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

Refs : [Gou] Gourdon Algèbre. [Per] Perrin Cours d'algèbre.
[OA] Objectif agrégation. [FGN2] ~~Francinou Gianella Nicolas Oraux X-ens~~ algèbre
[H2G2] Caldero Germoni tome 1. [Alm] Alm Théorie des groupes.
[MT] Mneimné Testard, Groupes de Lie classiques.

Devs :
11 Générateurs $Gl(E)$ $Sl(E)$ [Per] [FGN2]
95 Burnside
59 $SO_3(\mathbb{R})$ simple [FGN3]

Cadre : On fixe k un corps (commutatif) et E un k-espace vectoriel de dimension n finie.

I. Le groupe linéaire

1) Généralités

[Gou] 115

Def prop 1 : Soit $f \in \mathcal{L}(E)$, on a équivalence entre (i) f bijective (ii) f injective (iii) f surjective. La fonction f est alors un automorphisme linéaire, on note $Gl(E)$ l'ensemble des automorphismes de E.

Prop 2 : L'ensemble $Gl(E)$ est un groupe pour la composition des applications.

[Per] 95.

Prop 3 : La donnée d'une base B de E induit un isomorphisme entre $Gl(E)$ et $Gl_n(k)$, groupe des inversibles de l'anneau $\mathcal{M}_n(k)$, en fait $Gl(E) = \mathcal{L}(E)^\times$.

Rq 4 : Cet isomorphisme n'est pas canonique, il dépend du choix (arbitraire) de la base B.

Prop 5 : On a, pour $f \in \mathcal{L}(E)$, $f \in Gl(E) \Leftrightarrow \det f \neq 0$. Ce qui n'a plus de sens en dimension infinie. (ex : dérivation formelle des polynômes).

Prop 6 : Pour $f \in \mathcal{L}(E)$, on a équivalence entre
- $f \in Gl(E)$, - $\exists B$ base telle que $f(B)$ base - $\forall B$ base, $f(B)$ base.

Prop def 7 : Le déterminant $\det : Gl(E) \to k^*$ est un morphisme de groupes, on note $Sl(E)$ son noyau (groupe spécial linéaire).
Le choix d'une base donne un isomorphisme entre $Sl(E)$ et $Sl_n(k)$, le groupe des matrices de déterminant 1, on a en fait une suite exacte courte $Sl(E) \hookrightarrow Gl(E) \twoheadrightarrow k^*$.

2) Générateurs.

[Per] 96 97.

Prop def 8 : Soit $H \subseteq E$ un hyperplan, $u \in Gl(E)$ avec $u_{|H} = Id_H$, on a équivalence entre.
(i) $\det u = \lambda \neq 1$ (ii) $\lambda \in Sp(u)$, $E_\lambda = D$ de dim 1 et u est diagonalisable
(iii) $Im\, u - Id \not\subseteq H$ (iv) $\exists B$ base de E dans laquelle $Mat_B(u)$ a la forme (Fig 1)
On dit alors que u est une dilatation d'hyperplan H, de droite D et de rapport λ. Si $\lambda = -1$ et car $k \neq 2$, on dit que u est une réflexion.

Prop def 9 Avec les mêmes notations, on a équivalence entre
(i) $\det u = 1$ (ii) u n'est pas diagonalisable (iii) $D = Im(u - id) \subseteq H$.
i.e. $u \in Sl(E)$ (iv) $\exists a \in H \setminus \{0\}$, $f \in E^* \setminus \{0\}$ (de noyau H), $u(x) = x + a f(x)\ \forall x \in E$.
(v) Il existe une base de E dans laquelle u a pour matrice (Fig 2).
On dit alors que u est une transvection d'hyperplan H et de droite D, on notera $u = u(f, a)$.

