Groupes linéaires

Soit K un corps et $n \in \mathbb{N}^*$.

1 Le groupe $\mathrm{GL}_n(K)$

Définition 1.1. *Le* ***groupe linéaire*** *d'indice n sur K est $\mathrm{GL}_n(K)$, l'ensemble des matrices inversibles de taille $n \times n$ à coefficients dans K.*

Exercice 1. *Soit q une puissance de nombre premier. Calculer $|\mathrm{GL}_n(\mathbb{F}_q)|$.*

Exemple 1.2.

1. Soit $\lambda \in K^\times$. L'**homothétie** de rapport λ est $\lambda I_n \in \mathrm{GL}_n(K)$.
2. Soit $\lambda \in K^\times$ et $1 \leq i, j \leq n$ avec $i \neq j$. La **transvection** de coefficient λ et d'indice (i, j) est la matrice $T_{i,j}(\lambda)$ dont le coefficient en position (k, l) vaut
$$\begin{cases} 1 \text{ si } k = l \\ \lambda \text{ si } (k,l) = (i,j) \\ 0 \text{ sinon.} \end{cases}$$
3. Soit $\lambda \in K^\times$ et $1 \leq i \leq n$. La **dilatation** de rapport λ et d'indice i est la matrice $D_i(\lambda)$ dont le coefficient en position (k, l) vaut
$$\begin{cases} 1 \text{ si } k = l \neq i \\ \lambda \text{ si } (k,l) = (i,i) \\ 0 \text{ sinon.} \end{cases}$$

Théorème 1.3. *Le groupe $\mathrm{GL}_n(K)$ est engendré par les matrices de transvection et de dilatation.*

Démonstration. La multiplication à gauche par $D_i(\lambda)$ revient à multiplier la i-ième ligne par λ. La multiplication à gauche par $T_{i,j}(\lambda)$ revient à effectuer l'opération élémentaire $L_i \to L_i + \lambda L_j$. La terminaison de l'algorithme du pivot de Gauss donne donc le résultat. □

Remarque 1.4. Quand on multiplie à droite, ce sont les mêmes opérations mais sur les colonnes.

Proposition 1.5. *On a*
$$Z(\mathrm{GL}_n(K)) = \{\lambda I_n \mid \lambda \in K^\times\}.$$

Démonstration. L'inclusion directe est claire.

Réciproquement, rappelons que si deux matrices commutent alors elles stabilisent les espaces propres de de l'autre. Or, si $K.u \subset K^n$ est une droite vectorielle, on peut trouver une matrice inversible dont c'est un espace propre, il suffit de compléter le vecteur non nul u en une base de K^n et de considérer la matrice associée.

Donc si $M \in Z(\mathrm{GL}_n(K))$, M préserve toutes les droites vectorielles. Si $(e_1, \dots, e_n)$ est la base canonique de K^n, il existe $\lambda, \lambda_1, \dots, \lambda_n \in K$ tels que $Me_i = \lambda_i e_i$ pour $1 \leq i \leq n$ et $M(e_1 + \cdots + e_n) = \lambda(e_1 + \cdots + e_n) = \lambda e_1 + \cdots + \lambda e_n = \lambda_1 e_1 = \cdots + \lambda_n e_n$, ce qui implique que $M = \lambda I_n$. □

Définition 1.6. *Soit $M = (m_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(K)$. Le* ***déterminant*** *de M est*

$$\det(M) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} m_{i,\sigma(i)}.$$

Proposition 1.7. *On a*

$$\mathrm{GL}_n(K) = \{M \in \mathcal{M}_n(K) \mid \det M \neq 0\}.$$

Le déterminant est un morphisme de groupes de $\mathrm{GL}_n(K)$ dans $K^\times$.

