P. Maurer
ENS Rennes

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

Devs :

- Décomposition de Bruhat
- Morphismes de $\mathbb{S}^1$ vers $\mathrm{GL}_n(\mathbb{R})$

Références :

- Perrin, Cours d'algèbre
- Gourdon, Algèbre
- Caldero, H2G2
- FGN, Oraux X-ENS Algèbre 3
- Zavidovique, Un max de maths
- BMP, Objectif Agreg
- Rouvière, Petit guide de calcul différentiel

Dans tout ce qui suit, E est un espace vectoriel de dimension finie $n \in \mathbb{N}$ sur un corps commutatif k.

1 Généralités sur le groupe linéaire

1.1 Le groupe $(\mathrm{GL}(E), \circ)$

Proposition 1. *Soit $f \in \mathcal{L}(E)$ un endomorphisme. Les propositions suivantes sont équivalentes*

- *f est surjective,*
- $\mathrm{Ker}(f) = \{0\}$,
- *f est un isomorphisme,*
- *Pour toute base $\mathcal{B} = (e_1, \ldots, e_n)$ de E, la famille $\mathcal{B}' = (f(e_1), \ldots, f(e_n))$ est une base de E.*

Définition 2. *Si les conditions de la proposition 1 sont réunies, on dit que f est un automorphisme de E. On note $\mathrm{GL}(E)$ l'ensemble des automorphismes de E et on l'appelle groupe linéaire de E.*

Proposition 3. *L'ensemble $\mathrm{GL}(E)$ muni de la loi de composition $\circ$ est un groupe.*

Remarque 4. La donnée d'une base de E définit un isomorphisme de $\mathrm{GL}(E)$ vers le groupe $(\mathrm{GL}_n(k), \times)$ des matrices $n \times n$ inversibles, à coefficients dans k. Celui ci n'est toutefois pas canonique et dépend du choix de la base en question.

Proposition 5. *Pour $f \in \mathcal{L}(E)$, on a $f \in \mathrm{GL}(E) \Longleftrightarrow \det(f) \neq 0$.*

Proposition 6. *L'application déterminant est un morphisme de groupes entre $(\mathrm{GL}(E), \circ)$ et $(k^*, \times)$. Son noyau est appelé groupe spécial linéaire et est noté $\mathrm{SL}(E)$. Il est isomorphe au groupe $\mathrm{SL}_n(k)$ des matrices de déterminant 1.*

1.2 Transvections et dilatations

Proposition 7. *Soit H un hyperplan de E et $u \in \mathrm{GL}(E)$ tel que $u_{|H} = \mathrm{Id}_H$. Les conditions suivantes sont équivalentes :*

- *On a $\det(u) = \alpha \neq 1$ (i.e $u \notin \mathrm{SL}(E)$).*
- *L'endomorphisme u amdet une valeur propre $\alpha \neq 1$ et u est diagonalisable.*
- *On a $D = \mathrm{Im}(u - \mathrm{Id}_E) \notin H$.*
- *Dans une base convenable, u a pour matrice $D_i(\alpha) = I_n + (\alpha - 1) E_{ii}$ avec $i \in [\![1, n]\!]$ et $\alpha \neq 1$.*

On dit qu'un tel endomorphisme u est une dilatation d'hyperplan H, de droite D, et de paramètre α. La matrice $D_i(\alpha)$ est appelée une matrice de dilatation.

Proposition 8. *Soit H un hyperplan de E, et $f \in E^*$ tel que $H = \mathrm{Ker}(f)$. Soit $u \in \mathrm{GL}(E)$ tel que $u \neq \mathrm{Id}_E$ et $u_{|H} = \mathrm{Id}_H$. Les conditions suivantes sont équivalentes :*

- *On a $\det(u) = 1$ (i.e $u \in \mathrm{SL}(E)$).*
- *L'endomorphisme u n'est pas diagonalisable.*
- *On a $D = \mathrm{Im}(u - \mathrm{Id}) \subset H$.*
- *Il existe $a \in H$ non nul tel que $\forall x \in E$ $u(x) = x + f(x)\, a$,*
- *Dans une base convenable, u a pour matrice $T_{ij}(\lambda) = I_n + \lambda E_{ij}$ avec $\lambda \in k$ et i, $j \in [\![1, n]\!]$.*

On dit qu'un tel endomorphisme u est une transvection d'hyperplan H et de droite D. La matrice $T_{ij}(\lambda)$ est appelé une matrice de transvection.

