre E. Donc E=F. □

Définition 113. *Sous espaces supplémentaires*

Théorème I .6. *Tout sous espace F admet un supplémentaire dans E (E de dimension finie).*

Démonstration. Prendre une base de F, la compléter. □

II Rang

II .1 Rang et application linéaires

Définition 114. *rg(f)=dim(Im(f)).*

Théorème II .1. *Théorème du rang*

Démonstration. Posons dimE=n et dimKerf = r. $(w_1, \dots, w_r)$ base de Kerf et $(v_1, \dots, v_{n-r})$ telle que $(w_1, \dots, w_r, v_1, \dots, v_{n-r})$ soit une base de E. Soit $\mathcal{B} = (f(v_1), \dots, f(v_{n-r})$ base de Imf

B engendre Im f : prendre y=f(x), décomposer x dans la base de E et conclure.

B libre : $\sum_{i=1}^{n-r} \lambda_i f(v_i) = 0$ alors $f(\sum_{i=1}^{n-r} \lambda_i v_i) = 0$ donc $\sum_{i=1}^{n-r} \lambda_i v_i \in Kerf$

Donc $\sum_{i=1}^{n-r} \lambda_i v_i = a_1 w_1 + \dots a_r w_r$ Donc tous les coeff de cette relation sont nuls car la famille $(w_1, \dots, w_r, v_1, \dots, v_{n-r})$ est une base de E. □

Corollaire II .2. $f \in L(E, E')$ *où E et E' sont des ev de même dimension (finie). Alors :*
f injective $\iff$ *f surjective* $\iff$ *f bijective*

Démonstration. f injective $\iff \dim Kerf = 0 \iff dimE = rgf$ par thm du rang donc rg f = dim E', donc Imf= E' (Im f inclut dans E' et de même dimension). □

Application : formule de Grassman

II .2 Rang et matrices

Définition 115. *Rang d'une matrice = dimension de l'espace engendré par ses vecteurs colonnes.*

Proposition II .3. *A matrice de f dans un couple de base quelconque, alors rgA=rgf*

Corollaire II .4. *A matrice carré de taille n est inversible ssi rg(A)=n*

Proposition II .5. $P \in GL_m(K)$, $Q \in GL_n(K)$.

$$rg(PA) = rg(AQ) = rg(A)$$

Théorème II .6. *A équivalente à B ssi rg(A)=rg(B)*

Corollaire II .7. *rg(A)=rg(*^tA).

II .3 Calcul effectif du rang

III Dualité

Définition 116. *Espace dual = ensemble des formes linéaires sur E.*

Proposition III .1. $w \in E'$*, alors dim(Kerw) = n-1*
Noyau de w est un hyperplan de E, déterminé par w.

Définition, base duale, orthogonalité. Pas d'isomorphisme naturel entre E et E' : il faut fixer une base ;par contre il existe iso canonique entre E et bidual E".
Appli Dvp : Décomposition de Frobenius

IV Extension de corps

Degré d'une extension, multiplicativité du degré ;
Recasage développement degré d'une extension monogène de K(X) + application homographies.

LEÇON 152

DÉTERMINANT. EXEMPLES ET APPLICATIONS.

Références Ramis Warusfel niveau 1 (et 2), L1, Szpirglas

Développements
- Bezout
- thm Pascal
- Molien

Rapport jury (2015) Il s'agit encore d'une leçon où les résultats abondent et où le candidat devra faire des choix. On doit pouvoir, dans cette leçon, commencer par définir correctement le déterminant. Beaucoup de candidats entament la leçon en disant que le sous-espace des formes n-linéaires alternées sur un espace de dimension n est de dimension 1, ce qui est fort à propos. Toutefois, il est essentiel de savoir le montrer.

Il faut que le plan soit cohérent ; si le déterminant n'est défini que sur R ou C, il est délicat de définir det($XI_n - A$) avec A une matrice carrée.

L'interprétation du déterminant comme volume est essentielle.

Le calcul explicite est important, toutefois, le jury ne peut se contenter que d'un Vandermonde ou d'un déterminant circulant ! De même il est envisageable que des candidats s'intéressent aux calculs de déterminant sur Z avec des méthodes multimodulaires. Le résultant et les applications simples à l'intersection ensembliste de deux courbes algébriques planes peuvent trouver leur place dans cette leçon.

Il serait bien que la continuité du déterminant trouve une application, ainsi que son caractère polynomial.

Motivation / speech à l'oral Idée en vrac : Balancer la formule horrible avec les permutations. Insister sur le fait qu'elle est valable sur tout anneau A, donc cela motive le choix à priori pas du tout intuitif.

Donner l'interprétation quand k est un corps de forme n linéaire alternée. On retombe bien sur nos pieds, même si c'est pas la vision historique des choses.

Historiquement : volume d'un parallélogramme et système 2x2 ou 3x3 de Cramer. On trouve des formules sympa. Ca se généralise en dimension n, mais les temps de calculs sont trop long. Par contre ça donne des résultats théorique intéressant.

Le déterminant est en fait un outil à la fois très théorique et très pratique. Le plan fait bien remonter ces deux versants des choses.

L'application au polynôme caractéristique est frappante, l'étude de matrices compagnon permet en autre de montrer Cayley Hamilton, et avec un peu plus de travail, la décomposition de Frobenius.

Propriétés importantes : polynôme en les coeff de la matrice ; morphisme ; calcul par blocs.

I Déterminant : un outil théorique essentiel

(Suivre Ramis Warusfel niveau 1)

I .1 Définition et caractérisation

Le déterminant comme forme n-linéaire alternée

Définition 117. *$M \in M_n(A)$, avec A anneau commutatif. On définit le déterminant de M comme :*

$$\det M = \sum_{\sigma \in S_n} \epsilon(\sigma) m_{\sigma(1)1} \cdots_{\sigma(n)n}$$

En particulier, det M est un élément de A.

Exemple : $detP_\sigma = \epsilon(\sigma)$ (σ permutation).

det d'une matrice triangulaire = produit des coeff diagonaux (ok car tous les termes de la somme sont nuls sauf ceux qui correspondent à la permutation identité).

Remarque : Cardinal de Sn est n !, donc cette formule nécessite (n-1)n ! multiplications et n ! additions. Pas de panique, on ne l'utilisera jamais en pratique (mais utile pour la théorie)

Proposition I .1. *det :$E^n \to K$ est multilinéaire alternée, invariant par transposition.*

Rq : Ici E n'est pas un ev, mais un A-module (sinon écrire la prop avec les vecteurs colonnes comme dans RW).

Démonstration. L'invariance par transposition découle de la formule même.

Multilinéaire : pénible à écrire, le faire pour la première colonne pour alléger les notations. □

det M est dans A permet dans la suite de se placer dans $M_n(K_A)$ oùK_A est le corps des fractions, pour éviter de se faire des noeuds aux cerveaux (et éviter de parler de modules à l'oral).

E K-ev, K corps.

Proposition I .2. *f une forme multilinéaire alternée, $(v_1, \dots, v_n) \in E^n$ et $\sigma \in S_n$. Alors :*

$$f(v\sigma(1), \dots, v_{\sigma(n)}) = \epsilon(\sigma) f(v_1, \dots, v_n)$$

Démonstration. Le faire pour une transposition, par exemple (12) :

$$0 = f(v_1 + v_2, v_1 + v_2, v_3, \dots, v_n)$$

$$f(v_2, v_1, v_3, \dots, v_n) = -f(v_1, v_2, v_3, \dots, v_n)$$

Puis écrire σ comme produit de m transpositions et conclure par récurrence sur m. □

Proposition I .3. *Forme n linéaire alternée sur E est un K-ev de dimension 1. Le déterminant est celle qui vaut 1 pour l'identité.*

Démonstration. Soit d une forme n linéaire alternée.

A matrice, $e_1, \dots, e_n$ base canonique de $\mathbb{K}^n$. On a :

$$\begin{aligned} d(A) = &\quad d(\textstyle\sum_{k_1=1}^n a_{k_1,1} e_{k_1}, \dots, \dots, \sum_{k_n=1}^n a_{k_n,n} e_{k_n} && (152.1)\\ = &\quad \textstyle\sum_{k_1,\dots,k_n=1}^n a_{k_1,1} \dots a_{k_n,n} d(e_{k_1}, \dots, e_{k_n}) && (152.2) \end{aligned}$$

Deux possibilités pour les indices de la somme :

- Le n-uplet $(k_1, \dots, k_n)$ possède deux nombres égaux : donc la matrice $(e_{k_1}, \dots, e_{k_n})$ a deux vecteurs égaux. L'alternance de d assure $d(e_{k_1}, \dots, e_{k_n}) = 0$.
- Le n-uplet $(k_1, \dots, k_n)$ définit une permutation $\sigma \in S_n$ en posant $\sigma(j) = k_j$. Donc la matrice $(e_{k_1}, \dots, e_{k_n})$ résulte de la matrice identité en appliquant la perrmutation σ^{-1} à ses colonnes. L'alternance de d et la proposition précédente montrent : $d((e_{k_1}, \dots, e_{k_n})) = \epsilon(\sigma) d(e_1, \dots, e_n) = \epsilon(\sigma) d(\mathbb{I}_n)$

Par conséquent :

$$d(A) = \det A \; d(I_n)$$

□

Le déterminant comme morphisme de groupe

Proposition I .4. *A,B dans Mn(K), det(AB)=det(A) det(B)*

Rq : vrai si les matrices sont à coeff dans un anneau.

Démonstration. $f : M \mapsto det(AM)$ est multilinéaire en les colonnes de M, donc proportionnelle à det M. Pour A=I_n, on trouve la constante de proportionnalité vaut det A.

On peut aussi le faire par calcul dégeu via la formule du début (par exemple si on est dans un anneau). □

Corollaire I .5. *A inversible ssi $detA \in K^*$. En particulier, $det(A)^{-1} = det(A^{-1})$ lorsque A est inversible.*
$\det : A \mapsto \det A$ *est un morphisme surjectif de groupes multiplicatifs de $GL_n(K)$ dans K^*..*

Corollaire I .6. *det invariant par changement de base. On peut donc parler de déterminant d'un endormorphisme.*

De manière générale, on a :

Proposition I .7.

$$A^t com(A) = {}^t com(A)A = det(A)I_n$$

Démonstration. Pénible, pénible, pénible.

