TD8 : Groupe orthogonal (et symplectique)

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆
Soient K un corps de caractéristique $\neq 2$ et E un K-espace vectoriel de dimension finie. Soit q une forme quadratique non dégénérée sur E. Soit $u : E \to E$ une application (pas forcément linéaire a priori) telle que $u(0) = 0$ et pour tout $x, y \in E$, $q(u(x) - u(y)) = q(x - y)$.

a) Montrer que $u \in \mathrm{O}(E, q)$ (on pourra utiliser une base orthogonale).

b) L'hypothèse $u(0) = 0$ est-elle nécessaire ?

Solution de l'exercice 1.

a) On voit d'abord que pour tout $x \in E$, on a $q(u(x)) = q(x)$ (prendre $y = 0$ dans l'hypothèse). Ensuite, si on note b la forme polaire de q, on a pour tout $x, y \in E$, on a

$$q(u(x)) + q(u(y)) - 2b(u(x), u(y)) = q(u(x) - u(y)) = q(x - y) = q(x) + q(y) - 2b(x, y)\,,$$

donc $b(u(x), u(y)) = b(x, y)$.
On munit alors E d'une base orthogonale pour q, notée $(e_1, \ldots, e_n)$. Comme q est non dégénérée, on a $q(e_i) \neq 0$ pour tout i. Alors pour tout $i \neq j$, on a $b(u(e_i), u(e_j)) = b(e_i, e_j) = 0$ si $i \neq j$ et $q(e_i)$ si $i = j$. Cela assure que $(u(e_i))$ est une base orthogonale de (E, q).
Soit $x \in E$. On décompose $x = \sum_i \lambda_i e_i$ sur la base (e_i) et $u(x) = \sum_i \mu_i u(e_i)$ sur la base $(u(e_i))$. Pour montrer que u est linéaire, il suffit de montrer que $\lambda_i = \mu_i$ pour tout i. Pour cela, on calcule en utilisant l'orthogonalité des deux bases :

$$\mu_i q(e_i) = b(u(x), u(e_i)) = b(x, e_i) = \lambda_i q(e_i)$$

ce qui assure que $\lambda_i = \mu_i$ puisque $q(e_i) \neq 0$.
Donc u est linéaire, i.e. $u \in \mathrm{O}(E, q)$.

b) Oui. En effet, si l'on enlève l'hypothèse $u(0) = 0$, les applications vérifiant l'hypothèse sont exactement les isométries affines de (E, q), et il existe de telles isométries non linéaires dès que $E \neq \{0\}$ (par exemple, les translations de vecteur $\neq 0$).

Exercice 2 : ⋆
Soit E un $\mathbb{R}$-espace vectoriel de dimension finie $n \geq 1$.

a) Montrer que tout endomorphisme de E admet un sous-espace stable de dimension 1 ou 2.

b) Soit q une forme quadratique définie positive sur E. Montrer que pour tout $u \in \mathrm{O}(E, q)$, il existe une base orthonormée e de E, des entiers positifs r, s, t tels que $n = r + s + 2t$ et des réels $\theta_1, \ldots, \theta_t \in \mathbb{R} \setminus \pi\mathbb{Z}$, tels que

$$\mathrm{Mat}_e(u) = \begin{pmatrix} I_r & 0 & 0 & \ldots & 0 \\ 0 & -I_s & 0 & \ldots & 0 \\ 0 & 0 & R_{\theta_1} & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \ldots & R_{\theta_t} \end{pmatrix},$$

où R_θ désigne la matrice $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

c) En déduire que sous les hypothèses précédentes, $\mathrm{SO}(E,q)$ est connexe par arcs.

Solution de l'exercice 2.

a) Soit u un endomorphisme de E. On considère un polynôme $P \in \mathbb{R}[X]$ non nul et annulateur de u (par exemple le polynôme caractéristique). Il existe des polynômes $P_1, \dots, P_r$ de degré 1 ou 2 tels que $P = P_1 \dots P_r$. Alors $P(u) = P_1(u) \circ \cdots \circ P_r(u) = 0$, donc il existe $1 \leq i \leq r$ tel que $P_i(u)$ n'est pas injectif. Donc il existe $x \in Ker(P_i(u)) \setminus \{0\}$. Alors $\mathrm{Vect}_{\mathbb{R}}(x, u(x))$ est un sous-espace de dimension 1 ou 2 de E qui est stable par u.

b) Les cas $n = 1$ et $n = 2$ sont classiques (voir le cours). Le cas général se déduit de ces deux cas par une récurrence immédiate utilisant la question a) : on rappelle que si un sous-espace $F \subset E$ est stable par u, alors $F^{\perp}$ est stable par u.