Proposition 9. *Deux dilatations sont conjuguées dans $\mathrm{GL}(E)$ si et seulement si elles ont le même rapport.*

Proposition 10. *Soit τ une transvection de droite D et d'hyperplan H. Alors $u \tau u^{-1}$ est une transvection de droite $u(D)$ et d'hyperplan $u(H)$. Les transvections sont ainsi conjuguées dans $\mathrm{GL}(E)$.*

Théorème 11. *Les transvections engendrent* $\mathrm{SL}(E)$*.*

Corollaire 12. *Les transvections et les dilatations engendrent* $\mathrm{GL}(E)$*.*

1.3 Quelques calculs de cardinaux

Définition 13. *Pour* $n \in \mathbb{N}$*, on note* $U_n(k)$ *l'ensemble des matrices triangulaires supérieures dont les coefficients diagonaux sont tous égaux à 1. C'est un sous-groupe de* $\mathrm{GL}_n(k)$*.*

Proposition 14. *Soit* p *un nombre premier et* $n \in \mathbb{N}$*. Alors on a :*

- $|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1) \cdots (p^n - p^{n-1}) = m p^{\frac{n(n-1)}{2}}$,
- $|\mathrm{SL}_n(\mathbb{F}_p)| = (p^n - 1) \cdots (p^n - p^{n-2}) \cdot p^{n-1}$,
- $|U_n(\mathbb{F}_p)| = p^{\frac{n(n-1)}{2}}$.

Où $m = (p-1) \cdots (p^n - 1)$ *est premier avec* p*.*

Proposition 15.
Le nombre de matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$ *est :*

$$\sum_{n_1 + \cdots + n_q = n} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\mathrm{GL}_{n_i}(\mathbb{F}_q)|}$$

2 Sous-groupes de GL(E)

2.1 Centre, groupe dérivé et groupes projectifs

Proposition 16. *Soit* $u \in \mathrm{GL}(E)$*. Si* u *laisse invariantes toutes les droites vectorielles de* E*, alors* u *est une homotéthie.*

Corollaire 17. *Le centre* Z *de* $\mathrm{GL}(E)$ *est formé des homothéties* $x \mapsto \lambda x$*, avec* $\lambda \in k^*$*. Il est donc isomorphe à* k^**.*

Le centre de $\mathrm{SL}(E)$ *est* $Z \cap \mathrm{SL}(E)$*, il est isomorphe à* $\mu_n(k) = \{\lambda \in k : \lambda^n = 1\}$*.*

Définition 18. *On appelle groupe projectif linéaire, et on note* $\mathrm{PGL}(E)$*, le quotient de* $\mathrm{GL}(E)$ *par son centre* Z*. De même, le quotient de* $\mathrm{SL}(E)$ *par son centre est noté* $\mathrm{PSL}(E)$*.*

Proposition 19. *Si* k *est algébriquement clos, on a un isomorphisme* $\mathrm{PSL}(E) \simeq \mathrm{PGL}(E)$*.*

Théorème 20. *Rappelons que pour un groupe* G*, on note* $D(G)$ *le groupe dérivé de* G*, qui est engendré par les commutateurs* $[x,y] = xyx^{-1}y^{-1}$*, pour tout* $x, y \in G$*. On a alors :*

- $D(\mathrm{GL}_n(k)) = \mathrm{SL}_n(k)$ *sauf pour le cas* $(n = 2$ *et* $k = \mathbb{F}_2)$*,*
- $D(\mathrm{SL}_n(k)) = \mathrm{SL}_n(k)$ *sauf dans les deux cas* $(n = 2$ *et* $k = \mathbb{F}_2)$ *et* $(n = 2$ *et* $k = \mathbb{F}_3)$*.*

Théorème 21. *Le groupe* $\mathrm{PSL}_n(k)$ *est simple sauf dans les deux cas* $(n = 2$ *et* $k = \mathbb{F}_2)$ *et* $(n = 2$ *et* $k = \mathbb{F}_3)$*.*

Théorème 22. *(isomorphismes exceptionnels)*
On a les isomorphismes suivants :

- $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathcal{S}_3$,
- $\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathcal{S}_4$ *et* $\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathcal{A}_4$,
- $\mathrm{PGL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4) \simeq \mathcal{A}_5$,
- $\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathcal{S}_5$ *et* $\mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathcal{A}_5$.