Idée : $A^t com(A) = det(A)I_n$: développer suivant les lignes. L_j la jieme ligne de A, et C_j jième colonne de ${}^t com(A)$. On mq $L_l C_j = \delta_{lj} \det(A)$.

Pour ${}^t com(A)$ A, faire le développements suivant les colonnes (génial dis donc). □

Proposition I .8. *Soit $A \in M_{n,p}(K)$. Considérons une matrice carré inversible B, d'ordre r extraite de A. Le rang de A est égal à r ssi B ne possède aucune matrice bordante inversible.*

Corollaire I .9. *Le rang d'une matrice A est le maximum des ordres des matrices carrées inversibles extraites de A.*

I .2 Méthodes de calcul

Via la formule horrible avec permutations (pas efficace).
Développer par rapport ligne, colonne (Rq : pénible à montrer....)
Exemple déterminant de Vandermonde, matrice compagnon (développer par rapport à la dernière colonne).
Déterminant matrice triangulaire par blocs. On se ramène à de tels matrices par opérations élémentaires.
Produit des valeurs propres. (à mettre plus loin, comme csq du polynôme caractéristique et relation coeff racines ?)

I .3 Propriétés du déterminant

det polynômiale, donc continu (même C^∞).
Application : GLn(C) ouvert connexe (par arc).
Application : Matrice réelles semblables sur C le sont sur R.
Différentielle du déterminant [Rouvière] : attention, utilise la comatrice, donc il faut l'introduire avant...

I .4 Un exemple frappant : polynôme caractéristique

Définition 118. *Def. En particulier, C^∞ en les coeff de la matrice.*

Proposition I .10. $\xi_A(X) = X^n - Tr(A)X^{n-1} + \cdots + (-1)^n \det A$

Proposition I .11. $\xi_{AB} = \xi_{BA}$ *; donc en particulier le polynôme caractéristique est invariant par conjuguaison.*

Démonstration. Pas forcément trivial. (? ? ? ?) (c'est juste conséquence de detAB = det A det B où A,B à coeff dans un anneau). □

Proposition I .12. *Matrice compagnon associée à un polynôme P. Polynôme caractéristique = P*

Démonstration. Développer par rapport à la dernière colonne pour éviter une récurrence pénible (en développant p.r 1ère ligne). □

Cela peut fournir une première preuve de Cayley-Hamilton. Soit x dans E, on complète pour avoir $(x, f(x), \ldots, f^p(x))$ libre générant $Vect(f^i(x))$. On complète cette famille en une base de E ; dans cette base, la matrice de f est de la forme : $\begin{pmatrix} C_P & * \\ 0 & M \end{pmatrix}$ où P est le polynôme tel associé à la relation $f^p(x) = a_0 x + \cdots + a_{p-1} f^{p-1}(x)$.

$$\xi_f = \xi_{C(P)} \xi_M = P \xi_M$$

$$\xi(f(x)) = \xi_m(P(f)(x)) = 0$$

car P(f)(x)=0, par définition même de P.

Cette preuve est probablement à préférer dans cette leçon (valable sur tout corps, contrairement à la densité des matrices diagonalisables et met bien en valeur les propriétés du déterminant).

Remarque : (H2G2 II p.184)

On choisit une base dans l'espace des matrices : on écrit alors l'application $A \mapsto \chi(A)$ sous la forme $(x_{ij})_{1 \leq i,j \leq n} \mapsto (P_{kl}(x_{i,j}))_{kl}$ où les P_{kl} sont des polynômes en n^2 variables. Plus précisément, $P_{kl} \in \mathbb{Z}[x_{ij}]$ et sont indépendants du corps K (le déterminant est un polynôme à coefficients entiers indépendant du corps, de même que la somme et produit de deux matrices).

Théorème I .13. *Cayley Hamilton*

Démonstration. Preuve topologique de H2G2 (mais utilise le résultant, donc à replacer après ?).

Mais le plus simple c'est par densité de $D_n(C)$ dans $M_n(C)$.

Bref, on le prouve sur C. Comment récupérer le thm sur $M_n(A)$, A anneau ? Déjà on se met sur $M_n(K_A)$

Ensuite, la remarque précédente assure que les P_{kl} sont indépendants du corps K, donc dire que les P_{kl} sont nuls comme polynômes c'est dire que $\xi(M) = 0$ pour toute matrice M sur tout corps K_A. □

II Déterminant et rang : une utilisation pratique et théorique

II .1 Résolution de systèmes linéaires

(S) AX=B $(S_0) AX = 0$

Proposition II .1. *Sol(S_0) = sev de dimension p-r de K^p.*
Sol(S)= soit vide soit sous espace affine de dimension p-r de K^p, de direction S_0.

Proposition II .2. *Formules de Cramer. ; de Rouché-Fontené.*

II .2

II .3

III Un outil pratique en géométrie

[Szpirglas]

III .1 Lien avec le volume

Ref ? ? ? Un bouquin de niveau L1-L2 surement...

III .2 Intersections de droites

Les propriétés en coord barycentrique.
Recasage Pascal

III .3 Le déterminant de l'application de Sylverster

Trucs de base sur le résultant, on pompe le Szpirglas.

III .4 Intersection de courbes

Recasage Bézout

LEÇON 153

POLYNÔMES D'ENDOMORPHISME EN DIMENSION FINIE. RÉDUCTION D'UN ENDOMORPHISME EN DIMENSION FINIE. APPLICATIONS.

Références Gourdon, OA, H2G2

Développements

— Frobenius

— Image de l'exponentielle matricielle

Rapport jury (2015) Cette leçon est souvent choisie pour son lien avec la réduction, toutefois, le jury ne souhaite pas que le candidat présente un catalogue de résultats autour de la réduction, mais seulement ce qui a trait aux polynômes d'endomorphismes. Il faut consacrer une courte partie de la leçon à l'algèbre $K[u]$, connaître sa dimension sans hésiter. Les propriétés globales pourront être étudiées par les meilleurs. Le jury souhaiterait voir certains liens entre réduction de l'endomorphisme u et structure de l'algèbre $K[u]$. Le candidat peut s'interroger sur les idempotents et le lien avec la décomposition en somme de sous-espaces caractéristiques. Il faut bien préciser que, dans la réduction de Dunford, les composantes sont des polynômes en l'endomorphisme, et en connaître les conséquences théoriques et pratiques. L'aspect applications est trop souvent négligé. On attend d'un candidat qu'il soit en mesure, pour une matrice simple de justifier la diagonalisabilité et de déterminer un polynôme annulateur (voire minimal). Il est souhaitable que les candidats ne fassent pas la confusion entre diverses notions de multiplicité pour une valeur propre λ donnée (algébrique ou géométrique). Enfin, rappelons que pour calculer A^k, il n'est pas nécessaire en général de réduire A (la donnée d'un polynôme annulatrice de A suffit bien souvent).

Motivation / speech à l'oral Notations : E K-ev dimension finie, u un endomorphisme sur E.

I Polynômes et endomorphismes

I .1 L'algèbre $K[u]$

Définition 119. *Définition polynôme d'endomorphisme. $K[u]$ est une algèbre commutative.*

Définition 120. *Idéal des polynômes annulateur. Polynôme minimal π_u.*

Exemple : polynôme minimal d'un projecteur non trivial est X(X-1) ; d'une symétrie : (X-1)(X+1)

Proposition I .1.

$$K[u] \approx K[X]/(\pi_u)$$

donc $\dim K[u] = \deg \pi_u$

Proposition I .2. *Lemme chinois*

Proposition I .3. *Le polynôme minimal est un invariant de similitude.*

Proposition I .4. *P annulateur de u et λ valeur propre de u, alors $P(\lambda) = 0$.*

I .2 Quelques polynômes remarquables

Définition 121. *Polynôme caractéristique* ξ_u

Proposition I .5.

$$\lambda \in Sp(u) \iff \xi_u(\lambda) = 0$$

Corollaire I .6. *u inversible ssi 0 n'est pas racine du polynôme caractéristique.*

Proposition I .7. *Polynôme caractéristique est un invariant de similitude*

Définition 122. *Matrice compagnon*

Proposition I .8.

$$\pi_{C(P)} = \xi_{C(P)}(-1)^n$$

Proposition I .9. *Equivalence classiques sur les endomorphismes cycliques.*

Théorème I .10. *Cayley Hamilton*

Corollaire I .11.

$$\pi_u | \xi_u$$
$$\deg \pi_u \leq n = dim E = \deg \xi_u$$

Proposition I .12. *u nilpotent* $\iff \pi_u = X^k \iff \xi_u = X^n \iff$ *Sp(u)*=$\{0\}$

I .3 Lemme des noyaux, sous espaces stables

II Polynômes d'endomorphismes : un outil pour la réduction

II .1 Diagonalisation

II .2 Trigonalisation

II .3 Invariants de similitude

Théorème II .1. *Réduction de Frobenius*

III Applications

III .1 Calculs de puissances

Soit P un polynôme annulateur de u. Alors $X^k = PQ + R$ (division euclidienne) donc $u^k = R(u)$. Autrement dit, connaitre les puissances de u jusqu'à u^{degP-1} suffit pour calculer toutes les autres puissances de u.

Suites récurrentes linéaires

$$u_{n+p} = \sum_{i=0}^{p-1} a_i u_{n+i}$$

Alors en vectorisant correctement, on a $X_n = A^n X_0$ où $X_n =^t (u_n, u_{n+1}, \ldots, u_{n+p-1})$ et A la matrice qu'il faut pour que ça ait un sens.

Suite récurrentes linéaires

III .2 Exponentielle d'endomorphismes

Proposition III .1. $K[u]$ *est fermé (sous espace vectoriel de dimension finie), donc* $\exp(u) \in K[u]$.

Proposition III .2. *Développement*

$$\forall A \in GL_n(C) \quad \exists P \in C[X] : A = \exp(P(A))$$
$$\exp(M_n(C)) = GL_n(C)$$
$$\exp(M_n(R)) = \{B^2, B \in GL_n(R)\}$$

Application : $GL_n(C)$ est connexe.

