UGA, Agrégation interne novembre 2019

Groupe linéaire et sous-groupes

Dans toute la feuille on désigne par n entier ≥ 1, K un corps, E un K-espace vectoriel de dimension finie n et u un élément de $\mathrm{GL}(E)$.

A) Les endomorphismes tels que $\mathrm{rg}\,(u-\mathrm{id}_E)=1$, génération de SL, GL et O

Dans cette partie $n \geq 2$ et on étudie les éléments u de $\mathrm{GL}(E)$ qui ne sont pas l'identité, mais admettent cependant un "maximum" de points fixes dans E, cad. un hyperplan. On note donc $H = \mathrm{Ker}\,(u-\mathrm{id}_E)$ cet hyperplan, l une forme linéaire sur E telle que $H = \mathrm{Ker}\,l$, et D la droite vectorielle $\mathrm{Im}\,(u-\mathrm{id}_E)$. Pour un tel endomorphisme, deux cas se présentent, selon que H contient la droite D : on dit alors que u est une *transvection d'hyperplan H et de droite D*, ou qu'il ne la contient pas (cas des dilatations).

Exercice 1 TRANSVECTIONS Soit u un endomorphisme inversible de E tel que $\mathrm{Ker}\,(u-\mathrm{id}_E)=H$ est un hyperplan.

a) Montrer que les propriétés suivantes sont équivalentes :

i) u est une transvection ;

ii) il existe un vecteur non nul a dans $H=\mathrm{Ker}\,l$ tel que pour tout $x\in E$,

$$u(x) = x + l(x)a\,;$$

iii) u n'est pas diagonalisable ;

iv) le polynôme minimal de u est $(X-1)^2$;

v) il existe une base de E dans laquelle u a pour matrice $\begin{pmatrix} 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 1 & 1 \\ 0 & \dots & 0 & 1 \end{pmatrix}$.

b) On suppose que u est une transvection. Montrer que u^{-1}, les gug^{-1} pour $g\in\mathrm{GL}(E)$, ainsi que u^2 si K n'est pas de caractéristique 2, sont aussi des transvections, que l'on précisera avec les notations de 1.ii).

c) On suppose que K est de caractéristique $p>0$. Montrer que toute transvection est d'ordre p (noter que $(X-1)^2$ divise X^p-1).

Exercice 2 DILATATIONS Soit u un endomorphisme inversible de E tel que $\mathrm{Ker}\,(u-\mathrm{id}_E)=H$ est un hyperplan. On dit que u est une *dilatation* de E si $D=\mathrm{Im}\,(u-\mathrm{id}_E)$ n'est *pas* incluse dans H. La droite D qui est stable par u (donc propre pour une valeur propre λ) est alors en somme directe avec H. Voici donc plusieurs caractérisations de cette notion de *dilatation de rapport λ* :

Montrer que les propriétés suivantes sont équivalentes :

i) u est une dilatation de E de rapport λ, (d'hyperplan H et de droite D) ;

ii) on a $\det(u) = \lambda \neq 1$ (cad. $u \notin \mathrm{SL}(E)$) ;

iii) u admet une valeur propre $\lambda \neq 1$ (donc une droite propre D pour λ) et u est diagonalisable ;

iv) il existe une base de E dans laquelle la matrice de u est $diag(1, \ldots, 1, \lambda)$, avec $\lambda \in K^*$, $\lambda \neq 1$.

Notations : Soit $n \geq 2$. Pour i, j distincts dans $\{1, \ldots, n\}$, et $\lambda \in K^*$, on note $T_{ij}(\lambda)$ la matrice, dite de transvection, $I_n + \lambda E_{ij}$, où E_{ij} désigne la matrice $n \times n$ dont le seul coefficient non nul est le coefficient i, j qui vaut 1. Pour $\alpha \in K$ tel que $\alpha \neq 0, 1$ et pour $i \in \{1, \ldots, n\}$, on note $D_i(\alpha)$ la matrice diagonale, dite de dilatation, $I_n + (\alpha - 1)E_{ii}$ de $\mathrm{GL}_n(K)$. Ainsi on a $D_n(\alpha) = diag(1, \ldots, 1, \alpha)$.