2.2 Groupe orthogonal

Dans cette partie, on se donne f une forme sesquilinéaire sur E, non dégénérée.

Définition 23. *On appelle isométries de* E *(relativement à* f*) les automorphismes* $u \in \mathrm{GL}(E)$ *qui vérifient* $\forall x, y \in E \quad f(u(x), u(y)) = f(x, y)$*.*

Si f *est symétrique, on note* $O(f)$ *le groupe orthogonal : c'est l'ensemble des isométries de* E *relativement à* f*. On note* $\mathrm{SO}(f) = O(f) \cap \mathrm{SL}(E)$ *le groupe spécial orthogonal.*

Remarque 24. Si $u \in O(f)$, alors $\det(u) \in \{-1, 1\}$.

Notation 25. *On note aussi* $O^+(f) := \mathrm{SO}(f)$*, et* $O^-(f) := O(f) \setminus \mathrm{SO}(f)$ *l'ensemble des isométries de déterminant* -1*.*

Proposition 26. *Si* f *est symétrique (resp. hermitienne), et si* $\mathrm{car}(k) \neq 2$*, un élément* $u \in \mathrm{GL}(E)$ *est une isométrie si et seulement si il conserve la forme quadratique* q *attachée à* f*, i.e si on a*

$$\forall x \in E \quad q(u(x)) = q(x).$$

Dans la suite, on suppose que f est symétrique et que $\mathrm{car}(k) \neq 2$.

Proposition 27. *Soit* $u \in \mathrm{GL}(E)$ *avec* $u^2 = \mathrm{Id}$*, et soient* E^+ *et* E^- *les sous-espaces associés à* u*. Alors* u *est une isométrie si et seulement si* E^+ *et* E^- *sont orthogonaux.*

Remarque 28. Si $k = \mathbb{R}$ et si f désigne le produit scalaire usuel sur $E = \mathbb{R}^n$, alors on note $O_n(\mathbb{R})$ l'espace des matrices orthogonales, et $\mathrm{SO}_n(\mathbb{R})$ l'espace des matrices orthogonales de déterminant 1. Notons que dans ce cas, on a $A \in O_n(\mathbb{R}) \Longleftrightarrow {}^t A A = I_n$.

Théorème 29. *(Réduction des isométries)*

On suppose encore $k=\mathbb{R}$, $E=\mathbb{R}^n$ et f désigne le produit scalaire usuel.

Soit u un endomorphisme orthogonal. Il existe une base orthonormale dans laquelle la matrice de u est :

$$\begin{pmatrix} R(\theta_1) & & & & & \\ & \ddots & & & (0) & \\ & & R(\theta_r) & & & \\ & & & \varepsilon_1 & & \\ & (0) & & & \ddots & \\ & & & & & \varepsilon_s \end{pmatrix}$$

Où $R(\theta_i)=\begin{pmatrix} \cos(\theta_i) & -\sin(\theta_i) \\ \sin(\theta_i) & \cos(\theta_i) \end{pmatrix}$ *et $\varepsilon_i\in\{-1,1\}$, avec $\theta_i\in\mathbb{R}$ et $\theta_i\not\equiv 0\,[\pi]$.*

2.3 Sous-groupes finis et matrices de permutations

Définition 30. *Soit $(e_1,\dots,e_n)$ la base canonique de k^n. Pour $\sigma\in\mathcal{S}_n$, on note w_σ l'application linéaire donnée par $w_\sigma(e_i)=e_{\sigma(i)}$ pour tout $i\in[\![1,n]\!]$.*

Proposition 31. *L'application $w\colon\sigma\mapsto w_\sigma$ est un morphisme de groupes injectif de $\mathcal{S}_n$ dans $\mathrm{GL}_n(k)$.*

Théorème 32. *(Cayley)*

Soit G un groupe fini d'ordre $n\in\mathbb{N}$. Alors il existe un morphisme de groupes injectif $G\to\mathcal{S}(G)\simeq\mathcal{S}_n$.

Corollaire 33. *Si G est un groupe fini d'ordre $n\in\mathbb{N}$, alors on a un morphisme injectif*

$$G\to\mathcal{S}(G)\simeq\mathcal{S}_n\to\mathrm{GL}_n(k).$$

En notant $\varphi\colon G\to\mathrm{GL}_n(k)$ ce morphisme, on en déduit que $\varphi(G)$ est un sous-groupe de $\mathrm{GL}_n(k)$ d'ordre n.

