

Groupe orthogonal et quadriques : correction

Exercice 1.

1. Déjà, il est évident que si deux matrices antisymétriques A_1 et A_2 vérifient la conclusion, la matrice diagonale par blocs de blocs A_1 et A_2 la vérifiera également. De même, comme $[{}^tOS_1O, {}^tOS_2O] = {}^tO[S_1, S_2]O$ quand O est orthogonale, si la conclusion de l'exercice est vraie pour A antisymétrique, elle l'est également pour toute matrice orthogonalement semblable à A .

Maintenant, le cours affirme que toute matrice antisymétrique est orthogonalement semblable à une matrice diagonale par blocs, les blocs étant le bloc nul de taille 1×1 et le bloc $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Il suffit donc de vérifier que ces deux blocs vérifient la conclusion de l'exercice.

Pour le bloc nul, on a simplement $0 = [0, 0]$. Pour l'autre, il faut un peu plus bidouiller. Par exemple,

$$\left[\begin{pmatrix} 1/2 & 0 \\ 0 & -1/2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right] = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

2. Soit $M \in SO_n(\mathbf{R})$. D'après le cours, il existe $O \in O_n(\mathbf{R})$ telle que

$$M = {}^tO \operatorname{diag}(1, \dots, 1, R(\theta_1), \dots, R(\theta_s))O,$$

où $R(\theta) = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$. La matrice $M_t = {}^tO \operatorname{diag}(1, \dots, 1, R(t\theta_1), \dots, R(t\theta_s))$ fournit alors un chemin $[0, 1] \rightarrow SO_n(\mathbf{R})$ tel que $M_0 = \operatorname{id}$ et $M_1 = M$. Le groupe $SO_n(\mathbf{R})$ est donc bien connexe par arcs.

3. Une matrice orthogonale sous la forme $\operatorname{diag}(1, \dots, 1, -1, \dots, -1, R(\theta_1), \dots, R(\theta_s))$ (avec p coefficients égaux à 1 et q coefficients égaux à -1) est une involution si et seulement si elle est diagonale avec des coefficients égaux à ± 1 . De plus, le nombre de coefficients égaux à 1 dans M ne dépend que de la classe de conjugaison : c'est $\dim(M - \operatorname{id})$. Cela démontre donc que toute involution orthogonale dans $O_n(\mathbf{R})$ est conjuguée à une unique matrice diagonale $\operatorname{diag}(1, \dots, 1, -1, \dots, -1)$ avec p coefficients égaux à 1 et $n - p$ coefficients égaux à -1 . Le groupe $O_n(\mathbf{R})$ a donc $n + 1$ classes de conjugaison d'involutions. En particulier, si les groupes $O_n(\mathbf{R})$ et $O_m(\mathbf{R})$ sont isomorphes, $n = m$.

Exercice 2.

Déjà, une matrice antisymétrique est de trace nulle. Donc $\exp[\mathfrak{so}_n(\mathbf{R})] \subset SL_n(\mathbf{R})$. En outre, si ${}^tA = -A$, on obtient automatiquement ${}^t(\exp A) = \exp({}^tA) = \exp(-A) = \exp(A)^{-1}$. L'exponentielle envoie donc bien $\mathfrak{so}_n(\mathbf{R})$ dans SO_n . On pourrait même démontrer que, comme la notation le suggère, $\mathfrak{so}_n(\mathbf{R})$ est l'algèbre de Lie de $SO_n(\mathbf{R})$. Montrons maintenant la surjectivité.

On a vu que l'exponentielle possédait les propriétés suivantes (où $\operatorname{diag}(M_1, \dots, M_r)$ est la matrice diagonale par blocs, de blocs $M_1, \dots, M_r$)

$$\exp \operatorname{diag}(M_1, \dots, M_r) = \operatorname{diag}(\exp M_1, \dots, \exp M_r) \quad \exp(P^{-1}MP) = P^{-1}(\exp M)P.$$

Comme dans le premier exercice, pour montrer la surjectivité de $\exp : \mathfrak{so}_n(\mathbf{R}) \rightarrow \mathrm{SO}_n(\mathbf{R})$, il suffit donc de trouver un antécédant à $(1) \in \mathrm{SO}_1(\mathbf{R})$ et $\mathrm{R}(\theta) = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \in \mathrm{SO}_2(\mathbf{R})$.