[Per] 97 99

Prop 10 : Soit τ une transvection de droite D d'hyperplan H, et $u \in Gl(E)$, alors $u \tau u^{-1}$ est une transvection, de droite $u(D)$ et d'hyperplan $u(H)$.
Ainsi, les transvections sont conjuguées dans $Gl(E)$, pour $n \geq 3$, elles le sont dans $Sl(E)$ (transport par conjugaison).

Théo 11 : Les transvections engendrent $Sl(E)$, et les transvections et dilatations engendrent $Gl(E)$. DVP

II. Sous groupes de $Gl(E)$.

1) Centre et groupe dérivé

[Per] 98 102

Lemme 12 : Soit $u \in Gl(E)$, on a $(\forall x, \exists \lambda \in k \mid u(x) = \lambda x) \Rightarrow (\exists \lambda \mid \forall x, u(x) = \lambda x)$ autrement dit un automorphisme laissant invariant toute droite vectorielle est une homothétie.

Théo 13 : Le centre de $Gl(E)$ est donné par $Z(Gl(E)) = \{\lambda Id \mid \lambda \in k^*\} \simeq k^*$
le centre de $Sl(E)$ est donné par $Z(Sl(E)) = Z(Gl(E)) \cap Sl(E)$, donc constitué des $\lambda Id \in Gl(E)$ où $\lambda \in k^*$ est racine n-ième de l'unité.

Ex 14 : Sur $\mathbb{R}$. $Z(Sl(E)) = \{Id\}$ si n est impair, $\{\pm Id\}$ sinon. Sur $\mathbb{C}$, on a $Z(Sl(E)) \simeq \mathbb{Z}/n\mathbb{Z}$.

Def 15 : Le quotient de $Gl(E)$ (resp $Sl(E)$) par son centre est appelé groupe projectif (resp spécial) linéaire, noté $PGl(E)$ et $PSl(E)$. On note $PGl_n(k)$ et $PSl_n(k)$ les groupes matriciels correspondant.

Théo 16. On a $D(Gl_n(k)) = Sl_n(k)$ sauf dans le cas $n = 2$ et $k = \mathbb{F}_2$
On a $D(Sl_n(k)) = Sl_n(k)$ sauf pour $(n = 2, k = \mathbb{F}_2)$ et $(n = 2, k = \mathbb{F}_3)$.

Théo 17. Le groupe $PSl_n(k)$ est simple, sauf quand $(n = 2, k = \mathbb{F}_2)$ et $(n = 2$ et $k = \mathbb{F}_3)$.

On verra ces cas particuliers dans la partie III.

[OA] 251.

Prop 18 : Soit M un groupe abélien, $n \neq 2$, $k \neq \mathbb{F}_2$, tout morphisme $Gl_n(k) \to M$ se factorise par le déterminant.

Théo 19. Si $k = \mathbb{F}_p$, $\forall u \in Gl(E)$ $\varepsilon(u) = \left(\frac{\det u}{p}\right)$, où u est vu comme permutation de E, et $(\cdot)$ le symbole de Legendre. (Frobenius Zolotarev)

2) Groupe orthogonal.

Ici, on suppose car(k) $\neq 2$.

[Perr] 123 126 Def 20 : Soit f une forme sesquilinéaire sur E, non dégénérée. On appelle isométrie pour f tout endomorphisme $u \in GL(E)$ tel que $f(u(x),u(y)) = f(x,y)$. Si f est symétrique, on note $O(f)$ l'ensemble des isométries. On note $SO(f)$ l'ensemble des isométries de déterminant 1.

Prop 21 : Si f a pour matrice A et u U dans une base de E, alors $u \in O(f)$ si et seulement si ${}^tUAU = A$, on a donc $\det u = \pm 1$.

Prop 22 : Si q est la forme quadratique associée à f, alors $u \in O(f)$ si et seulement si u conserve q : $\forall x \in E$, $q(u(x)) = q(x)$.