Proposition 34. *Soit G un p-groupe agissant sur un ensemble X. On considère l'ensemble des points fixes de X pour cette action $X^G:=\{x\in X\ :\ \forall g\in G\quad gx=x\}$. Alors on a l'égalité :*

$$|X|\equiv|X^G|\ [p]$$

Définition 35. *Soit G un groupe d'ordre $p^\alpha m$ avec $p\nmid m$. On dit que $H<G$ est un p-Sylow de G si c'est un sous-groupe d'ordre p^α.*

Théorème 36. ***(Sylow)***

Soit G un groupe d'ordre $p^\alpha m$ avec $p\nmid m$. Alors :

1. *G possède au moins un p-Sylow.*
2. *Les p-Sylow sont tous conjugués entre eux.*
3. *En notant k le nombre de p-Sylow, on a $k\equiv 1\,(\mathrm{mod}\,p)$ et k divise m.*

3 Actions et topologie du groupe linéaire

3.1 Drapeaux et décomposition de Bruhat

Définition 37. *On appelle drapeau de k^n toute suite $(0=F_0\subset\cdots\subset F_n)$ de sous-espaces vectoriels de k^n telles que les inclusions soient strictes. Si de plus $\dim(F_i)=i$, on dit que le drapeau est complet. On note Drap l'ensemble des drapeaux complets de k^n.*

Notation 38. *On appelle drapeau complet canonique le drapeau $C:=\{0\}\subset\mathrm{Vect}(e_1)\subset\cdots\subset\mathrm{Vect}(e_1,\dots,e_n)$, où $(e_1,\dots,e_n)$ désigne la base canonique de k^n.*

Définition 39. *On note $B_n(k)$ l'ensemble des matrices triangulaires inversibles de $\mathrm{GL}_n(k)$.*

Proposition 40. *$B_n(k)$ est le stabilisateur de C pour l'action de $\mathrm{GL}_n(k)$ sur Drap. En particulier, c'est un sous-groupe de $\mathrm{GL}_n(k)$.*

Développement 1 :

Théorème 41. ***(Bruhat)***

En notant, pour $\sigma\in\mathcal{S}_n$, $B_n(\mathbb{K})\,w_\sigma\,B_n(\mathbb{K}):=\{tw_\sigma s\ :\ t,s\in B_n(\mathbb{K})\}$, on a la décomposition :

$$\mathrm{GL}_n(\mathbb{K})=\bigsqcup_{\sigma\in\mathcal{S}_n}B_n(\mathbb{K})\,w_\sigma\,B_n(\mathbb{K})$$

Corollaire 42. $\mathrm{GL}_n(\mathbb{K})$ *agit sur* $\mathrm{Drap}\times\mathrm{Drap}$ *et l'action possède $n!$ orbites.*

3.2 Actions de GL(E) sur les espaces de matrice

Proposition 43. *(Théorème du rang)*

$\mathrm{GL}_n(k)\times\mathrm{GL}_m(k)$ agit sur $\mathcal{M}_{n,m}(k)$ par équivalence, via :

$$\cdot\left\{\begin{array}{lcl}(\mathrm{GL}_n(k)\times\mathrm{GL}_m(k))\times\mathcal{M}_{n,m}(k) & \to & \mathcal{M}_{n,m}(k)\\ ((P,Q),M) & \mapsto & PMQ^{-1}\end{array}\right.$$

Chaque orbite pour cette action contient un représentant de la forme :

$$\begin{pmatrix} I_k & 0 \\ 0 & 0 \end{pmatrix}$$

L'entier k est appelé le rang de chaque matrice de l'orbite.

Proposition 44. $\mathrm{GL}_n(k)$ *agit sur* $\mathcal{M}_n(k)$ *par similitude, via :*

$$\cdot \begin{cases} \mathrm{GL}_n(k) \times \mathcal{M}_n(k) & \to & \mathcal{M}_n(k) \\ (P, M) & \mapsto & P^{-1}MP \end{cases}$$

Deux matrices sont dans la même orbite pour cette action si et seulement si elles sont semblables.

