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

Soit $\mathbb{K}$ un corps et E un $\mathbb{K}$-ev de dimension finie $n \in \mathbb{N}^*$.

I Groupe linéaire d'un espace vectoriel.

A Endomorphismes inversibles Rom 5.1

Définition 1 : On note $GL(E)$ le groupe des automorphismes de E et $GL_n(\mathbb{K})$ le groupe des matrices inversibles de $M_n(\mathbb{K})$.

Exemple 2 : Une homothétie est dans $GL(E)$.

Proposition 3 : Le choix d'une base de E permet de réaliser un isomorphisme d'algèbres de $\mathcal{L}(E)$ sur $M_n(\mathbb{K})$ qui induit un isomorphisme de groupes de $GL(E)$ sur $GL_n(\mathbb{K})$.

Théorème 4 : Soit $u \in \mathcal{L}(E)$. On a équivalence entre :

i) $u \in GL(E)$	v) $\det u \neq 0$
ii) $\ker u = \{0\}$	vi) u transforme toute base en une base
iii) $\mathrm{im}\, u = E$	vii) u admet un inverse à droite
iv) $\mathrm{rg}\, u = n$	viii) u admet un inverse à gauche.

B Déterminant et groupe spécial linéaire Rom 5.2

Définition 5 : Le groupe spécial linéaire est $SL(E) = \{u \in \mathcal{L}(E), \det u = 1\}$ et $SL_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}), \det A = 1\}$.

Proposition 6 : L'application det est un morphisme de groupes surjectif de $GL(E)$ sur $\mathbb{K}^*$.

Théorème 7 : $SL(E)$ est un sous-groupe distingué de $GL(E)$ isomorphe à $SL_n(\mathbb{K})$. Le groupe quotient $GL(E)/SL(E)$ est isomorphe à $\mathbb{K}^*$ et on a la suite exacte :

$$\{id\} \longrightarrow SL(E) \xrightarrow{i} GL(E) \xrightarrow{\det} \mathbb{K}^* \longrightarrow \{id\}$$

où i est l'injection canonique de $SL(E)$ dans $GL(E)$. $\mathrm{im}\, i = \ker p$

Exemple 8 : $-id_E \in SL(E) \iff \dim E \in 2\mathbb{Z}$, $id_E \in SL(E)$.

II Etude de GL(E)

A Dilatations, homothéties et transvections X.G 3.2.3 Per 4.2

Définition 9 : On dit que $u \in \mathcal{L}(E)$ est une homothétie de rapport $\lambda \in \mathbb{K}$ si $u = \lambda Id_E$.

Remarque 10 : L'ensemble des homothéties de rapport non nul forme un sous-groupe de $GL(E)$.

Lemme 2.2. Per

Proposition 11 : Soit H un hyperplan de E et $u \in GL(E)$ tel que $u_{|H} = id_H$. On a équivalence entre :
i) $\det u = \lambda \neq 1$ (i.e. $u \notin SL(E)$)
ii) u admet une valeur propre $\lambda \neq 1$ et u est diagonalisable
iii) $\mathrm{Im}(u - id) \not\subset H$
iv) il existe une base B telle que $\mathrm{Mat}_B\, u = I_n + (\lambda - 1) E_{n,n}$.

Définition 12 : On dit alors que u est une dilatation d'hyperplan $H = \ker(u - id_E)$, de droite $D = \mathrm{Im}(u - id)$, de rapport λ.
Lorsque $\lambda = -1$ et car $\mathbb{K} \neq 2$, u est appelée réflexion.

Corollaire 13 : Deux dilatations sont conjuguées dans $GL(E)$ si et seulement si elles ont même rapport.

Proposition 14 : Soit H un hyperplan de E, d'équation $f \in E^*$ ($H = \ker f$ et $f \neq 0$).
Soit $u \in GL(E)$, $u \neq id$ tel que $u_{|H} = id_H$. On a équivalence entre :
i) $\det u = 1$ (i.e. $u \in SL(E)$)
ii) u n'est pas diagonalisable
iii) on a $D = \mathrm{Im}(u - id) \subset H$
iv) l'homomorphisme induit, $\bar{u} : E/H \to E/H$ est l'identité de E/H.
v) $\exists a \in H, a \neq 0, \forall x \in E, u(x) = x + f(x)a$.
vi) il existe une base B telle que $\mathrm{Mat}_B\, u = I_n + E_{n-1,n}$.