Définition 1.8. *Le* ***groupe spécial linéaire*** *est le noyau du déterminant :*

$$\mathrm{SL}_n(K) = \{M \in \mathrm{GL}_n(K) \mid \det M = 1\}.$$

Exercice 2. *Soit q une puissance de nombre premier. Déterminer $|\mathrm{SL}_n(\mathbb{F}_q)|$.*

Proposition 1.9. *Le groupe $\mathrm{SL}_n(K)$ est engendré par les matrices de transvection.*

Démonstration. Il suffit de savoir que le pivot de Gauss permet de ramener une matrice M à

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \dots & \det M \end{pmatrix}.$$

□

Proposition 1.10. *On a*

$$Z(\mathrm{SL}_n(K)) = Z(\mathrm{GL}_n(K)) \cap \mathrm{SL}_n(K) = \{\lambda I_n \mid \lambda \in K, \lambda^n = 1\}.$$

Théorème 1.11. *On a*

$$D(\mathrm{GL}_n(K)) = D(\mathrm{SL}_n(K)) = \mathrm{SL}_n(K),$$

sauf si $n = 2$ et $K = \mathbb{F}_2$ ou $K = \mathbb{F}_3$.

Pour la démonstration, voir Perrin (Chap. IV, §3).

Remarque 1.12. On a $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$ (voir exercices) donc $D(\mathrm{GL}_2(\mathbb{F}_2)) = D(\mathrm{SL}_2(\mathbb{F}_2)) \simeq \mathbb{Z}/3\mathbb{Z}$ tandis que $D(\mathrm{GL}_2(\mathbb{F}_3)) = \mathrm{SL}_2(\mathbb{F}_3)$ mais $D(\mathrm{SL}_2(\mathbb{F}_3)) \simeq \mathbb{H}_8 \not\simeq \mathrm{SL}_2(\mathbb{F}_3)$ (voir Perrin comme ci-dessus).

2 Groupes orthogonaux et unitaires

Définition 2.1. *Soit q une forme quadratique sur K^n. Le **groupe d'isométries** de q est*

$$\mathrm{O}(q) = \{\varphi \in \mathrm{GL}(K^n) \mid q \circ f = q\}.$$

*En fixant une base, on lui associe un sous-groupe de $\mathrm{GL}_n(K)$. Dans le cas particulier de la forme quadratique « euclidienne » $(x_1, \dots, x_n) \mapsto x_1^2 + \cdots + x_n^2$ dans la base canonique de $\mathbb{R}^n$, ce groupe est le **groupe orthogonal** $\mathrm{O}_n(\mathbb{R})$.*

Proposition 2.2. *Si q est une forme quadratique sur K^n de matrice S dans une base $\mathcal{B}$ de K^n alors*

$$\mathrm{O}(q) \simeq \{M \in \mathrm{GL}_n(K) \mid M^\top S M = S\}.$$

En particulier, on a

$$\mathrm{O}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) \mid M^\top M = I_n\}.$$

Définition 2.3. *On définit le **groupe spécial orthogonal** comme*

$$\mathrm{SO}_n(R) = \{M \in \mathrm{O}_n(\mathbb{R}) \mid \det(M) = 1\}.$$

Remarque 2.4. On a $\mathrm{O}_1(\mathbb{R}) = \{-\mathrm{id}_\mathbb{R}, \mathrm{id}\} \simeq \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{SO}_1(\mathbb{R}) = \{\mathrm{id}_\mathbb{R}\}$. De plus,

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R}, a^2 + b^2 = 1 \right\} \simeq \mathbb{S}^1,$$

le cercle unité de $\mathbb{C}$, via $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mapsto a + ib$. En particulier, $\mathrm{SO}_2(\mathbb{R})$ est abélien.

Théorème 2.5. *Pour tout $n \geq 1$, le groupe $\mathrm{O}_n(\mathbb{R})$ est engendré par les matrices de réflexions (symétries orthogonales u telles que $\dim\ker(u - \mathrm{id}) = n - 1$) dans une base orthonormée. Pour tout $n \geq 3$, le groupe $\mathrm{SO}_n(\mathbb{R})$ est engendré par les matrices de retournements (symétries orthogonales u telles que $\dim\ker(u - \mathrm{id}) = n - 2$) dans une base orthonormée.*

Démonstration. Tout repose sur le fait que si $M \in \mathrm{O}_n(\mathbb{R})$ stabilise le sous-espace vectoriel F alors M stabilise $F^\perp$. On fait une récurrence sur la codimension r de l'espace des points fixes. Si $r = 0$ alors $M = I_n$ et il n'y a rien à prouver. Si l'on suppose le résultat vrai pour des codimensions strictement inférieures à r, on montre comment multiplier M par une matrice de réflexion pour augmenter la dimension de l'espace des points fixes. Pour ce faire, on prend $u \in \mathbb{R}^n$ de norme 1 tel que $Mu \neq u$, $H = \{Mu - u\}^\perp$ l'hyperplan médiateur de u et Mu, et S la matrice de réflexion par rapport à H. Alors SM admet $\mathrm{Vect}(u)$ et les points fixes de M pour points fixes, et on lui applique l'hypothèse de récurrence.