Théorème 45. *Soit* $m, n \in \mathbb{N}$. *On considère l'action de* $\mathrm{GL}_n(\mathbb{K})$ *par multiplication à gauche sur l'espace* $\mathcal{M}_n(\mathbb{K})$. *Alors :*

- *Deux matrices* A *et* A' *de* $\mathcal{M}_n(\mathbb{K})$ *ont la même orbite si et seulement si elles ont le même noyau.*
- *Toute matrice est dans l'orbite d'une unique matrice échelonnée en ligne réduite : on a la réunion disjoints suivante :*

$$\bigcup_{E \in \mathcal{E}_n} \mathrm{GL}_n(\mathbb{K}) \cdot E$$

Où $\mathcal{E}_n$ *désigne l'ensemble des matrices échelonnées réduites de taille* $n \times n$.

Remarque 46. Le théorème précédent se démontre via l'algorithme du pivot de Gauss. Partant d'une matrice $A \in \mathcal{M}_n(\mathbb{K})$, on la multiplie à gauche par des matrices élémentaires pour obtenir une matrice d'abord échelonnée en lignes, puis échelonnée en lignes réduite en annulant les coefficients éventuels au-dessus des pivots. On trouve alors P inversible telle que PA soit échelonnée réduite.

Théorème 47. *(Spectral)*

Le groupe orthogonal $\mathcal{O}_n(\mathbb{R})$ *agit sur l'ensemble des matrices symétriques réelles* $\mathcal{S}_n(\mathbb{R})$ *par similitude, et chaque orbite contient une matrice diagonale. Ces orbites sont caractérisées par les valeurs propres (comptées avec multiplicité) des matrices qui les composent.*

Théorème 48. *(Sylvester)*

$\mathrm{GL}_n(\mathbb{R})$ *agit sur* $\mathcal{S}_n(\mathbb{R})$ *par congruence, via :*

$$\cdot \begin{cases} \mathrm{GL}_n(\mathbb{R}) \times \mathcal{S}_n(\mathbb{R}) & \to & \mathcal{S}_n(\mathbb{R}) \\ (P, M) & \mapsto & {}^tPMP \end{cases}$$

Chaque orbite contient un représentant de la forme :

$$\begin{pmatrix} I_p & & \\ & I_q & \\ & & 0_{n-r} \end{pmatrix}$$

Où $r = p + q$ *est le rang des matrices de cette orbite. Le couple* (p, q) *est appelé la signature.*

3.3 Elements de topologie de $\mathrm{GL}(E)$

Proposition 49. $\mathrm{GL}_n(k)$ *est un ouvert dense de* $M_n(k)$.

Application 50. L'application det est différentiable sur $M_n(k)$, de différentielle $D_A \det(H) = \mathrm{Tr}(\mathrm{Com}(A^T) \cdot H)$.

Développement 2 :

Théorème 51. *Soit* $\varphi: (\mathcal{S}^1, \times) \to (\mathrm{GL}_n(\mathbb{R}), \times)$ *un morphisme de groupes continu. Il existe* $Q \in \mathrm{GL}_n(\mathbb{R})$, $r \in \mathbb{N}$, $k_1, \ldots, k_r \in \mathbb{Z}^*$ *tels que :*

$$\forall t \in \mathbb{R} \quad \varphi(e^{it}) = Q \begin{pmatrix} R_{tk_1} & & & & & \\ & \ddots & & & & \\ & & R_{tk_1} & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix} Q^{-1}$$

Où les matrices R_{tk_i} *sont des matrices de rotation :* $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ *pour* $\theta \in \mathbb{R}$.

Proposition 52. $\mathrm{GL}_n(\mathbb{C})$ *est connexe.* $O_n(\mathbb{R})$ *et* $\mathrm{GL}_n(\mathbb{R})$ *ont deux composantes connexes.*

Proposition 53. $O_n(\mathbb{R})$ *et* $\mathrm{SO}_n(\mathbb{R})$ *sont compacts.*

Lemme 54. *Soit* $G \subset \mathrm{SO}_3(\mathbb{R})$ *un sous-groupe distingué et connexe par arcs, non réduit à* $\{I_3\}$. *Alors* $G = \mathrm{SO}_3(\mathbb{R})$.

Corollaire 55. $\mathrm{SO}_3(\mathbb{R})$ *est simple.*

Proposition 56. *Soit* $A \in M_n(\mathbb{C})$. *Alors* $\mathbb{C}[A]^\times$ *est un ouvert connexe dans* $\mathbb{C}[A]$

Corollaire 57. *L'exponentielle de matrices* $\exp: \mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ *est surjective.*