On obtient facilement (pour les blocs 2×2 , il est utile de penser à la matrice $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ comme au nombre complexe $a + ib$; cette identification est un isomorphisme d'algèbres de Banach et fait donc correspondre l'exponentielle des matrices et celle des nombres complexes).

$$\exp(0) = (1) \quad \exp \begin{pmatrix} 0 & \theta \\ -\theta & 0 \end{pmatrix} = \mathrm{R}(\theta)$$

donc l'exponentielle envoie surjectivement $\mathfrak{so}_n(\mathbf{R})$ sur $\mathrm{SO}_n(\mathbf{R})$.

Exercice 3.

Convenons que dans cet exercice, on note multiplicativement le groupe $\mathbf{Z}/2\mathbf{Z}$, c'est-à-dire qu'on l'identifie à $\{\pm 1\}$.

1. Le cours garantit que les réflexions orthogonales par rapport à un hyperplan, qui sont toutes conjuguées, engendrent le groupe $\mathrm{O}_n(\mathbf{R})$. Comme le groupe $\mathbf{Z}/2\mathbf{Z}$ est abélien, toutes ces réflexions ont la même image $u \in \{\pm 1\}$. Si $u = 1$, le morphisme est trivial. Si $u = -1$, le morphisme coïncide avec le déterminant sur un système générateur, donc est le déterminant. Finalement,

$$\mathrm{Hom}(\mathrm{O}_n(\mathbf{R}), \mathbf{Z}/2\mathbf{Z}) = \{1, \det\}.$$

2. Tout élément de $\mathrm{O}_n(\mathbf{R})$ est un produit de réflexions par rapport à des hyperplans (à partir de maintenant, on dira simplement *réflexion*). Puisque son déterminant est 1, un élément de $\mathrm{SO}_n(\mathbf{R})$ est donc le produit d'un nombre pair de réflexions. Il suffit donc de démontrer que tout produit de deux réflexions est un produit de retournements.

Soit donc H_1 et H_2 deux hyperplans et ρ_1, ρ_2 les réflexions correspondantes. Évidemment, si $H_1 = H_2$, $\rho_1 = \rho_2$ et $\rho_1 \circ \rho_2 = \mathrm{id}$; on peut supposer $H_1 \neq H_2$.

- Si $n = 3$, on a l'égalité $\rho_1 \circ \rho_2 = (-\rho_1) \circ (-\rho_2)$ et les deux transformations $-\rho_i$ sont des retournements.
- Dans le cas général, on va essayer de se ramener au cas tridimensionnel. Les hyperplans H_1 et H_2 étant différents, leur intersection $H_1 \cap H_2$ est de codimension deux. Soit $F \subset H_1 \cap H_2$ un hyperplan de cette intersection : c'est un espace de dimension $n - 3$, et tous les vecteurs de cet espace sont fixés par ρ_1, ρ_2 et donc $\rho_1 \circ \rho_2$. L'orthogonal $F^\perp$ de F , de dimension 3, est stabilisé par les ρ_i . Leur restriction à $F^\perp$ sont d'ailleurs des réflexions. D'après le cas précédent, il existe deux retournements $\tilde{\sigma}_1, \tilde{\sigma}_2$ de $F^\perp$ dont le produit est $(\rho_1 \circ \rho_2)|_{F^\perp}$. Chacun des deux retournements $\tilde{\sigma}_i$ de $F^\perp$ se prolonge en un unique retournement σ_i sur $\mathbf{R}^n$ tout entier (il suffit de l'étendre par l'identité sur F), et l'on a bien $\sigma_1 \circ \sigma_2 = \rho_1 \circ \rho_2$.

3. Commençons par utiliser une technique de preuve proche de la première question.

Les retournements sont tous conjugués. Par définition, ce sont les transformations orthogonalement semblables à $\mathrm{diag}(-1, -1, 1, \dots, 1)$; à ce titre, ils forment une classe de conjugaison dans $\mathrm{O}_n(\mathbf{R})$. Pour montrer que cela reste une classe de conjugaison dans $\mathrm{SO}_n(\mathbf{R})$, remarquons que tout retournement commute avec une réflexion orthogonale ρ par rapport à un hyperplan : $\mathrm{diag}(-1, -1, 1, \dots, 1)$ commute avec $\mathrm{diag}(-1, 1, 1, \dots, 1)$. Cela permet de démontrer que deux retournements conjugués dans $\mathrm{O}_n(\mathbf{R})$ sont conjugués dans $\mathrm{SO}_n(\mathbf{R})$: s'ils sont conjugués par $\sigma \in \mathrm{SO}_n(\mathbf{R})$, il n'y a rien à montrer; s'ils sont conjugués par $\sigma \in \mathrm{O}_n^-(\mathbf{R})$, ils le sont aussi par $\sigma\rho \in \mathrm{SO}_n(\mathbf{R})$.