Définition 15 : Dans ce cas, on dit que u est une transvection d'hyperplan H et de droite D. Avec les notations de 14 on a $D = (a)$ et $D \subset H$.

Proposition 16 : Soit $u \in GL(E)$, $u \neq id$. Alors u est une transvection de droite D si et seulement si $u_D = id_D$ et $\bar{u} = id_{E/D}$.

Proposition 17 : Soit τ une transvection de droite D et d'hyperplan H et soit $u \in GL(E)$. Alors $\tau u \tau^{-1}$ est une transvection de droite $u(D)$ et d'hyperplan $u(H)$.

B Générateurs de SL(E) et GL(E). Per 4.2 et 4.3

Lemme 18 : Soient $x, y \in E\setminus\{0\}$. Il existe une transvection u ou un produit de deux transvections uv, tels que $u(x)=y$ ou $uv(x)=y$.

Théorème 19 : Les transvections engendrent SL(E).

Corollaire 20 : Les transvections et les dilatations engendrent GL(E).

Définition 21 : Soit $u, v \in GL(E)$ alors $[u,v] = uvu^{-1}v^{-1}$ est appelé commutateur de u et v.

Exemple 22 : si $u = id$ alors $[u,v] = vv^{-1} = id$.

Définition 23 : On note $D(GL(E))$ le sous-groupe de $GL(E)$ engendré par les commutateurs et $D(SL(E))$ celui engendré par les commutateurs de $SL(E)$.

Théorème 24 : On a $D(GL_n(\mathbb{K})) = SL_n(\mathbb{K})$ (sauf dans le cas $n=2, \mathbb{K}=\mathbb{F}_2$) et $D(SL_n(\mathbb{K})) = SL_n(\mathbb{K})$ (sauf si $n=2, \mathbb{K}=\mathbb{F}_2$ et $n=2, \mathbb{K}=\mathbb{F}_3$).

Théorème 25 : Le centre $Z(GL(E))$ est formé des homothéties $x \mapsto \lambda x$, $\lambda \in \mathbb{K}^*$. Il est isomorphe à $\mathbb{K}^*$. Le centre $SL(E)$ est $Z(GL(E)) \cap SL(E)$, il est isomorphe à $\mu_n(\mathbb{K}) = \{\lambda \in \mathbb{K}, \lambda^n = 1\}$.

C Cas des corps finis Rom 5.6 et Per 1.5

On considère $\mathbb{K}$ un corps fini de cardinal $q = p^\alpha$.

Proposition 26 : $|GL(E)| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = m\, p^{\frac{n(n-1)}{2}}$

Corollaire 27 : $|SL(E)| = \dfrac{|GL(E)|}{q-1} = q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n} (q^i - 1)$

Corollaire 28 : Soit $P = \{A = (a_{ij}) \mid a_{ij} = 0 \text{ si } i>j \text{ et } a_{ii} = 1\}$ l'ensemble des matrices triangulaires supérieures strictes. Alors P est un p sous-groupe de Sylow de $GL_n(\mathbb{K})$.

Lemme 29 : Soit G un groupe avec $|G| = n = p^\alpha m$, $p \nmid m$ et soit H un sous-groupe de G. Soit S un p Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un

Développement (Sylow 1) Soit G un groupe fini et p un diviseur premier de $|G|$, alors G contient au moins un p sous-groupe de Sylow.

Corollaire 30 : Si $|G| = p^\alpha m$, $p \nmid m$, G contient des sous-groupes d'ordre p^i pour tout $i \leq \alpha$.

Théorème 31 (Sylow 2) Soit G un groupe, $|G| = p^\alpha m$, $p \nmid m$ alors
i) Si H est un sous-groupe de G qui est un p-groupe, il existe un p Sylow S tel que $H \subset S$.
ii) Les p Sylow sont tous conjugués (et donc leur nombre k divise m).
iii) On a $k \equiv 1 \ [p]$ (donc $k \mid m$).

Corollaire 32 : Si S est un p Sylow on a :
$S \triangleleft G \iff S$ est l'unique p Sylow de $G \iff k = 1$.

Application 33 : Un groupe d'ordre 63 n'est pas simple.

III Sous-groupes des endomorphismes orthogonaux

A Isométries d'un espace euclidien. Rom 22.3

On considère E un espace euclidien.