Dans l'exercice clé suivant, on utilise le pivot de Gauss pour montrer que les *matrices de transvection* $T_{ij}(\lambda)$, $\lambda \in K^*$, (resp. ces matrices et les *matrices de dilatation* $D_i(\alpha)$), où $\alpha \in K^\times \setminus \{1\}$, engendrent le groupe de matrices $\mathrm{SL}_n(K)$ (resp. $\mathrm{GL}_n(K)$). Au vu des équivalences montrées en A), les endomorphismes associés dans toute base à ces matrices sont resp. des transvections et des dilatations. Ainsi le résultat sur les matrices prouvé ci-dessous montre, en passant aux endomorphismes associés, qu'a fortiori *les transvections engendrent SL*(E)*, resp. les transvections et les dilatations engendrent GL*(E) (voir [Rombaldi] pour un raisonnement direct avec les transvections).

Exercice 4 Soit $A \in \mathrm{GL}_n(K)$.

a) Pour i, j, λ donnés, décrire les opérations élémentaires correspondant à la multiplication à gauche, resp. à droite, de A par $T_{ij}(\lambda)$. Quel est l'effet de la multiplication à gauche de A par $T_{ij}(1)T_{ji}(-1)T_{ij}(1)$?

b) Montrer qu'il existe un produit à gauche de A par au plus deux matrices de transvection dont le coefficient $(1, 1)$ est le "pivot" 1. En déduire qu'il existe un tel produit A' dont la première colonne est ce 1 suivi de $n - 1$ zéros.

c) Montrer qu'en multipliant A' à droite par des matrices de transvection on peut annuler tous les coefficients $(1, j)$ où $j \geq 2$. On aboutit ainsi à une matrice $\begin{pmatrix} 1 & 0 \\ 0 & A_1 \end{pmatrix}$.

d) Conclure qu'il existe des matrices de transvection $U_1, \ldots, U_r$ et $V_1, \ldots, V_s$ telles que $A = U_r \ldots U_1 D_n(\det A) V_1 \ldots V_s$.

e) En déduire que les matrices de transvection engendrent $\mathrm{SL}_n(K)$ et que les matrices de transvection et de dilatation engendrent $\mathrm{GL}_n(K)$.

f) Complément : montrer que si $n = 2$, au plus $r + s = 4$ matrices de transvection suffisent pour écrire A comme en d), et que si $n \geq 3$, au plus $2n - 1$ telles matrices suffisent, dans tous les cas. Conclure que toute matrice de $\mathrm{SL}_n(K)$ est produit d'au plus n^2 matrices de transvection.

g) Expliquer pourquoi cette procédure permet de calculer $\det(A)$ et A^{-1}.

h) Montrer que le centre des groupes $\mathrm{SL}_n(K)$ et $\mathrm{GL}_n(K)$ est le sous-groupe de leurs matrices scalaires λI_n.

Exercice 5 Générateurs du groupe orthogonal On suppose que $K = \mathbb{R}$ et E est euclidien. Le *groupe orthogonal* $\mathrm{O}(E)$ est le groupe des isométries vectorielles de E. Les *réflexions* de E sont des dilatations de rapport -1, ce sont les isométries de E qui ont exactement un hyperplan de points fixes. On rappelle que pour tout sev F de E, E est somme directe de F et de $F^\perp$, et que si Fest stable par une isométrie u, alors $F^\perp$ l'est aussi (preuve ?).