Puisque $\mathbf{Z}/2\mathbf{Z}$ est abélien, tous les retournements ont donc la même image $u \in \{\pm 1\}$ par un morphisme $f : \mathrm{SO}_n(\mathbf{R}) \rightarrow \{\pm 1\}$. Si $n \geq 3$, il existe deux retournements dont le produit est encore un retournement : si on prend une base orthonormée $(e_1, \dots, e_n)$ de $\mathbf{R}^n$, le produit du retournement d'axe $\mathrm{Vect}(e_3, e_4, \dots, e_n)$ et de celui d'axe $\mathrm{Vect}(e_2, e_4, \dots, e_n)$ est le retournement d'axe $\mathrm{Vect}(e_1, e_4, \dots, e_n)$. En prenant l'image par f de cette relation, on obtient $u^2 = u$, donc $u = 1$. Ainsi, si $n \geq 3$, f coïncide sur une partie génératrice (les retournements) avec id . Le seul morphisme est donc le morphisme trivial.

Quand $n = 2$, il n'y a qu'un seul retournement ($\{0\}$ est le seul sous-espace de codimension 2), qui n'engendre évidemment pas $\mathrm{SO}_2(\mathbf{R})$ à lui tout seul. Il faut donc trouver une autre méthode. La propriété que nous allons utiliser est celle de *divisibilité* : tout élément de $\mathrm{SO}_2(\mathbf{R})$ est le carré d'une rotation. Son image dans $\mathbf{Z}/2\mathbf{Z}$ est donc le carré d'un élément : c'est donc 1. Au final, on a démontré pour tout $n \geq 2$

$$\mathrm{Hom}(\mathrm{SO}_n(\mathbf{R}), 1) = \{1\}.$$

Remarquons que la méthode de preuve employée dans $\mathrm{SO}_2(\mathbf{R})$ marcherait aussi bien pour $\mathrm{SO}_n(\mathbf{R})$: la réduction des isométries montre simplement que toute isométrie directe est un carré (c'est également une conséquence de la surjectivité de l'exponentielle).

Exercice 4.

A. Simplicité de $\mathrm{SO}_3(\mathbf{R})$.

1. On sait que si deux endomorphismes commutent, les espaces propres de l'un sont stables pour l'autre. Or, tout plan $P \subset \mathbf{R}^n$ est l'espace propre (associé à la valeur propre -1) du retournement d'axe $P^\perp$. Un élément central dans $\mathrm{SO}_n(\mathbf{R})$ ou dans $\mathrm{O}_n(\mathbf{R})$ doit donc stabiliser tous les plans vectoriels donc, si $n \geq 3$, toutes les droites, ce qui entraîne que c'est une homothétie.

La réciproque étant claire, dès que $n \geq 3$, le centre de $\mathrm{O}_n(\mathbf{R})$ (resp. $\mathrm{SO}_n(\mathbf{R})$) est constitué des homothéties appartenant à $\mathrm{O}_n(\mathbf{R})$ (resp. $\mathrm{SO}_n(\mathbf{R})$), d'où les centres suivants (il faut traiter le cas $n = 2$ à part, et utiliser les réflexions par rapport aux droites) :

	$n = 2$	$n \geq 3$ impair	$n \geq 4$ pair
$Z(\mathrm{O}_n(\mathbf{R}))$	$\{\pm \mathrm{id}\}$	$\{\pm \mathrm{id}\}$	$\{\pm \mathrm{id}\}$
$Z(\mathrm{SO}_n(\mathbf{R}))$	$\mathrm{SO}_2(\mathbf{R})$	$\{\mathrm{id}\}$	$\{\pm \mathrm{id}\}$