Calcul pratique

Soit Dunford, soit interpolation de Lagrange.

Utilité pratique

Résoudre X'=AX.

LEÇON 154

SOUS-ESPACES STABLES PAR UN ENDOMORPHISME OU UNE FAMILLE D'ENDOMORPHISMES D'UN ESPACE VECTORIEL DE DIMENSION FINIE. APPLICATIONS.

Références Gourdon, Grifone, Objectif Agregation

Développements

- Frobenius
- Cardinal cône nilpotent
- Lie Kolchin
- Table de S4

Rapport jury (2015) Les candidats doivent s'être interrogés sur les propriétés de l'ensemble des sous-espaces stables par un endomorphisme. Des études détaillées de cas sont les bienvenues, par exemple le cas d'une matrice diagonalisable, le cas d'une matrice nilpotente d'indice maximum. La décomposition de Frobenius trouve tout à fait sa place dans la leçon. Notons qu'il a été ajouté à l'intitulé la notion de familles d'endomorphismes. Ceci peut déboucher par exemple sur des endomorphismes commutant entre eux ou sur la théorie des représentations.

Motivation / speech à l'oral

I Propriétés de bases

I .1 Définition, endomorphisme induit

Définition 123. *Sev stable*

Exemple : Ker u, Im u, E tout entier. Cas projecteur.
u stabilise toutes les droites ssi u homothétie.

Proposition I .1. *Ker P(u) est stable. Polynôme caractéristique, sous espaces caractéristiques*

Proposition I .2. *Si u et v commutent, alors un sous espace u-stables est aussi v-stables*

Définition 124. *Endomorphisme induit*

Csq : polynôme caractéristique
Dans R, si n impair alors il existe un vecteur propre donc un sous espace stable de dimension 1. Dans C il existe toujours un vecteur propre.

I .2 Espaces propres, caractéristique

Définition 125. *Polynôme caractéristique.* $E_\lambda = Ker(u - \lambda Id)$ *est le sous espace propre associé à la valeur propre* λ*.*

Théorème I .3. *Les sous espaces propres sont en som directe. Cette somme vaut E ssi u est diagonalisable.*

Définition 126. *Polynôme minimal*

Proposition I .4. *Les racines du polynôme minimal de u sont exactement les valeurs propres de u.*

Démonstration. Division euclidienne du polynôme minimal par $X - \lambda$. □

Supposons pol minimal scindé

$$\mu_u(X) = \prod (X - \lambda_i)^{q_{\lambda_i}}$$

Définition 127. *Sous espace caractéristique* $E'_\lambda = Ker(u - \lambda Id_E)^{q_\lambda}$

Proposition I .5. *Le sous espace caractéristique contient le sous espace propre (associé à la même vp...) et est stable par u*

Lemme I .6. *Lemme des noyaux*

Conséquence : les sous espaces caractéristiques sont en somme directe, et leur somme est E.
Autre csq : Cayley Hamilton

I .3 Diagonalisation

Théorème I .7. *Les propriétés suivantes sont équivalentes :*
(i) l'endomorphisme u est diagonalisable sur k ;
(ii) il existe un polynôme scindé à racines simples dans k qui annule u ;
(iii) le polynôme minimal de u est scindé à racines simples dans k ;
(iv) pour chaque λ*, on a* $E_\lambda = E'_\lambda$

En particulier, avec (iv) on a que E est somme directe des espaces caractéristiques.

Théorème I .8. *A trigonalisable ssi poly caractéristique est scindé*

En particulier, sur corps algébriquement clos c'est plié.
En fait on peut faire mieux, on peut prendre une base associée aux sous espaces caractéristiques : on a une matrice diagonale par bloc. Ca fait le lien avec la section suivante.

II Défaut de diagonalisabilité : décomposition d'endomorphismes et diagonalisation par blocs

II .1 Nilpotence

Def matrices nilpotentes. On peut caser Fitting ici pour le motiver (+ dvt cardinal cône nilpotent éventuellement)

II .2 Décomposition de Dunford

Découle du lemme des noyaux. Limite HS ?

II .3 Réduite de Jordan

Lemme II .1. *Noyaux itérés*

Théorème II .2. *Réduction de Jordan*

II .4 Endomorphismes cyclique ; décomposition de Frobenius

Les quelques lemmes nécessaire pour la preuve du dvt Frobenius (Gourdon)

III Application aux familles d'endomorphismes

III .1 Représentation

Def ; on va jusqu'à Maschke. Insister sur sous représentation aussi.

III .2 Diagonalisation, trigonalisation simultanée

Les prop usuelles quand ça commute (famille infinie). On recase Lie Kolchin (dvt).

LEÇON 155

ENDOMORPHISMES DIAGONALISABLES EN DIMENSION FINIE.

Références Gourdon Grifone H2G2

Développements

— Frobenius
— exp $S_n(R) \to S_n^{++}(R)$ isomorphisme
— FFT (dans rapport)

Rapport jury (2015) Il faut ici pouvoir donner des exemples naturels d'endomorphismes diagonalisables et des critères de diagonalisabilité. On peut croire que le calcul de l'exponentielle d'un endomorphisme diagonalisable est immédiat une fois que l'on connaît les valeurs propres et ceci sans diagonaliser la matrice, par exemple à l'aide des projecteurs spectraux. On peut sur le corps des réels et des complexes donner des propriétés topologiques. Mentionnons que l'affirmation l'ensemble des matrices diagonalisables de $M_n(K)$ est dense dans $M_n(K)$ nécessite quelques précisions sur le corps K et la topologie choisie pour $M_n(K)$. Sur les corps finis, on a des critères spécifiques de diagonalisabilité. On peut dénombrer les endomorphismes diagonalisables, ou possédant des propriétés données, liées à la diagonalisation. Le lien peut aussi être fait avec la théorie des représentations et la transformée de Fourier rapide.

Motivation / speech à l'oral

I Diagonalissation

I .1 Espaces propres, caractéristique

Définition 128. *Polynôme caractéristique.* $E_\lambda = Ker(u - \lambda Id)$ *est le sous espace propre associé à la valeur propre* λ*.*

Théorème I .1. *Les sous espaces propres sont en som directe. Cette somme vaut E ssi u est diagonalisable.*

Définition 129. *Polynôme minimal*

Proposition I .2. *Les racines du polynôme minimal de u sont exactement les valeurs propres de u.*

Démonstration. Division euclidienne du polynôme minimal par $X - \lambda$. □

Supposons pol minimal scindé

$$\mu_u(X) = \prod (X - \lambda_i)^{q_{\lambda_i}}$$

Définition 130. *Sous espace caractéristique* $E'_\lambda = Ker(u - \lambda Id_E)^{q_\lambda}$

Proposition I .3. *Le sous espace caractéristique contient le sous espace propre (associé à la même vp...) et est stable par u*

Lemme I .4. *Lemme des noyaux*

Conséquence : les sous espaces caractéristiques sont en somme directe, et leur somme est E.
Autre csq : Cayley Hamilton

I .2 Diagonalisation

Théorème I .5. *Les propriétés suivantes sont équivalentes :*
(i) l'endomorphisme u est diagonalisable sur k ;
(ii) il existe un polynôme scindé à racines simples dans k qui annule u ;
(iii) le polynôme minimal de u est scindé à racines simples dans k ;
(iv) pour chaque λ, on a $E_\lambda = E'_\lambda$

En particulier, avec (iv) on a que E est somme directe des espaces caractéristiques.

I .3 Application

Réduction de systèmes linéaires $U_{n+1} = AU_n$; X'=AX ; calcul de puissance de matrice

II Défaut de diagonalisation

Théorème II .1. *A trigonalisable ssi poly caractéristique est scindé*

En particulier, sur corps algébriquement clos c'est plié.
En fait on peut faire mieux, on peut prendre une base associée aux sous espaces caractéristiques : on a une matrice diagonale par bloc. Ca fait le lien avec la section suivante.

II .1 Décomposition de Dunford

II .2 Endomorphismes cycliques ; Frobenius

Diagonalisation par blocs.

II .3

III Famille d'endomorphismes

III .1 Diagonalisation simultanée

Pour famille d'endomorphismes qui commutent

III .2 Endomorphismes auto-adjoints

Matrices symétriques, thm spectral ; recasage développement exponentielle

III .3 Représentation

Maschke dans un groupe abélien ? (à voir)

LEÇON 156

EXPONENTIELLE DE MATRICES. APPLICATIONS.

Références Szpirglas (p.358 un complément parfait sur l'exponentielle !) ; Mneimné Testard Introduction à la théorie des groupes de Lie classiques ; Denis Serre, Matrices ; (Brian C. Hall, Lie Groups, Lie Algebras, and Representations)

Développements

- $\exp(M_n(\mathbb{R}))$
- O(p,q)
- $\exp : S_n \to S_n^{++}$ homéomorphisme

Rapport jury (2015)

Motivation / speech à l'oral

I Motivations, définition et premières propriétés

I .1 Systèmes d'équations différentielles linéaires à coefficients constants

Soit A une matrice de $M_n(\mathbb{K})$., et X(t) un vecteur colonne. On s'intéresse à :

$$\begin{cases} \frac{dX}{dt} &= AX(t) \\ X(0) &= X_0 \end{cases}$$

On sait résoudre ce système en dimension 1. Il s'agit de généraliser cela à des dimensions supérieures.

On procède via un développement d'Euler Mac-Laurin de la solution X(t) en puissance de t :
$X(t) = X_0 + \dot{X}_0 t + \ddot{X}_0 \frac{t^2}{2} + \dots$ avec $\dot{X}_0 = \frac{dX}{dt}_{(t=0)}$
De plus, on remarque que : $\frac{d^n X}{dt^n} = A^n X(t)$
Donc : $X(t) = X_0 + tAX_0 + \frac{(tA)^2}{2} X_0 + ...$

On reconnait le développement en série entière de l'exponentielle classique, et on note : X(t)=exp(tA) X_0

Définition 131. *Pour $A \in M_n(\mathbb{K})$, on appelle exponentielle de A la série : $\sum_{k=0}^{\infty} \frac{1}{k!} A^k$. Cette série converge normalement sur tout compact de $M_n(\mathbb{K})$. En particulier, l'exponentielle est une fonction continue.*

La convergence est assurée sur tout compact de $M_n(\mathbb{K})$; il suffit, pour le voir simplement, de prendre une norme d'opérateur sous-multiplicative, et on a facilement :
$\|exp(A)\| \leq exp(\|A\|)$. Comme K est complet, cela assure la convergence normale. Le résultat ne dépend pas de la norme choisie car on est en dimension finie.