Prop 23 : Si $u \in GL(E)$ est tel que $u^2 = Id$, il existe $E = E^+ \oplus E^-$ une décomposition de E telle que $u_{|E^+} = Id_{E^+}$ et $u_{|E^-} = -Id_{E^-}$. Si $E^- \neq \{0\}$, on dit que u est une involution, si $\dim E^- = 1$ (resp 2), on dit que u est une réflexion (resp un renversement).

Prop 24 : Si $u \in GL(E)$ est telle que $u^2 = Id$, E^+ et E^- les espaces associés à u, alors u est une isométrie pour f ssi E^+ et E^- sont orthogonaux.

Prop 25 : Soit $F \subseteq E$ un sous espace non isotrope ($F \cap F^\perp = \{0\}$) et τ_F la symétrie orthogonale par rapport à F, et $u \in O(q)$, alors $u \tau_F u^{-1}$ est la symétrie orthogonale par rapport à $u(F)$, i.e $\tau_{u(F)}$ (transport par conjugaison).

[Perr] 143 Théo 26 : Si f est le produit scalaire usuel sur $\mathbb{R}^n$, alors $O_q \simeq O_n(\mathbb{R})$ est engendré par les réflexions, et $SO(q)$ par les renversements$_{n\geq 3}$ (plus précisément, tout élément en est produit de n éléments au plus).

Théo 27 (Cartan Dieudonné admis) Cette situation est vraie pour q quelconque.

3) Sous groupes finis de GL(E).

[OA] 187 188 Def 28 : Soit $\sigma \in \mathfrak{S}_n$, on pose $u_{\sigma B} \in GL(E)$ l'endomorphisme défini sur une base B de E par $\forall i$, $u_{\sigma B}(e_i) = e_{\sigma(i)}$.
On appelle alors matrice de permutation la matrice P_σ associée à $u_{\sigma B}$ dans la base B. On a ainsi $P_\sigma = (\delta_{i,\sigma(j)})_{i,j \in [\![1,n]\!]}$

Prop 29 : L'application $\sigma \mapsto P_\sigma$ définie de $\mathfrak{S}_n$ dans $GL_n(k)$ est un morphisme de groupes, injectif.

Prop 30 : On a $\det P_\sigma = \varepsilon(\sigma)$.

Théo 31 (Brauer): Si P_σ et P_τ sont conjuguées dans $GL_n(k)$, alors σ et τ sont conjuguées dans $\mathfrak{S}_n$ (la réciproque est évidente). [OA] 205

Prop 32 : Soit G un groupe fini, il existe un morphisme de groupe injectif $G \to GL_n(k)$ pour $n = |G|$. [Perr] 18

App 33 (Sylow) Soit $|G| = mp^\alpha$ où p est premier et $p \nmid m$, alors G admet un sous groupe d'ordre p^α.

Prop 34 : Tout sous groupe fini de $GL_n(k)$ dont tous les éléments sont d'ordre 2 admet pour ordre au maximum 2^n. Ainsi $GL_n(k) \simeq GL_m(k) \Leftrightarrow n = m$. [OA] 205

Théo 35 (Burnside) Tout sous groupe d'exposant fini de $GL_n(\mathbb{C})$ est fini. DVP [FGN2] 195

III. Actions de GL(E) et de ses sous groupes.

1) Action sur les sous espaces de E.

Def 36 : On fait agir $GL(E)$ sur E par $f.x = f(x)$. Et sur l'ensemble des sous espaces vectoriels de même dimension par $f.(V) = f(V)$. [ULm]

Rq 37 : Ces actions sont des actions de groupes transitives.

Prop 38 La restriction à $SL(E)$ de ces actions est encore transitive. De même si E est euclidien, la restriction à $SO(E)$ est transitive.

