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

Dorian Cacitti-Holland

2020-2021

Références.

1. Algèbre et géométrie de Jean-Etienne Rombaldi
2. Cours d'algèbre de Daniel Perrin
3. Algèbre de Xavier Gourdon
4. Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni
5. L'algèbre discrète de la transformation de Fourier de Gabriel Peyré

Développements.

1. Générateurs de $SL(E)$ et de $GL(E)$
2. Théorèmes de Sylow
3. Réduction dans $O_n(\mathbb{R})$

Table des matières

1 Groupe linéaire d'un espace vectoriel

1.1 Endomorphismes inversibles

(Chapitres 5.1 d'Algèbre et géométrie de Jean-Etienne Rombaldi, IV.0 du Cours d'algèbre de Daniel Perrin et 3.3 d'Algèbre de Xavier Gourdon)

On considère E un espace vectoriel de dimension finie n.

1. Définition : Soit $u \in End(E)$, alors on dit que u est inversible s'il existe $v \in End(E)$ tels que $u \circ v = id_E = v \circ u$, on note $GL(E)$ leur ensemble
2. Exemple : $\lambda id_E \in GL(E)$
3. Proposition : $GL(E)$ est un groupe
4. Exemple : $GL(\mathbb{R}) \simeq \mathbb{R}^*$
5. Théorème : Soit $u \in End(E)$ alors $u \in GL(E)$ si et seulement si $ker(u) = \{0\}$ si et seulement si $Im(u) = E$ si et seulement si $rg(u) = n$ si et seulement si $det(u) \neq 0$ si et seulement si u transforme toute base de E en une base de E si et seulement si u admet un inverse à droite si et seulement si u admet un inverse à gauche
6. Définition : Soit $A \in M_n(K)$, alors on dit que A est inversible s'il existe $B \in M_n(K)$ tel que $AB = I_n = BA$, on note $GL_n(K)$ leur ensemble
7. Proposition : $GL_n(K)$ est un groupe et $GL_n(K) \simeq GL(E)$

1.2 Déterminant et $SL(E)$

(Chapitre 5.2 d'Algèbre et géométrie de Jean-Etienne Rombaldi et IV.1 du Cours d'algèbre de Daniel Perrin)

1. Proposition : $u \in GL(E) \Longleftrightarrow det(u) \in K^*$
2. Corollaire : det est un morphisme de groupes surjectif de $GL(E)$ dans K^*
3. Corollaire : Si E est un $\mathbb{C}$ ou $\mathbb{R}$-espace vectoriel alors $GL(E)$ est un ouvert de $End(E)$, $GL(E)$ est même dense dans $End(E)$
4. Définition : $SL(E) = ker(det)$ est appelé groupe spécial linéaire de E
5. Exemple : $-id_E \in SL(E) \Longleftrightarrow n \in 2\mathbb{Z}$
6. Lemme : Soit G, G' des groupes et $u : G \longrightarrow G'$ un morphisme de groupe alors $ker(u) \triangleleft G$
7. Proposition : $SL(E) \triangleleft GL(E)$
8. Corollaire : $GL(E)/SL(E) \simeq K^*$

2 Etude de $GL(E)$

2.1 Dilatations, homothéties et transvections

(Chapitres 3.2 d'Algèbre de Xavier Gourdon et IV.2 du Cours d'algèbre de Daniel Perrin)

1. Définition : Soit $u \in End(E)$ et $\lambda \in K$, alors on dit que u est une homothétie de rapport λ si $u = \lambda id_E$

2. Proposition : Dans ce cas, $u \in GL(E) \iff \lambda \neq 0$, dans ce cas u^{-1} est l'homothétie de rapport λ^{-1}
3. Proposition : u homothétie si et seulement si u stabilise toutes les droites vectorielles de E
4. Proposition : Soit H hyperplan de E et $u \in GL(E)$ tels que $u_u|H = id_H$, alors $\lambda := det(u) \neq 1$ si et seulement si u admet une valeur propre $\lambda \neq 1$ si et seulement si $Im(u - id_E) \nsubseteq H$ su et seulement s'il existe une base b de E tel que $Mat_b(u) = I_n + \lambda E_{n,n}$
5. Définition : Dans ce cas, on dit que u est une dilatation d'hyperplan $H = ker(u - id_E)$, de droite $D = Im(u - id_E)$ et de rapport λ
6. Corollaire : Deux dilatations de même rapport sont conjugués
7. Proposition : Soit $H = ker(\varphi)$ hyperplan de E et $u \in GL(E) \backslash \{id_E\}$ tels que $u_{|H} = id_H$, alors $det(u) = 1$ si et seulement si u n'est pas diagonalisable si et seulement si $D = Im(u - id_H) \subset H$ si et seulement si $\overline{u} : E/H \longrightarrow E/H = id_{E/H}$ si et seulement s'il existe $a \in H \backslash \{0\}$ tel que $u(x) = x + f(x)a$ si et seulement s'il existe une base b de E telle que $Mat_b(u) = I_n + E_{n-1,n}$
8. Définition : Dans ce cas, on dit que u est une transvection d'hyperplan H et de droite D
9. Proposition : Soit $u \in GL(E) \backslash \{id_E\}$, alors u transvection de droite D si et seulement si $u_D = id_D$ et $\overline{u} = id_{E/D}$
10. Proposition : Soit τ transvection de droite D et d'hyperplan H et $u \in GL(E)$ alors $u \circ \tau \circ u^{-1}$ est une transvection de droite $u(D)$ et d'hyperplan $u(H)$