I .2 Premières propriétés

Proposition I .1. *Si A,B $\in M_n(\mathbb{K})$,* $\exp(A+B) \neq \exp(A)\exp(B)$

Contre exemple :
$A = \begin{pmatrix} 0 & 0 \\ \theta & 0 \end{pmatrix}$ $B = \begin{pmatrix} 0 & -\theta \\ 0 & 0 \end{pmatrix}$ donc $\exp(A) = I_n + A$ $\exp(B) = I_n + B$
mais $exp(A+B) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \neq \exp(A)\exp(B)$

Remarque : On peut montrer que :

$$AB = BA \iff \forall t \in \mathbb{R},\ exp(t(A+B)) = exp(tA)exp(tB)$$

Corollaire I .2. $\exp(\mathrm{A})$ *est inversible, d'inverse* $\exp(-\mathrm{A})$.

Proposition I .3. *Soient A* $\in\in M_n(\mathbb{K})$ *et P* $\in\in GL_n(\mathbb{K})$. *On a :*
exp(PAP^{-1}*)=P exp(A) P*$^{-1}$
exp(^{t} *A) =* ^{t} *exp(A)*
exp(Tr(A))=det(exp(A))
exp(Sp(A))=Sp(exp(A))

Proposition I .4. *Soit A* $\in M_n(\mathbb{C})$*; alors* $\exists\ P \in \mathbb{C}[X]$ *tel que exp(A) = P(A).*

Preuve $\mathbb{C}[A]$ est sev de $M_n(\mathbb{C})$, donc est complet (ou fermé) (dimension finie).
Ainsi : $\sum_{n=0}^{N} \frac{1}{n!} A^n \in \mathbb{C}[A]$, donc exp(A) $\in \mathbb{C}[A]$ (car $\mathbb{C}[A]$ est fermé).

I .3 Calcul de l'exponentielle

Cas particuliers où le calcul est facile
Si D=diag($\lambda_1 \dots \lambda_n$), alors exp(D)=diag(exp($\lambda_1 \dots \lambda_n$)).
Si la matrice est nilpotente, alors son exponentielle est une somme finie.
Dans certains cas, on peut reconnaitre une série entière.

Si A diagonalisable
Un autre cas simple est lorsque la matrice est diagonalisable. Alors soit on diagonalise la matrice, mais c'est pénible, car il faut calculer la matrice de passage (et l'inverser). Une méthode plus élégante est de tirer profit de la proposition I .4, et de trouver le polynôme P telle que exp(A)=P(A). Si l'on connait les valeurs propres de A, alors on peut passer par des polynômes interpolateur de Lagrange.
Soit A matrice diagonalisable dans $\mathbb{C}$, et $\{\lambda_1, ..., \lambda_n\}$ son spectre (valeurs propres non nécessairement distinctes). Alors : A = P^{-1} diag(λ_i) P.
Soit Q un polynôme tel que Q(λ_i)=e^{λ_i}. Donc $Q = \sum_{i=2}^{n} e^{\lambda_i} P_i$ avec $P_i = \prod_{j=1\dots n, j\neq i} \frac{X-\lambda_j}{\lambda_i - \lambda_j}$.
Il vient Q(A) = exp(A).

Application : donner un exemple

Si A non diagonalisable
Dunford probablement inutile car trouver la décompo de Dunford n'est pas trivial.
Si A réel, regarder si elle est diago sur $\mathbb{C}$.
Sinon, elle est toujours trigonalisable sur $\mathbb{C}$. On a le polynôme minimal de A : $\pi(X) = (X-\lambda_1)^{m_1} ... (X-\lambda_s)^{m_s}$, les λ_i étant distinctes. On fait une interpolation de Lagrange-Sylvester :

$$\begin{cases} r(\lambda_k) & = & e^{\lambda_k} \\ r'(\lambda_k) & = & e^{\lambda_k} \\ & \dots & \\ r^{m_k-1}(\lambda_k) & = & e^{\lambda_k} \end{cases}$$

Pour une preuve, raisonner par bloc de Young (pas complètement trivial non plus)

Avantage : on ne calcule pas les matrices de passage (et on n'en inverse pas non plus) ; par contre il faut quand même les valeurs propres. Pour les polynômes interpolateurs, il y a des formules toutes faites.
De plus, cette méthode est généralisable pour calculer les sommes $\sum_{k>0} a_k A^k$ (lorsque la somme converge).
Voir Grantmacher pour plus de détail (assez hardcore par contre)

Remarque sur Dunford

On peut être tenté d'utiliser la décomposition de Dunford pour calculer exp(A). En effet, A=D+N, et comme D et N commutent, on a exp(A)=exp(D)exp(N). N est nilpotente, donc exp(N) est une somme finie, et D est diagonalisable, donc exp(D) est censé être facile à calculer.
Via Dunford par Newton, on n'a pas besoin de connaître les valeurs propres de A, d'où à priori un gain par rapport à la méthode si dessus. Néanmoins, si pour calculer exp(D) on passe par Lagrange, alors autant faire Lagrange-Sylvester dès le début pour exp(A).... soit on diagonalise D, mais ce n'est pas forcément plus rapide.

Comparaison rapide :
Via Lagrange-Sylvester, on a un polynôme de même degré que le polynôme minimal.
Via Dunford on a log_2(n) opérations pour récupérer la décomposition, puis calculer exp(N) (au pire n-1 puissances de N), et exp(D) via Lagrange donne un polynôme de degré égal cardinal du spectre.

II Questions d'injectivité, de surjectivité et différentiabilité

II .1 Différentiabilité et logarithme

Proposition II .1. *La fonction exp est de classe C^∞. Sa différentielle en $0_{M_n(\mathbb{K})}$ vaut I_n. Elle réalise donc un difféomorphisme d'un voisinage ouvert de 0_n dans un voisinage ouvert de I_n dans $GL_n(\mathbb{K})$.*

Remarque : La preuve pour l'exponentielle de classe C^∞ est difficile. Voire Lafontaine (passage par de l'analyse complexe) ou Avez (preuve historique de Poincaré, par équa diff). Pour inversion locale, on a juste besoin de C^1, qui peut se voir plus facilement à la main.

Applications :
$GL_n(\mathbb{K})$ n'admet pas de sous groupes arbitrairement petits.
Soit $\phi : \mathbb{R} \to M_n(\mathbb{K})$ morphisme de groupe additif. Alors il existe une unique matrice A dans $M_n(\mathbb{K})$ telle que $\phi(t) = exp(tA)$. En particulier, ϕ est C^∞.

On a déjà introduit le logarithme pour les matrices nilpotentes, mais on généralise ici. On voit qu'on peut le définir sur toute la boule centrée en 0 de rayon 1, donc plus général que via inversion locale (où on n'a pas d'idée de la taille de voisinage...).

Proposition II .2. *Si $A \in B(I_n, 1) \bigcap GL_n(\mathbb{K})$, log(A) :=* $\sum_{n=1}^{n} (-1)^n \frac{(A-I_n)^n}{n}$

Proposition II .3. *Ainsi défini, le logarithme est continu*

Remarque : Un résultat classique donne : $inf_{\|.\|} \|A\| = \rho(A)$, où l'inf est pris sur toutes les normes d'opérateur subordonnée, et ρ est le rayon spectral. Donc le logarithme est défini pour toutes les matrices de rayon spectral inférieur à 1 (en particulier les matrices nilpotentes).

Proposition II .4.

$$\exp(\log A) = A$$

Faire gaffe, car pas trivial à démontrer.

Applications :

$$(I_n + \frac{A}{k})^k \to exp(A)$$

$$SiA_k \to A, \quad (I_n + \frac{A_k}{k})^k \to exp(A)$$

$$\left(exp(\frac{A}{k})exp(\frac{B}{k})\right)^k \to exp(A+B)$$

II .2 Injectivité et surjectivité

Proposition II .5. *L'exponentielle matricielle sur $M_n(\mathbb{K})$ n'est ni injective ni surjective.*

Sur $M_n(\mathbb{C})$ l'exponentielle n'est même pas injective dès la dimension 1. En dimension supérieure, ça ne s'améliore pas... Sur $M_n(\mathbb{R})$, on a des problèmes dès la dimension 2 :

$$exp\begin{pmatrix} 0 & -2k\pi \\ 2k\pi & 0 \end{pmatrix} = I_2$$

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = exp\begin{pmatrix} 0 & \pi \\ -\pi & 0 \end{pmatrix}$$

La matrice : $\begin{pmatrix} -1 & 0 \\ 0 & -2 \end{pmatrix}$ n'est pas dans l'image de l'exponentielle réelle (raisonner sur les valeurs propres), mais dans l'image de l'exponentielle complexe (car inversible).

La matrice chère au jury : $A = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ n'est pas dans l'image de l'exponentielle réelle (mais en tant que matrice inversible, est dans l'image de l'exponentielle complexe). Pour le voir, soit on montre en finesse que ce n'est pas un carré (cf

développement).
Le raisonnement par l'absurde sur les valeurs propres est probablement préférable à l'oral : Si on pouvait écrire A=exp(M) avec M$\in M_n(\mathbb{R})$, alors on a exp(Sp(A))=Sp(exp(M)), en particulier on aurait exp(λ)=-1, avec λ valeur propre de M. Mais λ^* est aussi valeur propre de M (car M réelle), donc M a 2 valeurs propres distinctes, donc polynômes caractéristique est scindé à racines simples (λ et λ^*) et annule M (Cayley-Hamilton), donc M est diagonalisable. Donc A est aussi diagonalisable, ce qui n'est pas possible.