Définition 34 : Une isométrie (ou application orthogonale) de E est une application $u : E \to E$ qui conserve le produit scalaire, c'est à dire telle que :
$$\forall (x,y) \in E \times E, \quad \langle u(x), u(y) \rangle = \langle x, y \rangle.$$
On note $O(E)$ l'ensemble des isométries de E.

Exemple 35 : Les seules homothéties de $O(E)$ sont $\pm id$.

Théorème 36 : Une application $u : E \to E$ est une isométrie si et seulement si elle est linéaire et conserve la norme, c'est à dire :
$$\forall x \in E, \ \|u(x)\| = \|x\|$$

Contre exemple 37 : Une application $u : E \to E$ qui conserve la norme n'est pas nécessairement linéaire et n'est donc pas une isométrie en général. Par exemple pour $e \in E$ de norme égale à 1, l'application $u : x \mapsto \|x\| e$ conserve la norme et n'est pas linéaire ($u(-x) = u(x) \neq -u(x)$ $\forall x \neq 0$).

Théorème 38 : Soient $B = (e_i)$ une base orthonormée de E et $u \in \mathcal{L}(E)$. Alors $u \in O(E)$

Théorème 39: Soient $\mathcal{B} = (e_i)$ une base orthonormée de E et $u \in \mathcal{L}(E)$ de matrice A dans $\mathcal{B}$. Alors $u \in O(E)$ ssi ${}^tAA = A\,{}^tA = I_n$.

Corollaire 40: Soit $u \in O(E)$, alors $\det u = \pm 1$.

B Réduction des endomorphismes orthogonaux. Rom 22.3 et 22.4

Lemme 41: Les seules valeurs propres réelles possibles d'une isométrie sont ± 1.

Lemme 42: Soit $u \in O(E)$. Il existe des sev $P_1, \dots, P_r$ de E de dimension égale à 1 ou 2, deux à deux orthogonaux, stables par u et tels que $E = \bigoplus_{i=1}^{r} P_i$

Proposition 43: Soit $u \in O(E)$. Si F est un sous espace vectoriel de E stable par u, alors son orthogonal $F^\perp$ est aussi stable par u.

Théorème 44 (réduction des endomorphismes orthogonaux)
Soit $u \in O(E)$ avec $n \geq 2$. Il existe une base orthonormée $\mathcal{B}$ de E dans laquelle la matrice de u s'écrit : $D = \begin{pmatrix} I_p & & & & (0) \\ & -I_q & & & \\ & & R_1 & & \\ & & & \ddots & \\ (0) & & & & R_r \end{pmatrix}$ où $\forall k \in [\![1,r]\!]$ $R_k = \begin{pmatrix} \cos\theta_k & -\sin\theta_k \\ \sin\theta_k & \cos\theta_k \end{pmatrix}$

avec $\theta_k \in]0, 2\pi[\setminus \{\pi\}$ et $p + q + 2r = n$

C Propriétés topologiques de $O(E)$. Rom 22.3 22.5 et 22.9

Théorème 45: Une isométrie est un automorphisme de E et $O(E)$ est un sous groupe de $GL(E)$.

Théorème 46: $O(E)$ est une partie compacte de $\mathcal{L}(E)$

Définition 47: On note $O^+(E) = \{u \in O(E), \det u = 1\}$ les automorphismes orthogonaux positifs et $O^-(E) = \{u \in O(E), \det u = -1\}$ les automorphismes orthogonaux négatifs

Théorème 48: $O^+(E)$ (resp $O_n^+(\mathbb{R})$) est un sous groupe distingué de $O(E)$ (resp $O_n(\mathbb{R})$) d'indice 2.

Corollaire 49. Les composantes connexes de $O(E)$ sont $O^+(E)$ et $O^-(E)$

Théorème 50: Pour $n = \dim E \geq 2$, le groupe $O(E)$ est engendré par l'ensemble des réflexions. Précisément, toute isométrie de E peut s'écrire comme le produit d'au plus n réflexions.

$\boxed{\text{Développement}}$ L'application $(\Omega, S) \mapsto \Omega S$ réalise un homéomorphisme de $O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R})$ sur $GL_n(\mathbb{R})$.

Références :

Rombaldi Mathématiques pour l'agrégation Rom

D. Perrin Cours d'Algèbre Per

X-G Algèbre X G