2.2 Générateurs de $SL(E)$ et $GL(E)$ et applications

(Chapitre IV.2 et IV.3 du Cours d'algèbre de Daniel Perrin)

1. Lemme : Soit $x, y \in E \backslash \{0\}$ alors il existe $u \in GL(E)$ une transvection ou un produit de deux transvections telle que $u(x) = y$
2. Théorème : $SL(E)$ est engendré par les transvections
3. Corollaire : $GL(E)$ est engendré par les transvections et les dilatations
4. Définition : Soit $u, v \in GL(E)$, alors $[u, v] = uvu^{-1}v^{-1}$ est appelé commutateur de $GL(E)$
5. Exemple : Si $u = id_E$ alors $[u, v] = id_E$
6. Définition : On note $D(GL(E))$ le sous-groupe de $GL(E)$ engendré par les commutateurs, et $D(SL(E))$ celui engendré par les commutateurs d'éléments de $SL(E)$
7. Théorème : $D(GL(E)) = SL(E)$ et $D(SL(E)) = SL(E)$ (sauf dans si $n = 2$ et $K = \mathbb{F}_2$ ou $K = \mathbb{F}_3$)
8. Remarque : Quant au centre on a $Z(GL(E))$ est formé des homothéties non nulles et $Z(SL(E))$ des homothéties de rapport λ racine n-ième de l'unité

2.3 Cas des corps finis

(Chapitres IV.5 et I.5 du Cours d'algèbre de Daniel Perrin et 5.6 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

On considère K corps fini de cardinal $q = p^\alpha$

1. Proposition : $|GL(E)| = q^{\frac{n(n-1)}{2}} \prod_{k=1}^{n} (q^k - 1)$
2. Corollaire : $|SL(E)| = \frac{|GL(E)|}{q-1} = \prod_{k=2}^{n} (q^k - 1)$
3. Corollaire : Si $|K| = p$ alors le sous-groupe $T_n^{+1}(K)$ des matrices triangulaires supérieures de diagonale unitaire est un p-sous-groupe de Sylow de $GL_n(K)$
4. Lemme : Soit H un sous-groupe de G et S un p-sous groupe de Sylow de G, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-sous groupe de Sylow de H
5. Application : Théorème de Sylow (premier) : G contient au moins un p-sous groupe de Sylow
6. Théorème de Sylow (second) : Soit H p-sous-groupe de G, alors H est inclus dans un p-sous groupe de Sylow de G, de plus les p-sous groupes de Sylow sont tous conjugués et leur nombre k vérifie $k \mid n, k \equiv 1[p]$
7. Corollaire : Soit S un p-sous groupe de Sylow de G, alors $S \triangleleft G$ si et seulement si S est l'unique p-sous groupe de Sylow de G
8. Exemple : Un groupe d'ordre 63 n'est pas simple

3 Sous-groupe des endomorphismes orthogonaux

3.1 Définitions et propriétés

(Chapitre 22.3 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

On considère E un espace euclidien.

1. Définition : Soit $u \in End(E)$, alors on dit que u est orthogonal si $\langle u(x), u(y) \rangle = \langle x, y \rangle$, et on note $O(E)$ leur ensemble
2. Exemple : Les seules homothéties dans $O(E)$ sont id_E et $-id_E$
3. Théorème : Soit $u \in End(E)$, alors $u \in O(E)$ si et seulement si $\|u(x)\| = \|x\|$
4. Corollaire : Soit $u \in O(E)$, alors $u \in GL(E)$ et $u^* = u^{-1}$
5. Théorème : Soit $u \in End(E)$, alors $u \in O(E)$ si et seulement si u envoie toute base orthonormale de E sur une base orthonormale de E
6. Exemple : Si $dim(E) = 2$, soit $u \in End(E)$ rotation d'angle $\frac{\pi}{2}$, alors $u \in O(E)$
7. Théorème : Soit $(e_i)_{1 \leq i \leq n}$ base orthonormée de E et $u \in End(E)$ tel que $Mat_e(u) = A$, alors $u \in O(E)$ si et seulement si $A^tA = {}^tAA = I_n$
8. Corollaire : Soit $u \in End(E)$, alors $det(u) \in \{-1, 1\}$