Soit $u \in \mathrm{O}(E)$. On note $F_u = \{x \in E, u(x) = x\}$, et $p_u = n - \dim F_u$.

a) On suppose que $u \neq \mathrm{id}_E$. En considérant x non nul dans $F_u^\perp$ et $y = u(x)$, construire une réflexion s telle que $s \circ u$ est l'identité sur F_u et fixe x. Ainsi $p_{s \circ u} < p_u$.

b) Conclure par récurrence sur p_u que u est la composée d'au plus p_u réflexions.

c) Pour $n = 2, 3$, énumérer les types d'isométries de E et le nombre minimal de réflexions dont elles sont composées.

B) Applications au groupe linéaire

Exercice 6 Connexité

a) Si $K = \mathbb{R}$ ou $\mathbb{C}$, montrer avec l'exercice 4,d) que $\mathrm{SL}_n(K)$ est connexe par arcs.

b) Montrer de même que $\mathrm{GL}_n(\mathbb{C})$ est connexe par arcs.

c) Décrire les composantes connexes de $\mathrm{GL}_n(\mathbb{R})$.

Exercice 7 On suppose que le corps K est infini . Montrer que les matrices inversibles diagonalisables engendrent $\mathrm{GL}_n(K)$ (*indication :* il suffit de considérer les générateurs obtenus dans l'exercice 4 ; alors pour M matrice de transvection, écrire $M = D^{-1}(DM)$ où $D = diag(1, d_2, \ldots, d_n)$, avec $1, d_2, \ldots, d_n$ tous distincts dans K^*).

Exercice 8 application de la diagonalisabilité simultanée
On suppose que K et L sont deux corps de caractéristique différente de 2.

a) Soit G un sous-groupe fini de $\mathrm{GL}(E)$ dont tout élément g vérifie $g^2 = \mathrm{id}_E$. Montrer que G est abélien, puis montrer qu'il existe une base B de E qui diagonalise tous les éléments de G. Conclure que $\mathrm{card}\, G \leq 2^n$.

b) Soit $m \geq 1$ tel qu'il existe un morphisme injectif de $\mathrm{GL}_n(K)$ dans $\mathrm{GL}_m(L)$. Montrer que $n \leq m$.

c) Montrer qu'il n'existe pas d'isomorphisme entre les groupes $\mathrm{GL}_n(\mathbb{Q})$ et $\mathrm{GL}_m(\mathbb{R})$, ni entre les groupes $\mathrm{GL}_n(\mathbb{R})$ et $\mathrm{GL}_m(\mathbb{C})$ (*Indication :* penser aux centres, cf. 4.h)).

Exercice 9 SOUS-GROUPE D'EXPOSANT FINI, UN THÉORÈME DE BURNSIDE

a) Soit $A \in M_n(\mathbb{C})$ telle que $\mathrm{Tr}\,(A^k) = 0$ pour tout k entre 1 et n. Montrer que A est nilpotente (*indication :* considérer la liste de ses valeurs propres avec leur multiplicité).

Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$. Il existe alors $m \geq 1$ et une famille $(M_1, \ldots, M_m)$ dans G^m qui est une base de $\mathrm{Vect}(G)$. On note $f : G \to \mathbb{C}^m$ l'application qui à $A \in G$ associe $(\mathrm{Tr}\,(AM_i))_{1 \leq i \leq m}$.

b) Montrer que si $A, B \in G$ ont même image par f alors $AB^{-1} - I_n$ est nilpotente (*indication :* notant $D = AB^{-1}$, on montrera que pour tout $k \in \mathbb{N}$, $\mathrm{Tr}\,(D^k) = n$).

c) On suppose que toutes les matrices de G sont diagonalisables. Montrer que f est injective.

d) Montrer le *théorème de Burnside :* s'il existe N entier tel que tout A dans G vérifie $A^N = I_n$ (cad. si G est d'exposant fini), alors G est fini.