Def 39 : Soit $n \geq 1$, et $I = (p_1, \dots, p_r)$ une partition de n. On appelle drapeau de type $I = (p_1 \dots p_r)$ toute famille $(F_1, F_2 \dots F_r) = F_I$ de sous espaces vectoriels de k^n telle que $F_1 \subset \dots \subset F_r$ et $\forall k \in [\![1,r]\!]$, $\dim F_k = p_1 + \dots + p_k$. On pose $\mathcal{F}_I$ l'ensemble des drapeaux de type I. [H2G2] 74

Théo 40 : L'action de la def 36 induit une action de $GL_n(k)$ sur $\mathcal{F}_I$, cette action est transitive.

Rq 41 : Dans le cas de $\mathbb{R}$ ou $\mathbb{C}$, on peut en induire une topologie sur F_I.

2) Action de GL(E) et PGL(E) sur P(E).

Def 42 : On sait que k^* agit sur $E \setminus \{0\}$ par multiplication scalaire. Les orbites sous cette action s'identifient aux droites de E, on note $\mathbb{P}(E)$ l'ensemble de ces orbites, l'espace projectif associé à E (on note $\mathbb{P}^n(k) = \mathbb{P}(k^{n+1})$).

Prop 43 L'action $GL(E) \curvearrowright E$ induit une action transitive $GL(E) \curvearrowright \mathbb{P}(E)$, dont le noyau est le centre de $GL(E)$, d'où une action fidèle $PGL(E) \curvearrowright \mathbb{P}(E)$.

On a de même une action de $PSL(E)$ sur $\mathbb{P}(E)$, elle aussi transitive et fidèle.

[Per] 105 106

Dans le cas où $k=\mathbb{F}_q$ ou $q=p^d$, on peut dénombrer les éléments de ces objets

Prop 43 Si $\dim E = n$ on a

- $|\mathbb{P}(E)| = \frac{1}{q-1}(q^n - 1) = \sum_{i=0}^{n} q^i$, en particulier $|\mathbb{P}^1(k)| = q+1$.
- $|Gl_n(k)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})$
- $|Sl_n(k)| = (q^n-1)\dots(q^n-q^{n-2})q^{n-1} = N$
- $|PGl_n(k)| = |Sl_n(k)| = N$
- $|PSl_n(k)| = N/d$ où $d = \mathrm{pgcd}(n, q-1)$.

L'action de $PGl_2(k)$ sur $\mathbb{P}^1(k)$ nous permet de déduire un morphisme $PGl_2(k) \to \mathfrak{S}_{q+1}$, c'est ainsi de prouver le théorème suivant

Théo 44 : On a les isomorphismes exceptionnels de groupes suivants

- $Gl_2(\mathbb{F}_2) \simeq Sl_2(\mathbb{F}_2) \simeq PSl_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$
- $PGl_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ $\quad PSl_2(\mathbb{F}_3) \simeq \mathfrak{U}_4$
- $PGl_2(\mathbb{F}_4) \simeq PSl_2(\mathbb{F}_4) \simeq \mathfrak{U}_5$
- $PGl_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ $\quad PSl_2(\mathbb{F}_5) \simeq \mathfrak{U}_5$.

2) Actions sur les espaces de matrices.

a) Action par translation.

[H2G2] 130

$Gl_n(k)$ agit sur $\mathcal{M}_n(k)$ par multiplication à gauche, les orbites sont en bijection avec les sous espaces de k^n : $A \sim B \Leftrightarrow \mathrm{Ker} A = \mathrm{Ker} B$; et toute matrice est dans l'orbite d'une unique matrice échelonnée.

b) Action par équivalence.

3 7.

Le groupe $Gl_n(k) \times Gl_m(k)$ agit sur $\mathcal{M}_{n,m}(k)$ par $(P,T).M = PMT^{-1}$. Deux matrices ayant la même orbite sont dites équivalentes. On peut définir le rang d'une matrice comme sa classe d'équivalence par cette action.

Prop 45 : On note O_r l'orbite des matrices de rang r, on a alors
$$\overline{O_r} = \bigcup_{k \le r} O_k. \quad \forall r \le \min(n,m).$$

c) Action par conjugaison.