Pour $\mathrm{SO}_n(\mathbb{R})$, le point précédent montre que ses éléments sont produits d'un nombre pair de matrices de réflexions. Il suffit alors de montrer qu'un produit de deux réflexions est produit de deux retournements en dimension au moins 3, le cas critique étant celui de la dimension 3. Mais si S est une matrice de réflexion en dimension 3, alors $-S$ est une matrice de retournement ! □

Remarque 2.6.

1. Dans le plan, la rotation d'angle θ est la composée des symétries orthogonales par rapport à deux droites formant un angle de $\theta/2$ (faire un dessin et le voir en complexes).

2. On peut aussi montrer que le nombre de réflexions nécessaire est exactement la codimension de l'espace des points fixes.

3. Ces familles de générateurs sont utiles car ses éléments sont « simples », au sens où leurs points fixes sont nombreux, à l'instar des transpositions engendrant $\mathfrak{S}_n$ et les 3-cycles engendrant $\mathfrak{A}_n$. Ils bénéficient également de propriétés de conjugaison intéressantes.

Proposition 2.7. *Les réflexions sont conjuguées dans* $\mathrm{O}_n(\mathbb{R})$ *pour* $n \geq 2$ *et les retournements sont conjugués dans* $\mathrm{SO}_n(\mathbb{R})$ *pour* $n \geq 3$.

Corollaire 2.8. *On a*

$$Z(\mathrm{O}_n(\mathbb{R})) = \{-\mathrm{id}_{\mathbb{R}^n}, \mathrm{id}_{\mathbb{R}^n}\}$$

et

$$Z(\mathrm{SO}_n(\mathbb{R})) = \begin{cases} \mathrm{SO}_n(\mathbb{R}) & \text{si } n \leq 2 \\ \{\mathrm{id}_{\mathbb{R}^n}\} & \text{si } n \geq 3 \text{ est impair} \\ \{-\mathrm{id}_{\mathbb{R}^n}, \mathrm{id}_{\mathbb{R}^n}\} & \text{si } n \geq 3 \text{ est pair.} \end{cases}$$

Définition 2.9. *Pour* $n \geq 1$, *le* ***groupe unitaire*** *est*

$$\mathrm{U}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) \mid \overline{M}^\top M = I_n\}$$

et le ***groupe spécial unitaire*** *est*

$$\mathrm{SU}_n(\mathbb{C}) = \{M \in \mathrm{U}_n(\mathbb{C}) \mid \det M = 1\}.$$

Remarque 2.10. Tout comme le groupe orthogonal correspond aux isométries de la forme quadratique euclidienne de $\mathbb{R}^n$ dans une base orthonormée, le groupe unitaire correspond aux isométries de la forme hermitienne de $\mathbb{C}^n$ dans une base orthonormée. Cependant, la géométrie sous-jacente étant plus compliquée, on ne s'intéressera pas à ses systèmes de générateurs.

3 Exercices

Exercice 3. *Soit* K *un corps. Un groupe de matrices dans* $\mathcal{M}_n(K)$ *pour la multiplication est-il un sous-groupe de* $\mathrm{GL}_n(K)$ *?*

Exercice 4. *Soit* K *un corps et* $n \in \mathbb{N}^*$. *Montrer que*

$$\mathrm{GL}_n(K) \simeq \mathrm{SL}_n(K) \rtimes_\varphi K^\times$$

pour un certain morphisme φ *à déterminer. (Indication : Chercher une* ***section*** $s : K^\times \to \mathrm{GL}_n(K)$ *telle que* $\det \circ s = \mathrm{id}_{K^\times}$.*)*