Par contre, la matrice de taille 4 $B = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$ est dans l'image de l'exponentielle réelle (et complexe). Le raisonnement est plus compliqué. A est dans l'image de l'exponentielle complexe, donc peut s'écrire sous la forme d'un carré (complexe !), donc A=C^2, avec C $\in M_n(\mathbb{C})$. Mais A réelle donc A=$\overline{A}$ = $(\overline{C})^2$ avec C=exp(E) (C et E sont des matrices complexes). Donc si B=exp(M), on peut prendre M diagonale par bloc avec des blocs de la forme $E\overline{E}$. Bien sûr, M est complexe ; la question est donc existe-t-il une matrice de passage complexes P telle que PMP^{-1} soit réelle ?

En pensant à la matrice de rotation diagonalisée dans $\mathbb{C}$ (diagonale de i et -i), on peut exhiber un changement de base telle que M soit réelle.

En fait plus simplement on a $A^2 = \exp(E\overline{E})$ réel donc $E\overline{E}$ est aussi réel (prendre le log).

Lien avec la géométrie En dimension 2, on remarque un lien évident avec exponentielle matricielle et transformations géométriques élémentaires.

$A_\theta = \begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix}$ alors $exp(A_\theta) = \begin{pmatrix} cos\theta & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix}$ est la matrice de rotation.

$exp\begin{pmatrix} \rho & \theta \\ \theta & \rho \end{pmatrix} = \rho I_2 + A_\theta$est la matrice de similitude directe d'angle θ et de rapport ρ.

$exp\begin{pmatrix} 0 & \theta \\ \theta & 0 \end{pmatrix} = \begin{pmatrix} cosh\theta & -sinh(\theta) \\ sinh(\theta) & cosh(\theta) \end{pmatrix}$ est une rotation hyperbolique (cf Avez).

En dimension 3 (et supérieure), on renvoie à : `http://dyna.maths.free.fr/docs/lecons/developpement_algebre_379.pdf`

Proposition II .6. *Soit A $\in GL_n(\mathbb{C})$. Alors il existe $P \in C[X]$ tel que A=exp(P(A)).*

Conséquences :
exp($M_n(\mathbb{C})$) = $GL_n(\mathbb{C})$
exp($M_n(\mathbb{R})$) = $\{B^2,\ B \in GL_n(\mathbb{R})\}$
Applications :
$GL_n(\mathbb{C})$ est connexe par arcs
$\forall A \in GL_n(\mathbb{C})$ et $p \in \mathbb{N}^*, \exists B \in GL_n(\mathbb{C})$ tq $A = B^p$.

II .3 Homéomorphismes classiques de l'exponentielle

Théorème II .7. *exp : $\{$ensemble des matrices nilpotentes$\}$ $\to$ $\{$ensemble des matrices unipotentes$\}$ est un homéomorphisme.*

Cela permet de définir le logarithme sur l'ensemble des matrices nilpotente (qui s'exprime comme une somme finie).

Théorème II .8. *On note $S_n(\mathbb{R})^{++}$ l'ensemble des matrices symétriques définies positives. On a les propriétés suivantes :*
exp : $S_n(\mathbb{R}) \to S_n(\mathbb{R})^{++}$ réalise un homéomorphime
exp : $H_n(\mathbb{R}) \to H_n(\mathbb{R})^{++}$ réalise un homéomorphime

Preuve II .9. *Caldero-Germoni tome 1 ; Mneimné-Testard (Intro groupes de Lie classique).*

Proposition II .10. *Application : Décomposition polaire + sous groupe connexes de O(p,q) (cf Caldero ou D.Serre qui le fait pour tous les groupes U(p,q)).*

III Autre propriétés à caser

III .1 Lien avec la réduction des matrices

Proposition III .1. *Dunford multiplicative*

+ critère de diagonalisabilité de A et exp(A)

Autre idée de plan : I/ idem
II/ Régularité de l'exponentielle et applications
III/ Étude topologique de $GL_n(\mathbb{C})$
1/ Sous groupes à un paramètre
2/ exp : $S_n \to S_n^{++}$
3/ Étude de O(p,q)

IV Developpement : Image de l'exponentielle réelle (et complexe)

Théorème IV .1. *(Ensemble image de l'exponentielle : cas réel et complexe)*
exp($M_n(\mathbb{C})$) = $GL_n(\mathbb{C})$)
exp($M_n(\mathbb{R})$) = $\{A$ telles que $\exists B \in M_n(\mathbb{R}) : A = B^2\}$

Pour la preuve, nous allons en fait démonter un résultat plus fort sur l'exponentielle complexe, qui nous permettra de conclure quand à l'exponentielle réelle et complexe.

IV .1 Propriété de l'exponentielle complexe

Proposition IV .2. *Soit $A \in GL_n(\mathbb{C})$, alors il existe P $\in \mathbb{C}[X]$ tel que A=exp(P(A)).*

Première preuve par Dunford
A=D+N=D(I_n+$D^{-1}N$) car D inversible (puisque A l'est)
D diagonalisable, on peut donc l'écrire comme l'exponentielle d'une matrice polynôme en A (penser aux polynômes d'interpolation de Lagrange).
$D = P\ diag(e^{\mu_i})\ P^{-1}$, poser $Q(\lambda_i) = exp(\mu_i)$
I_n+$D^{-1}N$ est unipotente, donc I_n+$D^{-1}N$ = exp$\left(\sum_1^l \frac{(-1)^{k-1}}{k} (D^{-1}N)^k \right)$

Deuxième Preuve

Définition 132. *On appelle groupe topologique un triplet (G,.,T) tel que (G,+) soit un groupe et (G,T) soit un ensemble topologique. En particulier, les applications inverses ($g \to g^{-1}$) et translation ((g,h) $\to$ gh) sont continues.*

Lemme IV .3. *Soit G un groupe topologique, et soit H un sous groupe de G contenant un voisinage du neutre e. Alors H est ouvert et fermé dans G.*

Démonstration du lemme
Montrons H ouvert. On peut prendre V voisinage ouvert de e dans G, avec $V \in H$. Soit $h \in H$. On a aussi $h \in hV \in H \in G$, ainsi hV est un voisinage ouvert de h inclus dans H (par continuité du morphisme translation à gauche par h). Donc H est ouvert.
Montrons H est fermé. On a $H^c = \bigcup_{g \notin H} gV$; si $g \notin H, gV \in H^c$. Comme gV est ouvert, H^c est ouvert (en tant que réunion d'ouvert), et H est fermé.

Démonstration de la proposition
On considère $\mathbb{C}[A]$, algèbre commutative de dimension finie sur $\mathbb{C}$ engendré par A, isomorphe à $\mathbb{C}[A]/(\pi)$ avec π polynôme minimal de A.
1/ Pour $M \in \mathbb{C}[A]$, on a exp(M) $\in \mathbb{C}[A]$ (car fermé), et exp(M) est inversible
2/ On note U = $\mathbb{C}[A] \bigcap GL_n(\mathbb{C})$, c'est à dire l'ensemble des matrices de $\mathbb{C}[A]$ inversibles
Alors exp : $(\mathbb{C}[A], +) \to (U, .)$ est un morphisme
3/ Montrons que l'image de $\mathbb{C}[A]$ par exp est ouvert et fermé
La différentielle de exp en 0 est l'identité, qui est bien inversible. Par le théorème d'inversion locale, exp réalise un difféomorphisme entre un voisinage ouvert V_0 de 0 et un voisinage ouvert V_I de l'identité. Par le lemme précédent, exp($\mathbb{C}[A]$) est ouvert-fermé.
4/ Montrons U connexe : Soient M, N dans U. On construit un chemine γ tel que $\gamma M + (1-\gamma)N$ soit dans U. Clairement, un tel chemin est dans $\mathbb{C}[A]$, mais n'a aucune raison d'être inversible à priori.
Considérons $z \to det(zM + (1-z)N)$: c'est une application polynômiale en z, donc son ensemble de 0, noté K, est discret. Donc $\mathbb{C}\ K$ est connexe par arcs, et on dispose d'un chemin continu γ tel que $det(\gamma M + (1-\gamma)N)$ soit non nul, c'est à dire $\gamma M + (1-\gamma)N$ est inversible. Donc U est connexe.
Conclusion : exp($\mathbb{C}[A]$) est un ouvert-fermé non vide de U, et U est connexe. Donc exp($\mathbb{C}[A]$) = U

Remarque : En fait le lemme permet d'éviter de montrer que exp($\mathbb{C}[A]$) est ouvert-fermé, mais rajoute de la confusion à mon sens, donc à améliorer. A l'oral, introduire le morphisme plus clairement.
On peut montrer facilement que U est fermé : c'est le complémentaire de l'ensemble des zéros de la fonction continue dét : $\mathbb{C}[C] \to \mathbb{C}$.

IV .2 Démonstration du théorème

La proposition précédente assure que exp((M_n(ℂ)) = GL_n(ℂ))

Proposition IV .4. *Soit A une matrice de $GL_n(\mathbb{R})$. Il existe une matrice réelle M telle que A=exp(M) si et seulement si il existe une matrice réelle B telle que B=A^2.*

Preuve
Sens direct : prendre B=exp($\frac{M}{2}$)...
Sens retour : On peut voire B comme une matrice inversible complexe. Alors on dispose de P dans $\mathbb{C}[X]$ telle que B=exp(P(B)).
La grosse subtilité est que P est complexe (et n'a aucune raison d'être réel), donc il faut être intelligent.
Néanmoins, comme B est réelle, elle est égale à sa conjuguée, et B=B*=exp(P*(B)).
En multipliant B par B* on obtient :
B^2 = exp((P+P*)(B)), et P+P* est un polynôme réel, donc (P+P*)(B) est une matrice réelle, notons la C. Donc A=exp(C), d'où le résultat.

IV .3 Applications

Corollaire IV .5. *Si $A \in GL_n(\mathbb{C})$ et $p \in \mathbb{N}^*$, il existe $B \in GL_n(\mathbb{C})$ telle que A=B^p.*

Preuve : A=exp(M) ; donc B=exp($\frac{M}{k}$) convient.