3.2 Réduction dans $O(E)$

(Chapitre 22.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Lemme : Soit $u \in O(E)$, alors $Sp(u) \subset \{-1, 1\}$
2. Lemme : Soit $u \in O(E)$, alors il existe des sous-espaces vectoriels $F_1, ..., F_r$ de E deux à deux orthogonaux de dimension 1 ou 2 et stables par u tels que $E = \bigoplus_{i=1}^{r} F_i$
3. Proposition : Soit $u \in O(E)$ et F sous-espace vectoriel de E stable par F, alors $F^\perp$ est stable par u
4. Théorème de réduction des endomorphismes orthogonaux : Soit $u \in O(E)$, alors il existe une base orthonormée e de E telle que $Mat_e(u) = diag(I_p, I_q, R_1, ..., R_r)$ avec $p, q \in [\![1, n]\!], R_i = R(\theta_i), \theta_i \in]0, 2\pi[\setminus \{\pi\}$

3.3 Propriétés topologiques de $O(E)$

(Chapitres 22.3 d'Algèbre et géométrie de Jean-Etienne Rombaldi, II.3 et II.4 de H2G2 de Caldero et Germoni et VI.2 du Cours d'algèbre de Daniel Perrin)

1. Théorème : $O(E)$ est un sous-groupe de $GL(E)$
2. Théorème : $O(E)$ est un compact de $End(E)$
3. Définition : $SO(E) := O(E) \cap SL(E)$
4. Exemple : $SO(\mathbb{R}) = O(\mathbb{R}) \cap GL(\mathbb{R}) = \{id_{\mathbb{R}}\}$
5. Proposition : Les réflexions engendrent $O(E)$ et les renversement engendrent $SO(E)$
6. Proposition : $SO(E)$ est connexe
7. Corollaire : Les composantes connexes de $O(E)$ sont $SO(E)$ et $O^-(E) := O(E) \cap det^{-1}(\{-1\})$
8. Application : $SO_3(\mathbb{R})$ est un groupe simple

4 Représentations et caractères linéaires des groupes finis

4.1 Définitions et résultats importants

(Chapitre 6 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : Une représentation linéaire de G est un couple (ρ, V) avec V un $\mathbb{C}$-espace vectoriel de dimension finie et $\rho : G \longrightarrow GL(V)$ un morphisme de groupes, et un caractère linéaire est une application de la forme $\chi = tr \circ \rho$
2. Exemple : $(1, \mathbb{C})$ est la représentation triviale de G et $\chi_1 = 1$
3. Exemple : La représentation régulière de G est $(\rho_r, \mathbb{C}^n)$ avec $\rho_r(g)(e_k) = e_{gk}$ et $(e_k)_{k \in G}$ base de $\mathbb{C}^n$

4. Définition : On dit que (ρ, V) est une représentation irréductible si les seuls sous-espaces de V invariants par l'action de G sont $\{0\}$ et V
5. Exemple : $(1, \mathbb{C})$ est irréductible et $(\rho_r, \mathbb{C}^n)$ ne l'est pas car $Vect\left(\sum_{k\in G} e_k\right)$ est G-invariant
6. Lemme de Schur : Soit (ρ_1, V_1) et (ρ_2, V_2) deux représentations irréductibles de G, alors si V_1 et V_2 ne sont pas isomorphes alors il n'existe pas de morphismes u de V_1 dans V_2 tels que $u \circ \rho_1(g) = \rho_2(g) \circ u$, et sinon l'espace vectoriel de tels morphismes est de dimension 1
7. Proposition : Un caractère prend les mêmes valeurs dans une classe de conjugaison
8. Théorème de Mashke : Soit (ρ, V) une représentation de G, alors (ρ, V) est somme de sous-représentations irréductibles
9. Théorème : Les caractères irréductibles de G forment une base orthonormée des fonctions centrales muni de $\langle \varphi, \psi \rangle = \frac{1}{|G|}\sum_{g\in G} \overline{\varphi(g)}\psi(g)$, de plus leur nombre est égal au nombre de classes de conjugaison de G
10. Théorème : Un caractère linéaire est irréductible si et seulement si $\langle \chi, \chi \rangle = 1$

4.2 Conséquences sur les caractéristiques des groupes finis

(Chapitres 6 d'Algèbre et géométrie de Jean-Etienne Rombaldi et VIII.2 de L'algèbre discrète de la transformation de Fourier de Gabriel Peyré)

1. Théorème : $|G| = \sum_{k=1}^{p} (dim(V_k))^2$ avec $V_1, ..., V_p$ les représentations des caractéres irréductibles de G
2. Théorème : G est abélien si et seulement si toutes ses caractères irréductibles sont de degré 1
3. Définition : Le noyau d'un caractère χ de degré d est $ker(\chi) = \{g \in G, \chi(g) = d\}$
4. Proposition : Les sous-groupes distingués de G sont des intersections de noyaux de caractères linéaires irréducibles
5. Théorème : La table de caractères de S_4 est donnée en annexe
6. Application : On peut observer en annexe la table de caractères irréductibles de S_4 et en déduire que les sous-groupes distingués de S_4 sont $\{id\}, V_4, A_4, S_4$, et aussi que S_4 n'est pas abélien