Le groupe $Gl_n(k)$ agit sur $\mathcal{M}_n(k)$ par $P.M := PMP^{-1}$, cette action traduit le changement de bases, la réduction des endomorphismes consiste à trouver des représentants élémentaires des orbites de cette action.

90 100

Théo 46 : Soit $A \in \mathcal{M}_n(\mathbb{C})$, on note O_A l'orbite de A par l'action de $Gl_n(\mathbb{C})$ alors O_A est fermée dans $\mathcal{M}_n(\mathbb{C})$ ssi A est diagonalisable
$\overline{O_A} \ni 0 \Leftrightarrow A$ est nilpotente.

Prop 47 : Soit $B, A \in \mathcal{M}_n(\mathbb{R})$ alors A, B sont semblables dans $\mathcal{M}_n(\mathbb{C})$ ssi elles le sont dans $\mathcal{M}_n(\mathbb{R})$.

[H2G2] 108, 18

Théo 48 (Décomposition de Frobenius). On revient sur k arbitraire, Soit $u \in \mathcal{L}(E)$, il existe une unique suite de polynômes unitaires non constants $F_1, \dots, F_s \in k[X]$ avec

- $F_s | F_{s-1} | \dots | F_1$
- $\exists \mathcal{B}$ base de E telle que la matrice de u soit diagonale par blocs (et les blocs sont les compagnons des F_i).

d) Action par congruence. Ici $k = \mathbb{R}$ et E est euclidien,

Le groupe $Gl_n(k)$ agit sur $S_n(\mathbb{R})$ par ${}^tPAP = P.A$. C'est le changement de base pour les formes quadratiques.

Théo 49 (Sylvester). Les orbites sont les couples d'entiers de somme $\le n$, c'est la signature des formes quadratiques.

Théo 50 : Toute matrice de $S_n(\mathbb{R})$ est équivalente à une diagonale dans $O_n(\mathbb{R})$, c'est la pseudo réduction simultanée.

IV. Éléments de topologie.

On se place dans $k = \mathbb{R}$ ou $\mathbb{C}$, $\mathcal{M}_n(k)$ est muni d'une norme quelconque

[MT] 11-34

1) Densité.

Prop 51 : L'ensemble $Gl_n(k)$ est dense dans $\mathcal{M}_n(k)$.

Appli 52 : $\forall A, B \in \mathcal{M}_n(k)$, $\chi_{AB} = \chi_{BA}$, en particulier $\mathrm{tr}(BA) = \mathrm{tr}(AB)$.

Appli 53 : Il existe une base de $\mathcal{M}_n(k)$ formée de matrices de rang p $(1 \le p \le n)$.

2) Connexité.

Prop 54 : L'ensemble $Gl_n(\mathbb{C})$ est connexe dans $\mathcal{M}_n(\mathbb{C})$, cependant $Gl_n(\mathbb{R})$ n'est pas connexe et a deux composantes connexes ($Gl_n^+(\mathbb{R})$ et $Gl_n^-(\mathbb{R})$).

Prop 55 : Les ensembles $Sl_n(\mathbb{C})$ et $Sl_n(\mathbb{R})$ sont connexes dans $\mathcal{M}_n(\mathbb{C})$, $\mathcal{M}_n(\mathbb{R})$.

Prop 56 : $SO_n(\mathbb{R})$ est connexe par arcs et $O_n(\mathbb{R})$ a deux composantes connexes homéomorphes.

3) Compacité.

Prop 57 : Le groupe $O_n(\mathbb{R})$ est compact

Appli 58 : La décomposition polaire $(O,S) \mapsto OS$ induit un homéomorphisme entre $S_n^{++} \times O_n(\mathbb{R})$ et $Gl_n(\mathbb{R})$

[FGN3] 67

Théo 59 : Le groupe $SO_3(\mathbb{R})$ est simple. DVP