Corollaire IV .6. *$GL_n(\mathbb{C})$ n'admet pas de sous-groupes arbitrairement petits.*

Preuve On montre qu'il existe un voisinage V de I_n dans GL$_n$(ℂ) tel que le seul sous-groupe contenu dans V soit $\{I_n\}$.
Par le théorème d'inversion locale, exp réalise un difféomorphisme de U (voisinage de 0) dans V. On note V'=exp(U), et U'=exp(U/2).
V' est ouvert. Soit M ∈ V', on a M=exp(A) avec A dans U'. Il existe donc k ℕ tel que ka ∈ U \ U'. On a : exp(kA)=M^k ∈ V\V', donc $M^k \notin$ V'.
Donc M^k sort de V', et il n'existe pas de sous groupe arbitrairement petit (autre que le singleton $\{I_n\}$).

IV .4 Autre méthode, via l'homéomorphisme entre nilpotente et unipotentes

cf M. Zavidovique, Un max de maths (belle preuve d'imagination pour le titre du livre....).

IV .5 Autre méthode, uniquement dans le cas complexe

Proposition IV .7. *Soit exp : $M_n(\mathbb{C}) \to M_n(\mathbb{C})$*
Alors $Im(exp_{\mathbb{C}}) = GL_n(\mathbb{C})$

Preuve laborieuse, à évitier
exp(M)exp(-M) = In donc exp(M) ∈ $GL_n(\mathbb{C})$
Réciproquement, soit A ∈ $GL_n(\mathbb{C}$. On suppose dans un premier temps que A n'admet qu'une seule valeur propre (non nulle), notée $\lambda = exp(\mu)$. $N = \frac{1}{\lambda}(B - \lambda I_n)$ est nilpotente. Ainsi, I_n+N est unipotente, on dispose donc de M telle que exp(M)=I_n+N. Donc A=exp(μM). (Besoin d'une ou deux lignes de détails).

Considérons maintenant le cas général, où Sp(A)=$\{\lambda_1, ..., \lambda_r\}$. On a E en somme directe avec les sous espace propres : $E = +Ker(A - \lambda_i I_n)$. On travaille alors sur chaque sous espace propre E_i, où l'on dispose d'une matrice M_i telle que exp(M_i)=A sur E_i. La matrice M=diag($M_1, ...M_r$) vérifie bien, par construction, exp(M)=A.

Extension au cas réel Le cas réel est plus compliqué. En effet, on voit que même pour n=1, Im(exp) n'est pas $\mathbb{R}^*$, mais $\mathbb{R}_+^*$. Il est alors loisible de conjecturer que seule les matrices positives réelles (c'est à dire pouvant d'écrire comme un carré) vont être dans l'image de la fonction exponentielle.

Proposition IV .8. *Soit exp : $M_n(\mathbb{R}) \to M_n(\mathbb{R})$*
Alors $Im(exp_{\mathbb{R}}) = \{A$ telles que $\exists B \in M_n(\mathbb{R}) : A = B^2\}$

LEÇON 157

ENDOMORPHISMES TRIGONALISABLES. ENDOMORPHISMES NILPOTENTS.

Références Grifone

Développements

— Lie Kolchin (Chambert Loir)
— Cardinal cône nilpotent (H2G2)

Rapport jury (2015) Il est possible de mener une leçon de bon niveau, même sans la décomposition de Jordan, à l'aide des noyaux itérés. On doit savoir déterminer si deux matrices nilpotentes sont semblables grâce aux noyaux itérés (ou grâce à la décomposition de Jordan si celle-ci est maîtrisée). Deux endomorphismes trigonalisables qui commutent sont simultanément trigonalisables, mais une grande proportion de candidats pensent à tort que la réciproque est vraie. Notons que l'étude des nilpotents en dimension 2 débouche naturellement sur des problèmes de quadriques et que l'étude sur un corps fini donne lieu à de jolis problèmes de dénombrement.

Motivation / speech à l'oral Résolution de systèmes X'=AX ; classification

I Endomorphismes trigonalisables et sous espaces stables

Parler aussi de sous espace caractéristiques

I .1 Définition et caractérisation

Définition 133. *Endo trigo*

Proposition I .1. *f trigo sur* $\mathbb{K}$
$\iff$ *il existe* $(e_1, \dots, e_n)$ *base telle que* $(e_1, \dots, e_p)$ *est stable* $\forall p$
$\iff$ *polynôme caractéristique scindé*
$\iff$ *polynôme minimal scindé*
$\iff$ *il existe un polynôme annulateur scindé.*

Corollaire I .2. *Si K algébriquement clos, tout endomorphisme est trigonalisable.*

I .2 Trigonalisation simultanée

Proposition I .3. *Si f et g sont trigonalisables et commutent, alors ils sont trigonalisables dans une même base.*

Rq : hypothèses importantes, donner contre exemples.
On peut généraliser : une famille quelconque d'endomorphismes trigonalisables qui commute est cotrigonalisable.

Proposition I .4. *u, v cotrigonalisables, alors u+v et uv sont trigonalisables*

Donner contre exemples.

Théorème I .5. *Lie Kolchin*

II Décomposition des matrices trigonalisables à l'aide de matrices nilpotentes

II .1 Nilpotence

Définition 134. *Endomorphisme nilpotent*

Rq : Nilp(E) est un cône ; ce n'est ni un idéal de L(E) ni un sous espace vectoriel.

Proposition II .1. *f, g nilpotent et commutent, alors f+g est nilpotent.*
f,g commutent et f nilpotent alors $f \circ g$ nilpotent.

Proposition II .2. *Cardinal du cône nilpotent.*

II .2 Application à la réduction

Noyaux itérés, Jordan

II .3

III Etude approfondie

III .1 Etude du cône nilpotent

Cardinal du cône nilpotent

III .2 Propriétés topologiques

$T_n(R)$= ensemble des matrices trigonalisables

Théorème III .1. *L'ensemble des matrices diagonalisables à vp deux à deux distinctes est dense dans l'ensemble des matrices trigonalisables.*

Proposition III .2. *$T_n(R)$ est fermé dans $M_n(R)$.*

III .3 Exponentielle

bijection nilpotent unipotent par l'exponentielle

LEÇON 158

MATRICES SYMÉTRIQUES RÉELLES, MATRICES HERMITIENNES.

Références Gourdon, Grifone, H2G2, (Rouvière)

Développements

— O(p,q) (H2G2, Serre)

— exp isomorphisme S_n^+ dans S_n^{++} (H2G2)

— gradient pas optimal (Ciarlet)

—

Rapport jury (2015) C'est une leçon transversale. La notion de signature doit bien sûr figurer dans la leçon et on ne doit surtout pas se cantonner au cas des matrices définies positives. L'action du groupe linéaire sur l'espace des matrices symétriques peut donner un cadre naturel à cette leçon. Curieusement,il est fréquent que le candidat énonce l'existence de la signature d'une matrice symétrique réelle sans en énoncer l'unicité dans sa classe de congruence. L'orthogonalisation simultanée est un résultat important de cette leçon. Il faut en connaître les applications géométriques aux quadriques. On doit faire le lien avec les formes quadratiques et les formes hermitiennes. La partie réelle et la partie imaginaire d'un produit hermitien définissent des structures sur l'espace vectoriel réel sous-jacent.

Motivation / speech à l'oral

I Algèbre bilinéaire, sesquilinéaire

I .1 Formes bilinéaires symétriques ou antisymétriques

[H2G2]

Définition 135. *E K-ev.* $b : E \times E \to \mathbb{K}$ *est une forme bilinéaire si pour tout x* $y \mapsto b(x, y)$ *et* $y \mapsto b(y, x)$ *sont linéaires sur E.*

Définition 136. $\psi_b : E \times E^*$ *tel que* $\forall x, y \quad < \psi_b(x), y >= b(x, y)$ *Ici le crochet* $<, >$ *désigne l"évaluation d'une forme linéaire en un vecteur.*

Définition 137.

$$Kerb := Ker\psi_b = \{x \in E, \quad \forall y \ , \ b(x, y) = 0\}$$

b est non dégénérée si Kerb est réduit à $\{0\}$.

$$rgb := dimE - dimKerb$$

Définition 138. *Formes symétriques, antisymétriques*

Proposition I .1. *Une forme bilinéaire s'écrit de manière unique comme somme d'une forme symétrique et antisymétrique.*

$$b(x, y) = \frac{b(x, y) + b(y, x)}{2} + \frac{b(x, y) - b(y, x)}{2}$$

(sauf en caractéristique 2...)

Proposition I .2.

$$M_n(R) = S_n(R) \oplus A_n(R)$$
$$H_n(C) = S_n(R) \oplus A_n(R)$$

I .2 Représentation matricielle des formes quadratiques

Définition 139. *e base, b forme bili ;* $mat(b, e) = (a_{ij})$ *où* $a_{ij} = b(e_i, e_j)$ *est la matrice de b dans e.*

Lemme I .3. *Changement de base ; relation de congruence*

Théorème I .4. *Réduction de Gauss*

Théorème I .5. *Sylvester*

I .3 Forme quadratique définies positives

Définition 140. *q(x)>0 alors matrice est SDP*

II Etude générale

II .1 Réduction

Matrice SDP a toute ses vp strictement positives.

Théorème II .1. *Théorème spectral*

Application : Minima Dérivée seconde (hessienne) est HDP alors extréma local.

II .2 Réduction simultanée

Théorème II .2. *Réduction simultanée*

Application : classification des quadriques dans R sur Rev

II .3 Etude topologique

S_n^{++} est ouvert de S_n
S_n^{+} est un cône convexe d'intérieur S_n^{++}
Racine carré :
$S_n^{++} \to S_n^{++}; A \mapsto A^2$ est homéomorphisme. On peut parler de racine carré pour une matrice SDP.

Proposition II .3. *exp :* $S_n^{+} \to S_n^{++}$ *homéomorphisme*

Théorème II .4. *Décomposition polaire*

Théorème II .5. *Etude O(p,q)*

II .4 Analyse numérique

Gradient à pas optimal ; Gauss Seidel, Choleski (éventuellement)

LEÇON 159

FORMES LINÉAIRES ET DUALITÉ EN DIMENSION FINIE. EXEMPLES ET APPLICATIONS.