c) Soit $u \in \mathrm{SO}(E,q)$. La question b) assure qu'il existe une base e de E dans laquelle la matrice P de u est de la forme susmentionnée. Comme $\det(u) = 1$, s est pair, donc on peut écrire P sous la forme

$$P = \begin{pmatrix} I_r & 0 & \dots & 0 \\ 0 & R_{\theta_1} & \dots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & R_{\theta_t} \end{pmatrix},$$

avec $\theta_i \in \mathbb{R}$. Pour tout $x \in [0;1]$, on pose

$$P(x) := \begin{pmatrix} I_r & 0 & \dots & 0 \\ 0 & R_{x\theta_1} & \dots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & R_{x\theta_t} \end{pmatrix}.$$

Alors l'application $f : [0;1] \to \mathrm{SO}_n(\mathbb{R})$ définie par $x \mapsto P(x)$ est bien définie et continue, et $P(0) = I_n$, $P(1) = P$. Cela assure la connexité par arcs de $\mathrm{SO}(E,q)$.

Exercice 3 : $\star\star$

Soit $\mathbb{F}_q$ un corps fini à q éléments, de caractéristique différente de 2. Soient $n \geq 1$, $b \in \mathbb{F}_q$ et $\varepsilon \in \mathbb{F}_q^{\times} \setminus \mathbb{F}_q^{\times 2}$. Notons $S(2n,b)$, $S(2n+1,b)$ et $S_\varepsilon(2n,b)$ les nombres respectifs de solutions des équations

$$x_1^2 - y_1^2 + \cdots + x_n^2 - y_n^2 = b, \tag{1}$$
$$x_1^2 - y_1^2 + \cdots + x_n^2 - y_n^2 + x_{n+1}^2 = b, \tag{2}$$
$$x_1^2 - y_1^2 + \cdots + x_n^2 - \varepsilon y_n^2 = b. \tag{3}$$

a) Montrer

$$S(2n,b) = \begin{cases} q^{2n-1} + q^n - q^{n-1} & \text{si } b = 0; \\ q^{2n-1} - q^{n-1} & \text{si } b \neq 0; \end{cases}$$

$$S(2n+1,b) = \begin{cases} q^{2n} & \text{si } b = 0; \\ q^{2n} - q^n & \text{si } b \notin \mathbb{F}_q^{\times 2}; \\ q^{2n} + q^n & \text{si } b \in \mathbb{F}_q^{\times 2}; \end{cases}$$

$$S_\varepsilon(2n,b) = \begin{cases} q^{2n-1} - q^n + q^{n-1} & \text{si } b = 0; \\ q^{2n-1} + q^{n-1} & \text{si } b \neq 0. \end{cases}$$

b) En déduire

$$|\mathrm{O}_{2n+1}(\mathbb{F}_q)| = 2q^{n^2}\prod_{i=1}^{n}(q^{2i}-1),$$
$$|\mathrm{O}^+_{2n}(\mathbb{F}_q)| = 2q^{n(n-1)}(q^n-1)\prod_{i=1}^{n-1}(q^{2i}-1),$$
$$|\mathrm{O}^-_{2n}(\mathbb{F}_q)| = 2q^{n(n-1)}(q^n+1)\prod_{i=1}^{n-1}(q^{2i}-1).$$

Solution de l'exercice 3.

a) On montre les formules (1), (2) et (3) par récurrence sur k. Soit $b \in \mathbb{F}_q$. On a clairement

$$S(1,b) = \begin{cases} 1 & \text{si } b = 0; \\ 0 & \text{si } b \notin \mathbb{F}_q^{\times 2}; \\ 2 & \text{si } -b \in \mathbb{F}_q^{\times 2}. \end{cases}$$

Calculons $S(2,b)$. Si $b=0$, l'équation $(x_1-y_1)(x_2-y_2)=0$ a $2q-1$ solutions. Si $b \neq 0$, elle a les $q-1$ solutions suivantes

$$x_1 = \frac{1}{2}\left(\frac{b}{c}+c\right), \qquad y_1 = \frac{1}{2}\left(\frac{b}{c}-c\right), \qquad c \in \mathbb{F}_q^\times.$$