Exercice 10 PETITS SOUS-GROUPES DE $\mathrm{GL}(E)$ On suppose que $K = \mathbb{C}$ et on munit $\mathcal{L}(E)$ de la norme triple subordonnée à une norme de E. On considère un sous–groupe borné G de $\mathrm{GL}(E)$.

a) Soit $u \in G$. Montrer que les valeurs propres de u sont de module 1.

b) Si u n'est pas diagonalisable, et si $u = d + n$ est sa décomposition de Dunford, justifier qu'il existe $x \in \mathrm{Ker}\, n^2$ tel que $x \notin \mathrm{Ker}\, n$. En considérant $u^p(x)$, où $p \to \infty$, conclure à une absurdité. Par suite u est diagonalisable.

b) On suppose que $G \subset B(\mathrm{id}_E, \sqrt{2})$ (boule ouverte de centre id_E et de rayon $\sqrt{2}$). Montrer que G est réduit à $\{\mathrm{id}_E\}$.

C) si $K = \mathbb{R}$ ou $\mathbb{C}$: densité, sous-groupes compacts

Dans cette partie $K = \mathbb{R}$ ou $\mathbb{C}$. Sur le K-espace vectoriel de dimension finie $\mathcal{L}(E)$, toutes les normes sont équivalentes et définissent la même topologie.

Exercice 11 Montrer que le groupe $\mathrm{GL}(E)$ est ouvert et dense dans $\mathcal{L}(E)$. Pouvez-vous en donner une application ?

Exercice 12 **a)** Montrer que les groupes $\mathrm{O}_n(\mathbb{R})$ et $\mathrm{U}_n(\mathbb{C})$ sont compacts.

On rappelle l'énoncé de la *décomposition polaire* (pour $K = \mathbb{R}$) : toute matrice de $\mathrm{GL}_n(\mathbb{R})$ s'écrit de manière unique comme le produit d'une matrice orthogonale et d'une matrice symétrique définie positive.

b) Utiliser la décomposition polaire et le théorème spectral pour montrer que $\mathrm{O}_n(\mathbb{R})$ est un sous-groupe compact *maximal* de $\mathrm{GL}_n(\mathbb{R})$, cad. qu'il est égal à tout sous-groupe compact qui le contient.

c) Montrer que tout sous-groupe fini G de $\mathrm{GL}_n(K)$ est conjugué à un sous-groupe de $\mathrm{O}_n(\mathbb{R})$ resp. $\mathrm{U}_n(\mathbb{C})$ (selon que $K = \mathbb{R}$ ou $\mathbb{C}$) (*indication :* revenir dans $\mathrm{GL}(E)$ et considérer la moyenne des G-transformés d'un produit scalaire resp. hermitien donné, puis utiliser le résultat 15.d) ou son analogue sur $\mathbb{C}$).

D) (Sous-groupes du) groupe linéaire et action de groupe

Exercice 13 **a)** Le groupe $\mathrm{GL}(E)$ agit naturellement sur E. Cette action est–elle transitive ? Quelles sont ses orbites ? Quel est le stabilisateur d'un vecteur u de E ?

b) Même question pour l'action de $\mathrm{SL}(E)$ et de $\mathrm{O}(E)$, si E est euclidien.

Exercice 14 Dénombrement sur les corps finis
Soit $\mathbb{F}_q$ un corps fini à q éléments (par exemple $\mathbb{Z}/p\mathbb{Z}$ si $q = p$ est premier).

a) Montrer que le groupe $\mathrm{GL}_n(\mathbb{F}_q)$ opère *simplement transitivement* sur l'ensemble $\mathcal{B}$ des bases de $(\mathbb{F}_q)^n$ (cad. : pour toutes bases $B = (e_1, \ldots, e_n)$ et $B' = (e'_1, \ldots, e'_n)$ de $(\mathbb{F}_q)^n$, il existe un unique g dans $\mathrm{GL}_n(\mathbb{F}_q)$ tel que $g(e_i) = e'_i$ pour tout i).

b) En déduire l'ordre du groupe $\mathrm{GL}_n(\mathbb{F}_q)$.