Exercice 5. *1. Soit* $n \in \mathbb{N}^*$ *et* G *un sous-groupe abélien fini de* $\mathrm{GL}_n(\mathbb{C})$. *Montrer que les éléments de* G *sont diagonalisables dans une même base.*

2. Soit K *un corps de caractéristique différente de* 2. *Quel est le cardinal du plus grand sous-groupe abélien fini* G *de* $\mathrm{GL}_n(K)$ *tel pour tout* $M \in G, M^2 = I_n$ *?*

3. Montrer que si $\mathrm{GL}_n(K) \simeq \mathrm{GL}_m(K)$ *alors* $n = m$.

Exercice 6. *Soit* p *un nombre premier et* $n \in \mathbb{N}^*$. *Montrer que l'ensemble des matrices unipotentes, c'est-à-dire triangulaires supérieures avec des* 1 *sur la diagonale, est un* p*-Sylow de* $\mathrm{GL}_n(\mathbb{F}_p)$.

Exercice 7 (Quelques propriétés topologiques)**.** *Soit* $n \in \mathbb{N}^*$.

1. *Montrer que* $\mathrm{GL}_n(\mathbb{C})$ *est connexe par arcs et que* $\mathrm{GL}_n(\mathbb{R})$ *ne l'est pas.*

2. *Montrer que* $\mathrm{SL}_n(\mathbb{C})$ *et* $\mathrm{SL}_n(\mathbb{R})$ *sont connexes par arcs et en déduire les composantes connexes de* $\mathrm{GL}_n(\mathbb{R})$*. Est-ce que ce sont des groupes compacts ?*

3. *Faire de même avec* $\mathrm{O}_n(\mathbb{R})$ *et* $\mathrm{SO}_n(\mathbb{R})$*.*

Exercice 8 (Un zeste de géométrie projective)**.** *Soit K un corps et $n \geq 1$. On note*

$$\mathbb{P}^n(K) = (K^{n+1} \setminus \{0\})/\sim$$

où $\sim$ désigne la relation d'équivalence de colinéarité.

1. *Montrer que* $\mathrm{GL}_{n+1}(K)$ *agit de manière transitive sur* $\mathbb{P}^n(K)$*. Identifier le stabilisateur d'un élément et le noyau de cette action.*

2. *Faire de même avec* $\mathrm{SL}_{n+1}(K)$*.*

3. *On note*
$$\mathrm{PGL}_n(K) = \mathrm{GL}_n(K)/Z(\mathrm{GL}_n(K))$$
et
$$\mathrm{PSL}_n(K) = \mathrm{SL}_n(K)/Z(\mathrm{SL}_n(K)).$$
On suppose désormais que $K = \mathbb{F}_q$. Calculer
$$|\,\mathrm{PGL}_n(\mathbb{F}_q)|, |\,\mathrm{PSL}_n(\mathbb{F}_q)| \text{ et } |\mathbb{P}^n(\mathbb{F}_q)|.$$

4. *Montrer que*
$$\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3.$$

5. *Montrer que*
$$\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$$
et
$$\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{A}_4.$$

6. *Montrer que*
$$\mathrm{PGL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4) \simeq \mathfrak{A}_5.$$

Remarque. On peut aussi montrer (mais c'est plus difficile) que

$$\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathfrak{S}_5, \mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathfrak{A}_5, \mathrm{PSL}_2(\mathbb{F}_9) \simeq \mathfrak{A}_6, \mathrm{PSL}_4(\mathbb{F}_2) \simeq \mathfrak{A}_8$$

et ce sont les seuls « isomorphismes exceptionnels » de ce type. Pour $n \geq 2$, les groupes $\mathrm{PSL}_n(K)$ sont tous simples, sauf $\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{S}_3$ et $\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$. De même, on définit $\mathrm{PSO}_n(\mathbb{R}) = \mathrm{SO}_n(\mathbb{R})/Z(\mathrm{SO}_n(\mathbb{R}))$ pour $n \geq 3$ et ces groupes sont tous simples.