Références Schwartz

Développements

- Frobenius
- Théorème de structure des groupes abéliens finis
- Extrémas liés

Rapport jury (2015) Il est important de bien placer la thématique de la dualité dans cette leçon : celle-ci permet de créer une correspondance féconde entre un morphisme et son morphisme transposé, un sous-espace et son orthogonal (canonique), les noyaux et les images, 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. 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 facilement d'obtenir les équations d'un sous-espace vectoriel ou d'exhiber une base d'une intersection d'hyperplans. Cette leçon peut être traitée sous différents aspects : géométrique, algébrique, topologique, analytique, etc. Il faut que les développements proposés soient en lien direct, comme toujours, avec la leçon ; proposer la trigonalisation simultanée est un peu osé ! Enfin rappeler que la différentielle d'une fonction réelle est une forme linéaire semble incontournable.

Motivation / speech à l'oral

I Premiers résultats

I .1 Forme linéaire

Définition 141. *Forme linéaire : application de E dans R. Notation avec le crochet de dualité.*

Exemple : différentielle d'une application différentiable. Evaluation, dérivation en un point, intégration sur un segment.
Dans la suite, E ev dimension finie, E^* l'espace des formes linéaires de E.

I .2 Base duale

Proposition I .1. *E^* est un espace vectoriel de même dimension que E ; de plus, en fixant une base on a un isomorphisme entre E et E^*, donné par la base duale.*

Exemple :

I .3 Hyperplans

Définition 142. *$\phi \in E^*$, H=Ker ϕ.*

dim H = n-1 par théorème du rang.
Exemple : ensemble des matrices de trace nulle ; $\{(x, y, z) : x + y + z = 0\}$

Proposition I .2. *H hyperplan* $\iff$ *dim H=n-1*

Corollaire I .3. $H = Ker\phi_1 = Ker\phi_2 \iff \phi_1, \phi_2$ *sont proportionnelles*

Corollaire I .4. *Équation d'un hyperplan*

I .4 Intersection d'hyperplans

Théorème I .5. *Extrémas liés.*

II Orthogonalité et algèbre bilinéaire

On motive le passage à l'algèbre linéaire par l'orthogonalité.

II .1 Orthogonal

Définition 143.

Proposition II .1. *Prop inclusions de parties orthogonales*

Théorème II .2. *F sev de E,* $\dim F + \dim F^\perp = \dim E$

II .2

II .3

III Construction effectives à partir de la dualité

III .1 Endomorphisme transposé

Définition, représentation matricielle, changement de base dans le dual.

III .2 Existence de suppémentaire stable

Insister sur le lemme qui fait marcher la récurrence dans la réduction de Frobenius, et s'appuie sur la dualité.
Recaser Frobenius.

LEÇON 160

ENDOMORPHISMES REMARQUABLES D'UN ESPACE VECTORIEL EUCLIDIEN (DE DIMENSION FINIE).

Références H2G2 I, Serre, Szpirglas

Développements

— SU(2) SO(3)

— $\exp : S_n \to S_n^{++}$ homéomorphisme

Rapport jury (2015) Dans cette leçon, les candidats doivent bien prendre conscience que le caractère euclidien de l'espace est essentiel pour que l'endomorphisme soit remarquable. Par exemple, des développements comme le lemme des noyaux ou la décomposition de Dunford n'ont rien à faire ici. 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.

Motivation / speech à l'oral

Notations ϕ forme bilinéaire symétrique définie positive. $\phi(x,y) =< x,y >$.
Parler de symétries orthogonales, projection orthogonales.

I Endormorphisme adjoint

I .1 Définition

[Szpirglas]

Définition 144. *Def*

Proposition I .1. *S'il existe, l'adjoint existe toujours.*

Proposition I .2. *En dimension finie, l'adjoint existe*

Démonstration. □

Dans la suite, on est toujours en dimension finie.

Proposition I .3. *Si F stable par u, alors $F^\perp$ stable par u^*.*

Propriétés de bases sur l'adjoint.
Représentation matricielle.

I .2 Endomorphisme normaux

Définition 145. *u est dit normal s'il commute avec son adjoint.*

Exemple : Symétriques, antisymétriques orthogonaux.

I .3 Réduction des endomorphismes normaux

II Matrices symétriques, hermitiennes

Les introduire par les formes quadratiques ?

II .1 Etude générale

Théorème II .1. *Théorème spectral*

Matrice SDP, HDP.
Exemple : la Hessienne est une matrice symétrique.
SDP est un ouvert de S_n, S_n^+ est un cône convexe
Parler de réduction simultanée, classification des quadriques sur R.

II .2 Décomposition polaire et conséquences

Décompo polaire.
Appli : rayon spectral égal à norme 2 (faire pour matrices inversible puis densité de GLn(C) dans Mn(C).
$\exp : S_n \to S_n^{++}$ est homéomorphisme.

III Etude des groupes orthogonaux

III .1 Action de GL_n sur M_n par congrucente

Introduire l'action et les orbites (théorème de Sylvester) et stabilisateur (O(n), O(p,q)).
Recaser le développement sur O(p,q).
Dans C : l'équivalent sont les groupes unitaires (normal car l'orbite sous congruence n'est pas la même...).
Parler de la réduction qui implique l'existence d'une base telle que toute matrice de O(n) s'écrive : $diag(1, \dots, 1, -1, \dots, -1, R_{\theta 1}, \dots$ où les R_θ sont des matrices de rotation.

III .2 Etude topologique

Compacité

Proposition III .1. *$O(n)$ est compact. Corollaire : O(p,q) l'est ssi pq=0.*

Proposition III .2. *exp : $S_n \to S_n^{++}$ homéomorphisme.*

Démonstration. Utilise la décomposition polaire. Pas complètement dans le cadre de la leçon, mais on utilise ce résultat dans la suite. □

Connexité

Proposition III .3. *$GL_n(C)$ est connexe.*
$GL_n(R)$ a deux composantes connexes : GL_n^+ et GL_n^-.

Proposition III .4. *O_n a deux composantes connexes : SO_n et l'autre.*
U_n est connexe.

Démonstration. Pour O_n : union disjointe de SO_n et l'autre. SO_n connexe par arc car on met sous forme normale (diagonale de 1 et de rotations, éventuellement d'angle π (ie on regroupe les -1 2 par 2 ; il y en a un nombre pair car le det vaut 1)). Puis on fait un chemin reliant cette matrice à l'identité.
Puis $O_n^- = MSO_n$ pour n'importe quelle matrice M dans O_n^-.
Pour U_n : on a par décomposition polaire $GL_n(C)$ homéomorphe à $U_n \times H_n^{++}$ et $GL_n(C)$ est connexe. □

Proposition III .5. *O(p,q) a 2 composantes connexes si pq=0, 4 sinon.*
U(p,q) est connexe.

Démonstration. Voir Serre.
Vient du fait que O(p) et O(q) ont 2 composantes connexes sauf dans les cas dégénérés pq=0.
U(p,q) est connexe car U(p) et U(q) le sont toujours.

□

III .3 Cas particulier des petites dimension

Dimension 2

O(2) Rotations etc

SU(2) Réalisation de SU(2) comme la sphère des quaternion pour la norme donnée par le déterminant. Quelques propriétés sur $\mathbb{H}$.

Dimension 3

Lemme III .6. *SO_3 est engendré par les retournements.*

Savoir que c'est vrai en toute dimension, mais la preuve (récurrence) n'est pas triviale. En dimension 3, une preuve expresse (géométrique) convient.

Théorème III .7. *On a l'isomorphisme exceptionnel $SU(2) \approx SO_3/\{+ - I_2\}$*

LEÇON 161

ISOMÉTRIES D'UN ESPACE AFFINE EUCLIDIEN DE DIMENSION FINIE. APPLICATIONS EN DIMENSIONS 2 ET 3.

Référence : Ramis-Warusfel-Moulins, Szpirglas

Motivation : pavage régulier en cristallo ; exemple graphène et NaCl (analogie avec empilement balles de tennis). L'étude complète des pavages (même limité au plan $\mathbb{R}^2$) est trop dure, donc ici on s'arrête juste avant, cad aux groupes d'isométries préservant un partie de R^2 ou R^3 (3ème partie). Avant d'en arriver là, il aura fallu étudier les isométries en détail ; leur prop générales (1ere partie), et les classifier (2eme partie).

I Le groupe des isométries

I .1 Groupe Is(E)

Définition 146. *On appelle isométrie de E toute application f de E dans E qui conserve les distances.*

Remarque : Si f est une application affine, dire que f est une isométrie revient à dire que pour tout couple de points (M,N) de E, $||\vec{f}(\vec{MN})|| = ||\vec{MN}||$, cad $\vec{f}$ conserve la norme, donc est un automorphisme orthogonal. La réciproque est aussi vraie.

Proposition I .1. *Soit $f : E \to E$ application affine. Pour que f soit une isométrie, il faut et suffit que sa partie linéaire $\vec{f}$ soit une translation orthogonale de $\vec{E}$, cad appartienne au groupe $O(\vec{E})$.*

Démonstration. Basée sur le lemme :

Lemme I .2. *$\phi : \vec{E} \to \vec{E}$ application quelconque. Si $\forall (u,v) \in \vec{E}$ $||\phi(\vec{v}) - \phi(\vec{u})|| = ||\vec{v} - \vec{u}||$ et $\phi(\vec{0} = \vec{0})$ alors ϕ est un automorphisme orthogonal.*

□

Lemme I .3. *S partie affinement libre de E ; n=dimE et p=Card S.*

Toute isométrie laissant fixe chaque poit de S peut s'écrire comme composée d'un certain nombre k de réflexions, avec $k \leq n + 1 - p$

Théorème I .4. *Les isométries de E sont exactement les transformations affines de E dont la partie linéaire est une transformation orthogonale de $\vec{E}$. Elles forment donc un sous groupe du groupe affine GA(E), noté Is(E).*

I .2 Déplacements, antidéplacements

Définition 147. *On appelle déplacement noté $Is^+(E)$ (resp. antidéplacement, notés $Is^-(E)$) de E une isométrie dont la partie linéaire est un automorphisme orthogonal de déterminant +1 (resp. -1).*

Proposition I .5. *L'ensemble des déplacements de E est un sous groupe (distingué) du groupe des isométries de E.*

Démonstration. $f \to \det(\vec{f})$ est un morphisme de Is(E) dans $\{-1, 1\}$. So noyau est un sous groupe distingué du sous groupe Is(E). □

Définition 148. *Les déplacements de E ayant un point fixes sont appelés rotations affines de l'espace affine euclidien E.*

I .3 Décomposition en produit de réflexions

Corollaire I .6. *1/ Is(E) est engendré par les réflexions. Plus précisément, toute isométrie de E est la composée d'au plus réflexions.*

2/ Soient f une isométrie de E possédant au moins un point fixe et p la dimension de l'espace des points fixes de f. Alors f est la composée d'au plus n-p réflexions.