Calculons enfin $S_\varepsilon(2,b)$. Soit $K = \mathbb{F}_q[\sqrt{d}]$. On a $K \simeq \mathbb{F}_{q^2}$ et les éléments de K s'écrivent sous la forme $x+y\sqrt{d}$, avec $x,y \in \mathbb{F}_q$. On définit la norme $N(x+y\sqrt{d}) = x^2-dy^2$. On constate que $S_\varepsilon(2,b)$ est le nombre d'éléments de K de norme b. Or $N : K^* \to \mathbb{F}_q^*$ est un morphisme de groupes surjectif, son noyau ayant pour cardinal $q+1$. On en déduit que $S_\varepsilon(2,b) = q+1$.
Remarque : les quantités $S(2,b)$ et $S_\varepsilon(2,b)$ s'interprètent géométriquement comme les nombres de points à coordonnées dans $\mathbb{F}_q$ de coniques (non dégénérées) définies dans le plan affine $(\mathbb{F}_q)^2$. Or il est classique que l'ensemble des points d'une conique *projective* non dégénérée et non vide sur un corps quelconque est en bijection (cette bijection étant donnée par des fractions rationnelles) avec la droite projective sur ce corps (considérer par exemple l'ensemble des droites passant par un point fixé de la conique, et regarder l'intersection de ces droites avec la conique). Cela assure qu'une conique projective non dégénérée sur $\mathbb{F}_q$ (qui est non vide : compter les carrés dans $\mathbb{F}_q$) a exactement $q+1$ points. Pour passer à une conique affine, il suffit de regarder le nombre de points de notre conique projective sur la droite à l'infini dans $\mathbb{P}^2(\mathbb{F}_q)$: dans le cas de $S(2,b)$, ce nombre vaut 2 ; dans le cas de $S_\varepsilon(2,b)$, ce nombre vaut 0. Cela explique les deux entiers obtenus.
Montrons maintenant par récurrence la formule (1) pour n quelconque. Les solutions de (1) sont exactement les solutions de l'équation

$$x_1^2 - y_1^2 + \cdots + x_{n-1}^2 - y_{n-1}^2 = a, \qquad x_n^2 - y_n^2 = b-a, \qquad a \in \mathbb{F}_q. \tag{4}$$

Si $b=0$, le nombre de solution vaut donc

$$\begin{aligned} & S(2(n-1),0)S(2,0) + \sum_{a\in\mathbb{F}_q^\times} S(2(n-1),a)S(2,b-a) \\ = \;& (q^{2n-3}+q^{n-1}-q^{n-2})(2q-1) + (q-1)(q^{2n-3}-q^{n-2})(q-1) \\ = \;& q^{2n-1}+q^n-q^{n-1} \end{aligned}$$

Si $b \neq 0$, le nombre des solutions de (1) vaut

$$\begin{aligned} & S(2(n-1),0)S(2,b) + S(2(n-1),-b)S(2,0) + \sum_{a\in\mathbb{F}_q^\times, a\neq -b} S(2(n-1),a)S(2,b-a) \\ = \;& (q^{2n-3}+q^{n-1}-q^{n-2})(2q-1) + (q^{2n-3}-q^{n-2})(2q-1) + (q-2)(q^{2n-3}-q^{n-2})(q-1) \\ = \;& q^{2n-1}-q^{n-1}. \end{aligned}$$

Les formules (2) et (3) se prouvent exactement de la même façon.

b) Montrons $|\mathrm{O}^+_{2n}(\mathbb{F}_q)| = 2q^{n(n-1)}(q^n-1)\prod_{i=1}^{n-1}(q^{2i}-1)$ (les autres formules se prouvent de façon analogue).

Le cas où $n=1$ a été fait en cours (et le cas $n=0$ est évident). On prouve le cas général par récurrence.

Soit $Q(x_1,y_1,\ldots,x_n,y_n) = x_1^2 - y_1^2 + \cdots + x_n^2 - y_n^2$. Alors $\mathrm{O}^+_{2n}(\mathbb{F}_q) = \mathrm{O}((\mathbb{F}_q)^{2n}, Q)$. Soit $v \in \mathbb{F}_q^{2n}$ tel que $Q(v) = 1$ (un tel v existe). Il est facile de voir que l'orbite de v sous l'action de $\mathrm{O}_{2n}(Q,\mathbb{F}_q)$ est l'ensemble des $w \in \mathbb{F}_q^{2n}$ tels que $Q(w) = 1$ (on peut par exemple compléter v et w en deux bases orthogonales et considérer la matrice de passage).

On a donc $|\mathrm{Orb}(v)| = S(2n,1) = q^{2n-1} - q^{n-1}$. D'un autre côté, puisque $\mathbb{F}_q^{2n} = \langle v\rangle \oplus \langle v\rangle^\perp$, on a $\mathrm{Stab}(v) = \mathrm{O}(\langle v\rangle^\perp) = \mathrm{O}_{2n-1}(\mathbb{F}_q)$.