Exercice 9. 1. *Montrer que*

$$\mathrm{GL}_n(\mathbb{Z}) = \{M \in \mathcal{M}_n(\mathbb{Z}) \mid \det(M) = \pm 1\}.$$

2. *Soit*
$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$
et
$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$
Montrer que $\langle S, T\rangle = \mathrm{SL}_2(\mathbb{Z})$. *Indication : Calculer les puissances de* S *et* T *et étudier l'effet de leur multiplication à gauche sur une matrice.*

3. *Écrire* $\begin{pmatrix} 19 & 8 \\ 7 & 3 \end{pmatrix}$ *comme produit de puissances de* S *et* T.

Exercice 10. *Pour* $n \in \mathbb{N}^*$, *notons*
$$\mathrm{O}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) \mid M^\top M = I_n\}.$$
Montrer que, pour $n \geq 2$, $\mathrm{O}_n(\mathbb{C})$ *n'est pas compact. L'identifier à un groupe de la forme* $\mathrm{O}(q)$ *pour une certain forme quadratique à identifier.*

Exercice 11. *Montrer que si* $n \in \mathbb{N}^*$ *est impair alors* $\mathrm{O}_n(\mathbb{R}) \simeq \mathrm{SO}_n(\mathbb{R}) \times \mathbb{Z}/2\mathbb{Z}$. *Est-ce encore vrai pour n pair ?*

Exercice 12 ($\mathrm{SO}_3(\mathbb{R})$ est simple)**.** *Soit* $H \triangleleft \mathrm{SO}_3(\mathbb{R})$ *non trivial. On va montrer que* $H = \mathrm{SO}_3(\mathbb{R})$ *et donc que* $\mathrm{SO}_3(\mathbb{R})$ *est simple.*

1. *Soit* $N \in H \setminus \{I_3\}$. *Justifier que l'image de l'application* $\varphi : M \mapsto \mathrm{tr}(MNM^{-1}N^{-1})$, *définie sur* $\mathrm{SO}_3(\mathbb{R})$, *est un intervalle de la forme* $[a, 3]$, *avec* $a \in [-1, 3[$.

2. *Justifier que pour* $n \in \mathbb{N}^*$ *assez grand, il existe* $M \in \mathrm{SO}_3(\mathbb{R})$ *telle que* $MNM^{-1}N^{-1}$ *soit une rotation d'angle* $\pm\frac{\pi}{n}$.

3. *Conclure que* H *contient un renversement, puis que* $H = \mathrm{SO}_3(\mathbb{R})$.

Exercice 13. 1. *Montrer que*
$$\mathrm{SU}_2(\mathbb{C}) = \left\{ \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1 \right\}.$$

2. *Soit* $\mathbb{H}$ *la* $\mathbb{R}$*-algèbre des* ***quaternions*** *de dimension* 4 *engendrée par les matrices*
$$I_2, I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, K = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{C}).$$
On admet que $\mathbb{H}$ *est une algèbre à division non commutative, de centre* $\mathbb{R}I_2$ *et que* $\langle I, J\rangle \simeq \mathbb{H}_8$. *Montrer que* $\mathrm{SU}_2(\mathbb{C})$ *s'identifie alors à la sphère* $\mathbb{S}^3 \subset \mathbb{R}^4$.

3. *On notera désormais* $q = a + ib + jc + kd$ *les quaternions, avec* $a, b, c, d \in \mathbb{R}$. *La* ***norme*** *de* q *est donnée par* $|q|^2 = a^2 + b^2 + c^2 + d^2$. *Donner un argument non calculatoire pour montrer que la norme est multiplicative sur* $\mathbb{H}$.

4. *Appelons* ***partie réelle*** *de* $q = a + ib + jc + kd$ *le réel* a. *Un quaternion* ***imaginaire pur*** *est un quaternion de partie réelle nulle. Soit* $q \in \mathbb{H}$ *un quaternion unitaire (de norme* 1*). Montrer que la conjugaison par* q *correspond à une isométrie positive, qui préserve le sous-espace vectoriel des quaternions imaginaires purs.*

5. *En déduire que* $\mathrm{SO}_3(\mathbb{R}) \simeq \mathrm{SU}_2(\mathbb{C})/\{I_2, -I_2\}$.