Corollaire I .7. *L'action naturelle du groupe Is(E) sur les repères orthonormés est simple et transitive. Soit $k \in \{0, \dots, n\}$. L'action naturelle de Is(E) sur les sous espaces affines de dimension k de E est transitive.*

Proposition I .8. *Prolongement des isométries*

Toute isométrie ϕ d'une partie S de E dans E se prolonge en une isométrie de E.

II Classification des isométries en dimension 2 et 3

II .1 Forme réduite d'une isométrie

Théorème II .1. *Toute isométrie f de E s'écrit de manière unique $f = t_{\vec{u}} \circ g$ où g est une isométrie possédant au moins un point fixe et $\vec{u}$ un vecteur invariant par $\vec{f}$, ce qui revient à dire que g et $t_{\vec{u}}$ commutent.*

Cette décomposition est appelée forme réduite de f.

II .2 En dimension 2

Définition 149. *A point de E, α angle. La rotation de centre A et d'angle α est l'unique isométrie laissant fixe A et dont la partie linéaire est la rotation vectorielle d'angle α.*

Définition 150. *D droite et $\vec{u}$ vecteur non nul directeur de D. On appelle symétrie glissée d'axe D et de vecteur $\vec{u}$ le composé (commutatif) $\sigma := t_{\vec{u}} \circ s_D$*

Théorème II .2. *1/ Les déplacements de E sont les translations et les rotations non triviales.*

2/ Les antidéplacements de E sont les réflexions et les symétries glissées.

Proposition II .3. *D, D' deux droites de E distinctes et $f := s_{D'} \circ s_D$ 1/ Si $D \parallel D'$, $f = 2t_{\vec{u}}$ où $\vec{u}$ est l'unique vecteur de $\vec{D}^{\perp}$ tel que $D' = D + \vec{u}$.*

2/ Si $D \cap D' = \{O\}$ f est la rotation de centre O et d'angle $2\widehat{DD'}$

II .3 En dimension 3

Définition 151.

$$R(\theta) := \begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad S(\theta) := \begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & -1 \end{pmatrix} \tag{161.1}$$

Théorème II .4. *Soit ϕ transformation orthogonale de $\vec{E}$. Il existe un unique réel $\theta \in [0, \pi]$ et une base orthonormée B de $\vec{E}$ tels que la matrice de ϕ dans la base B soit $R(\theta)$ ou $S(\theta)$.*

Définition 152. *Rotations, vissages, symétries glissées, rotations-symétries*

Théorème II .5. *1/ Les déplacements de E sont les translations, rotations et les vissages.*

2/ Les antidéplacements de E sont les réflexions, symétries glissées, et les rotations-symétries.

III Isométries laissant fixe une partie finie du plan ou de l'espace

III .1 D_n

III .2 S4

LEÇON 190

MÉTHODES COMBINATOIRES, PROBLÈMES DE DÉNOMBREMENT.

Référence : De Biasis (Maths pour l'agreg et le capes)
Combes (Algèbre et géométrie)
Il faut dans un premier temps dégager clairement les méthodes et les illustrer d'exemples significatifs. L'utilisation de séries génératrices est un outil puissant pour le calcul de certains cardinaux. Le jury s'attend à ce que les candidats sachent calculer des cardinaux classiques et certaines probabilités ! L'introduction des corps finis (même en se limitant aux cardinaux premiers) permet de créer un lien fécond avec l'algèbre linéaire.

I Méthodes élémentaires

I .1 Les outils de base

Nourdin

Définition 153. *Définition ensemble. Il y a $Card(E)^{card(F)}$ applications de E dans F. Il y a n ! bijections*

I .2 Par un calcul direct

de Biasi p.10
Exo : Calcul du nombre de matchs dans un tournoi simple de tennis à n joueurs engagés (une seul vainqueur, donc n-1 vaincu, et chaque match élimine 1 joueur, donc n-1 matchs).

Définition 154. *E un ensemble à n éléments, $p \leq n$. Un p-arrangement est un p uplet formé d'éléments de E deux à deux distincts.*

Principe de multiplication On énumère les éléments de E en p étapes, chaque étape comportant n_k choix, alors $|E| = n_1 \dots n_p$.

Proposition I .1. *Le nombre de p-arrangement d'un n-ensemble est $A_n^p = n(n-1)\dots(n-p+1) = \frac{n!}{(n-p)!}$*

Démonstration. Par raisonnement direct : n choix pour le premier, n-1 pour le second, etc
Ou par récurrence (lol). □

Exercices :
Tirage de p boules dans une urne en contenant n : ordonné (successif), avec remise (n^p) ou sans remise (A_n^p).
Alphabet braille : 6 points disposés en rectangle, en relief ou non. On a donc $2^6 = 64$ signes différents possible.
Généralisation à l'alphabet chinois ou japonais.

Définition 155. *Une permutation de E est un n-arrangement, où $n = |E|$. Il y en a n !.*

Principe d'addition

Définition 156.

I .3 Par double comptage

Proposition I .2. *Formule du binôme de Newton*

Démonstration. A et B deux parties disjointes ayant a et b éléments.

Le nombre d'applications de E dans $A \bigcup B$ est $(a+b)^n$.

Soit $\mathcal{A}_p$ le nombre des applications telles que p éléments de E aient leurs images dans A, les n-p autres dans B. Les $\mathcal{A}_p$ sont disjoints et $\mathcal{A} = \bigcup_p \mathcal{A}_p$ est l'ensemble des applications de E dans $A \bigcup B$.

Or $A \bigcup B = C_n^p a^p b^{n-p}$ (nombres de façons de choisir p éléments de E)x(nombre d'applications de ces p éléments dans A)x(nombre d'applications des n-p autres éléments dans B).

Rq : preuve par récurrence aussi possible. □

Théorème I .3. *Loi de réciprocité quadratique (un peu osé ici ?)*

Théorème I .4. *Formule de Burnside*

Principe des tiroirs Si n+1 objets sont rangés dans n tiroirs, alors au moins un tiroir contient au moins 2 objets.

Exemple : Dans un groupe de 6 personnes, il y a :

-Au moins 3 personnes qui se connaissent mutuellement.

-Soit 3 personnes qui ne connaissent aucune des deux autres.

I .4 Par estimation

Problèmes de Fermi ; nombres de caractères chinois ?

I .5 En probabilité sur ensemble fini ou dénombrable

Proposition I .5. $P(A) = \frac{CardA}{CardE}$ *(nombre de cas favorable / nombre de cas possible)*

Exo : On jette trois dès, quelle est la proba d'obtenir au moins deux faces portant le même chiffre. Quelle est la proba que la somme des trois chiffres soit paire ?

Mon voisin a deux enfants, dont une fille. Quelle est la proba que l'autre soit un garçon ?

Proposition I .6. *Principe de réflexion pour une chaine de Markov.*

Proposition I .7. *Marche aléatoire en dimension 1. Problème de la ruine du joueur.*

Démonstration. □

Proposition I .8. *Formule de Bayes*

Exo : Un livre contient 4 erreurs. A chaque relecture, une erreur est corrigée avec une proba 1/3. Les relectures étant indépendantes, combien en faut-il pour corriger toutes les erreurs avec proba 0.90 ?

Quelques lois de proba usuelles

II Des fonctions particulières

II .1 Indicatrice d'Euler

[Perrin p.24-25]

Définition 157. *On appelle fonction d'Euler et on note $\phi(n)$ le nombre d'entier x tel que $1 \leq x \leq n$ et x premier avec n.*

Proposition II .1. $\phi(n) = |(\mathbb{Z}/\ltimes Z)^*$

Si $pgcd(m,n) = 1$ alors $\phi(mn) = \phi(n)\phi(m)$ Si p premier, $\phi(p) = p-1$ et $\phi(p^\alpha) = p^{\alpha-1}(p-1)$

Proposition II .2.

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

II .2 Séries génératrices

Définition 158. *Soit (a_n) une suite à valeur dans un anneau intègre, on appelle série génératrice la série formelle :*

$$\phi(t) = \sum a_n t^n$$

Proposition II .3. *Suite de Fibonacci $F_0 = F_1 = 1, F_n = F_{n-1} + f_{n-2}$*
La série génératrice est $\phi(t) = \sum F_n t^n = \frac{1}{1-t-t^2}$, donc $F_n = \frac{\beta^{n+1} - \alpha^{n+1}}{\sqrt{5}}$ $\alpha = \frac{1-\sqrt{5}}{2}$ $\beta = \frac{1+\sqrt{5}}{2}$

Proposition II .4. *Partition entier*

Proposition II .5. *Nombre de Bell*

III Dénombrement sur corps fini

Proposition III .1. *Cardinaux usuels*
$|GL_n(F_q)| = \prod_{i=0}^{n-1}(q^d - q^i)$ *(compter les bases)*
$|SL_n(F_q)| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1})q^{n-1} = N$
$PGL_n(F_q) = |SL_n(F_q)| = N$
$|PSL_n(F_q) = N/d$ *où d=pgcd(n,q-1).*

Proposition III .2 (H2G2 2eme tome p. 217)**.** *Le cardinal du cône nilpotent dans $M_n(F_q)$ vaut $q^{n(n-1)}$.*

Proposition III .3. *Perrin p.113*
$GL_2(F_2) = SL_2(F_2) = PSL_2(F_2) = S_3$
$PGL_2(F_3) = S_4$ *et* $PSL_2(F_3) = A_4$
$PGL_2(F_4) =$??