2. La réduction des isométries en dimension 3 prouve que toute isométrie $u \in \mathrm{SO}_3(\mathbf{R})$ est conjuguée à une matrice de la forme $\mathrm{diag}(1, R(\theta))$. Cela démontre à la fois que pour tout $u \in \mathrm{SO}(3)$, $\mathrm{tr} u \in [-1, 3]$ et que $\mathrm{tr} u = 3$ si et seulement si $\theta = 0 \pmod{2\pi}$, c'est à dire si $u = \mathrm{id}$. Ainsi, tout sous-groupe non trivial contient un élément u tel que $\mathrm{tr} u \in [-3, 1[$.
3. Soit

$$\chi : \begin{array}{ccc} \mathrm{SO}_3(\mathbf{R}) & \rightarrow & \mathrm{SO}_3(\mathbf{R}) \\ v & \mapsto & uvu^{-1}v^{-1}. \end{array}$$

Comme N est distingué, $\chi(v)$, qui est le produit de u et d'un conjugué de u^{-1} , est toujours un élément de N . En outre, comme $u \neq \mathrm{id}$, la première question entraîne l'existence d'un élément $v \in \mathrm{SO}_3(\mathbf{R})$ tel que $\chi(v) \neq \mathrm{id}$; soit $t_0 = \mathrm{tr} \chi(v) < 3$. L'application $\mathrm{tr} \circ \chi$ étant une application continue définie sur un ensemble connexe, son image est un intervalle. Puisqu'elle contient t_0 et $3 = \mathrm{tr} \mathrm{id} = \mathrm{tr} \chi(u)$, elle contient $[t_0, 1]$.

4. En particulier, on peut trouver dans N un élément de trace $1 + 2\cos(\pi/k)$ pour k assez grand. La réduction des isométries entraîne qu'un tel élément est conjugué à $\mathrm{diag}(1, R(\pi/k))$, donc d'ordre $2k$. Sa puissance k -ième est donc un élément d'ordre 2 de $\mathrm{SO}_3(\mathbf{R})$, et la réduction des isométries impose alors que c'est un retournement.

5. D'après les questions qui précèdent, tout sous-groupe distingué non trivial N de $SO_3(\mathbf{R})$ contient un retournement. Puisque ceux-ci forment une classe de conjugaison et une partie génératrice, cela impose $N = SO_3(\mathbf{R})$: le groupe $SO_3(\mathbf{R})$ est simple.

B. Simplicité de $PSO_n(\mathbf{R})$, $n \geq 5$.

1. On a un isomorphisme

$$\begin{array}{ccc} SO(F^\perp) & \rightarrow & G_F \\ u_0 & \mapsto & \text{l'unique } u \in SO_n(\mathbf{R}) \text{ tel que } \begin{cases} u|_F = \text{id}_F \\ u|_{F^\perp} = u_0, \end{cases} \end{array}$$

où $SO(F^\perp)$ désigne l'ensemble des isométries de $F^\perp$ pour le produit scalaire induit par le produit scalaire canonique de $\mathbf{R}^n$ (la réciproque de cet isomorphisme est simplement la restriction à $F^\perp$ d'un endomorphisme de G_F). En particulier, G_F est isomorphe à $SO_{n-\dim F}(\mathbf{R})$.

2. Soit u dans N différent de $\{\pm \text{id}\}$. Comme toute droite est l'intersection de deux plans, u , qui ne stabilise pas toutes les droites, ne peut pas non plus stabiliser tous les plans. Soit donc A un plan tel que $u(A) \neq A$. Observons que si ρ est le retournement d'axe A , le commutateur $u\rho u^{-1}\rho^{-1}$ est le produit des retournements $u\rho u^{-1}$, d'axe $u(A)$, et $\rho^{-1} = \rho$, d'axe A . En particulier, il vaut déjà l'identité sur $A^\perp \cap u(A)^\perp = (A + u(A))^\perp$, un espace de codimension ≤ 4 , forcément non trivial. En outre, comme $u(A) \neq A$, le commutateur n'est pas trivial : on a trouvé un élément $v \neq \text{id}$ fixant un vecteur unitaire (en particulier, ce n'est pas non plus $-\text{id}$).

3. Notre élément v n'appartient pas au centre de $O_n(\mathbf{R})$, donc il existe une réflexion avec laquelle v ne commute pas. Soit également x un vecteur unitaire fixé par v et s l'involution indirecte coïncidant avec $-\text{id}$ sur $\text{Vect}(s)$ et $-\text{id}$ sur $\text{Vect}(s)^\perp$: elle commute avec u .