c) Montrer que cet ordre est produit de $q^{n(n-1)/2}$ par un entier premier à q. Exhiber un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_q)$ d'ordre $q^{n(n-1)/2}$ (il s'agit donc d'un *p-sous-groupe de Sylow*, où p est la caractéristique de $\mathbb{F}_q$).

d) Soit $d \leq n$ un entier. En utilisant l'action de $\mathrm{GL}_n(\mathbb{F}_q)$, montrer que le nombre de sous-espaces vectoriels de $(\mathbb{F}_q)^n$ de dimension d est $|\mathrm{GL}_n(\mathbb{F}_q)|/|\mathrm{GL}_d(\mathbb{F}_q)|.|\mathrm{GL}_{n-d}(\mathbb{F}_q)|q^{d(n-d)}$.

Exercice 15 Groupes orthogonaux des différents produits scalaires

On suppose que $K = \mathbb{R}$, et on note PS_E l'ensemble des produits scalaires sur E.

a) Montrer que $\mathrm{GL}(E)$ agit sur PS_E via la formule $(u.b)\,(x, y) = b\big(u^{-1}(x), u^{-1}(y)\big)$, pour tous u dans $\mathrm{GL}(E)$, b dans PS_E, et x, y dans E.

Soient b, b' dans PS_E, et $B = (e_i)_i$, $B' = (e'_i)_i$ des bases de E orthonormées resp. pour b et b'. On note u l'endomorphisme qui envoie B sur B'.

b) Montrer que $u.b = b'$.

Ainsi $\mathrm{GL}(E)$ agit transitivement sur PS_E. On note resp. $\mathrm{O}(b)$ et $\mathrm{O}(b')$ les groupes orthogonaux associés à b et b'.

c) Montrer que ces groupes sont les stabilisateurs de b resp. b' sous l'action de $\mathrm{GL}(E)$.

d) Déduire de b) et c) que *$O(b')$ est le conjugué $u \circ O(b) \circ u^{-1}$.*

Exercice 16 Les groupes $\mathrm{SO}_2(\mathbb{R})$ et $\mathrm{O}_2(\mathbb{R})$ On suppose que $n = 2$ et $K = \mathbb{R}$, et que E est muni d'un produit scalaire.

a) Montrer que le groupe $\mathrm{SO}(E)$ est abélien, isomorphe au groupe $\mathbb{U}$ des nombres complexes de module 1.

b) Montrer que $\mathrm{SO}(E)$ agit simplement transitivement sur la sphère unité de E.

c) Montrer que tout sous-groupe fini de $\mathrm{SO}(E)$ est cyclique, et que $\mathrm{SO}(E)$ contient un unique sous-groupe de chaque cardinal ≥ 1.

d) Décrire les éléments de $\mathrm{SO}(E)$ d'ordre infini.

On note O^- l'ensemble des isométries négatives de E, cad. des symétries orthogonales par rapport à une droite vectorielle (O^- n'est *pas* un sous-groupe).

e) Montrer que si $r \in \mathrm{SO}(E)$ n'est pas $\pm\mathrm{id}_E$, alors r ne commute avec aucun élément s de O^- ; reconnaître l'isométrie $s \circ r \circ s^{-1}$.

f) Soit G un sous-groupe de $\mathrm{O}(E)$ non inclus dans $\mathrm{SO}(E)$, et $s \in G$ une isométrie négative. On note $G^+ = G \cap \mathrm{SO}(E)$. Montrer que G^+ est un sous-groupe d'indice 2 de G, que G est l'union disjointe de G^+ et de $s \circ G^+ = G^+ \circ s$. G est-il abélien ?

g) Donner deux éléments de $\mathrm{O}(E)$ d'ordre 2 dont le composé est d'ordre infini.