Dans ces conditions, $[u, \tau s] = u\tau s u^{-1}s^{-1}\tau^{-1} = u\tau u^{-1}\tau^{-1}$ est le produit non trivial de deux réflexions : il fixe un espace de codimension ≤ 2 . Notons qu'on a bien $\tau s \in SO_n(\mathbf{R})$.

4. Soit $N \triangleleft SO_n(\mathbf{R})$ un sous-groupe distingué non inclus dans $\{\pm \text{id}\}$. Les questions précédentes impliquent en particulier qu'il existe un sous-espace F de dimension $n - 3$ tel que $N \cap G_F \neq \{\text{id}\}$. La partie précédente implique alors que N contient G_F tout entier. En particulier, N contient un retournement, donc $N = SO_n(\mathbf{R})$.

Cela permet de dresser la liste exhaustive des sous-groupes distingués de $SO_n(\mathbf{R})$: il y a $\{\text{id}\}$, $\{\pm \text{id}\}$ si n est pair, et $SO_n(\mathbf{R})$ tout entier. Cela démontre donc la simplicité de $PSO_n(\mathbf{R})$: si n est impair, tout est déjà dit et si n est pair, les sous-groupes distingués de $PSO_n(\mathbf{R})$ sont en bijection avec les sous-groupes de $SO_n(\mathbf{R})$ contenant $\{\pm \text{id}\}$ donc ils sont triviaux.

Exercice 5.

Vu les hypothèses, la classe de similitude de M est $\left\{ N \in M_2(M) \mid \text{tr } N = \text{tr } M \text{ et } \det N = \det M \right\}$ (n'oublions pas que deux matrices réelles semblables sur $\mathbf{C}$ le sont sur $\mathbf{R}$!) Quitte à translater par $-t/2I_2$, on peut supposer $\text{tr } M = 0$.

En paramétrant l'hyperplan affine $\{\text{tr } N = 0\}$ sous la forme $\left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \right\}$, le déterminant est la forme quadratique $\begin{bmatrix} a & b \\ c & -a \end{bmatrix} = -(a^2 + bc) = -a^2 + \frac{(b+c)^2}{4} - \frac{(b-c)^2}{4}$ qui est non dégénérée et de signature $+-$.

La quadrique est donc une hyperboloïde à une nappe si $\det M < 0$ (cas où M diagonalisable sur $\mathbf{R}$) et une hyperboloïde à deux nappes si $\det M > 0$ (cas non diagonalisable). Le cas $t = 0$ est exclu car il donne un spectre multiple (ce serait un point dans le cas de la matrice nulle et un cône épointé dans le cas d'une matrice nilpotente non nulle).

Notons que la connexité ou la non-connexité de la classe de similitude se voit directement : la classe de similitude est une orbite d'une action continue de $GL_n(\mathbf{R})$. Comme ce groupe a deux composantes connexes, l'orbite a soit une soit deux composantes connexes. Plus précisément (on note $\cdot$ l'action par conjugaison) :

$$\begin{aligned} \text{la classe de } M \text{ est connexe} &\Leftrightarrow GL_n^+(\mathbf{R}) \cdot M = GL_n^-(\mathbf{R}) \cdot M \\ &\Leftrightarrow \exists P \in GL_n^-(\mathbf{R}), Q \in GL_n^+(\mathbf{R}) : P \cdot M = Q \cdot M \\ &\Leftrightarrow \exists R \in GL_n^-(\mathbf{R}) : R \cdot M = M \\ &\Leftrightarrow \text{Stab}(M) \cap GL_n^-(\mathbf{R}) \neq \emptyset. \end{aligned}$$

On doit donc voir directement qu'une matrice inversible 2×2 commute avec une matrice de déterminant < 0 si et seulement si elle est diagonalisable. Un sens est clair : $\text{diag}(a, b)$ commute avec $\text{diag}(1, -1)$. Pour l'autre, remarquons qu'un calcul de discriminant montre qu'une matrice de déterminant < 0 est diagonalisable (sur $\mathbf{R}$) de spectre simple. Elle a donc deux droites propres. Une matrice commutant avec celle-là doit donc stabiliser les deux droites propres, ce qui la diagonalise.