Exercice 17 Le groupe $\mathrm{SO}_3(\mathbb{R})$

On suppose que $n = 3$ et $K = \mathbb{R}$, et que E désigne un espace euclidien. Si D est une droite vectorielle de E, on note r_D la rotation d'angle π autour de D (appelée aussi demi–tour). Ainsi, r_D appartient au groupe spécial orthogonal $\mathrm{SO}(E)$ (mais pas $-\mathrm{id}_E$).

1. Quelle est l'isométrie $-r_D$? Montrer avec l'exercice 5 que $\mathrm{SO}(E)$ est engendré par les demi–tours.

2. Montrer que $\mathrm{SO}_3(\mathbb{R})$ est connexe par arcs (utiliser la forme réduite des rotations).

3.a) On note S^2 la sphère unité de E pour la norme euclidienne. L'action de $\mathrm{SO}(E)$ sur S^2 est–elle transitive ? simplement transitive ? fidèle ?

b) Pour D droite vectorielle de E et g dans $\mathrm{SO}(E)$, reconnaître l'isométrie $g \circ r_D \circ g^{-1}$.

c) En déduire que $\mathrm{SO}(E)$ n'est pas abélien, et montrer que son centre est $\{\mathrm{id}_E\}$. À quelle condition deux demi-tours r_D, $r_{D'}$ commutent-ils ?

d) Soit g un élément de $\mathrm{SO}(E)$. Montrer que g est un demi-tour si et seulement s'il existe v dans S tel que $g(v) = -v$.

e) Soit maintenant G un sous–groupe de $\mathrm{SO}(E)$ qui agit transitivement sur S^2. Montrer avec d) que G contient un demi–tour.

f) En déduire avec 3.a),b) que G contient tous les demi–tours. Conclure que $G = \mathrm{SO}(E)$.

E) Exponentielle de matrice et groupe linéaire pour $K = \mathbb{C}$

Ce paragraphe est juste une ébauche, avec quelques suggestions et références

On se donne $A \in M_n(\mathbb{C})$. Rappeler et justifier la définition de $\exp(A) \in M_n(\mathbb{C})$.

une liste de propriétés et résultats :

a) SI A et B commutent dans $M_n(\mathbb{C})$, alors on a $\exp(A)\exp(B) = \exp(A+B) = \exp(B)\exp(A)$.

$\exp(A)$ est inversible d'inverse $\exp(-A)$, et de déterminant $e^{\mathrm{tr}(A)}$.

b) (DUNFORD MULTIPLICATIF) Toute matrice de $\mathrm{GL}_n(\mathbb{C})$ est de manière unique le produit d'une matrice diagonalisable de $\mathrm{GL}_n(\mathbb{C})$ par une matrice *unipotente* (c'est-à-dire dont 1 est l'unique valeur propre) qui commutent.

Si $A = D + N$ est la décomposition de Dunford usuelle de A, la décomposition multiplicative de $\exp(A) \in \mathrm{GL}_n(\mathbb{C})$ est $\exp(D)\exp(N)$.

c) L'exponentielle réalise une bijection des matrices nilpotentes sur les unipotentes [FGN Algèbre 2, 4.24].

Toute matrice de $\mathrm{GL}_n(\mathbb{C})$ est l'exponentielle d'une matrice complexe (c'est faux sur $\mathbb{R}$, même pour les matrices de déterminant > 0) [idem], ou [Skandalis p97].

d) L'application $f_A \colon t \mapsto \exp(tA)$ de $(\mathbb{R}, +)$ dans $\mathrm{GL}_n(\mathbb{C})$ est un morphisme de groupes dérivable, de dérivée $t \mapsto A\exp(tA)$. En particulier son image est un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$, dit *sous-groupe à un paramètre*.

voir [FGN Algèbre 2, 4.26] pour la *réciproque* : tout morphisme continu de $(\mathbb{R}, +)$ dans $\mathrm{GL}_n(\mathbb{C})$ est un tel morphisme f_A.

◊ ◊ ◊