On en déduit les formules suivantes en utilisant l'hypothèse de récurrence (le cardinal de $\mathrm{O}_{2n-1}(\mathbb{F}_q)$) :

$$\begin{aligned} |\mathrm{O}^+_{2n}(\mathbb{F}_q)| &= |\mathrm{Orb}(v)||\mathrm{Stab}(v)| \\ &= (q^{2n-1}-q^{n-1})2q^{(n-1)^2}\prod_{i=1}^{n-2}(q^{2i}-1) \\ &= 2q^{n(n-1)}(q^n-1)\prod_{i=1}^{n-1}(q^{2i}-1). \end{aligned}$$

Comme mentionné plus haut, les deux autres cas se prouvent de manière similaire.

Exercice 4 : $\star\star$

Soit V un $\mathbb{R}$-espace vectoriel de dimension 3 muni de la forme quadratique définie positive $f(x_1,x_2,x_3) = x_1^2+x_2^2+x_3^2$. Le but de cet exercice est de montrer que $\mathrm{SO}(V,f)$ est simple. Soit N un sous-groupe distingué non trivial de $\mathrm{SO}(V,f)$.

a) Montrer que si N contient un renversement, alors $N = \mathrm{SO}(V,f)$.

b) Soit N_0 la composante connexe de l'identité de N. Montrer que N_0 est un sous-groupe distingué de $\mathrm{SO}(V,f)$.

c) Montrer que $N = \{\mathrm{id}\}$ si et seulement si $N_0 = \{\mathrm{id}\}$.

d) Montrer que la fonction

$$\begin{aligned} \varphi : N_0 &\longrightarrow [-1,1] \\ g &\longmapsto \frac{\mathrm{tr}(g)-1}{2} \end{aligned}$$

est bien définie et continue.

e) Montrer qu'il existe $g \in N_0$ tel que $\varphi(g) \leq 0$.

f) Montrer qu'il existe $g \in N_0$ tel que $\varphi(g) = 0$.

g) Conclure.

Solution de l'exercice 4.

a) Le cours assure que les renversements engendrent $\mathrm{SO}(V,f)$. Montrons que tous les renversements sont conjugués dans $\mathrm{SO}(V,f)$. Remarquons d'abord qu'en dimension 3, un renversement n'est autre qu'un demi-tour autour d'une droite, i.e. une rotation d'angle π. Soient r_1 et r_2 deux renversements d'axes respectifs Δ_1 et Δ_2. Pour montrer que r_1 et r_2 sont conjugués, il suffit de montrer qu'il existe $u \in \mathrm{SO}(V,f)$ tel que $u(\Delta_1) = \Delta_2$. Et ceci est évident puisque par exemple $\mathrm{SO}(V,f)$ agit transitivement sur l'ensemble des vecteurs de V de norme 1. Donc les renversements engendrent $\mathrm{SO}(V,f)$ et sont tous conjugués, or N est distingué, donc N contient un renversement si et seulement si $N = \mathrm{SO}(V,f)$.

b) Vérifions les faits classiques suivants : tout d'abord, la multiplication $m : \mathrm{SO}(V,f)\times\mathrm{SO}(V,f) \to \mathrm{SO}(V,f)$ est continue, donc $m(N_0 \times N_0) \subset N$ est connexe et contient id, donc il est contenu dans N_0, donc N_0 est stable par composition. De même, il est stable par inverse. Or il contient id, donc N_0 est un sous-groupe de N. Pour tout $g \in \mathbb{N}$, le morphisme $c_g : \mathrm{SO}(V,f) \to \mathrm{SO}(V,f)$ défini par $c_g(x) := gxg^{-1}$ est continu, donc $c_g(N_0) \subset N$ est connexe et contient id, donc $c_g(N_0) \subset N_0$, ce qui assure que N_0 est distingué dans N.

c) Le sens direct est évident. Montrons la réciproque : on suppose donc $N_0 = \{\mathrm{id}\}$. Soit $g \in N$. L'application $\varphi_g : \mathrm{SO}(V,f) \to N$ définie par $h \mapsto [h,g]$ est continue, donc $\mathrm{Im}\,(\varphi_g) \subset N_0 = \{\mathrm{id}\}$. Cela assure que $g \in Z(\mathrm{SO}(V,f))$, donc $N \subset Z(\mathrm{SO}(V,f))$. Or le cours assure que $Z(\mathrm{SO}(V,f)) = \{\mathrm{id}\}$, donc $N = \{\mathrm{id}\}$.

d) Il est clair que φ est continue (c'est la restriction d'une application linéaire). Pour tout $r \in \mathrm{SO}(V,f)$, l'exercice 2 assure qu'il existe une base e de V et $\theta \in [0, 2\pi[$ tels que

$$\mathrm{Mat}_e(r) = \begin{pmatrix} 1 & 0 \\ 0 & R_\theta \end{pmatrix},$$

donc $\varphi(r) = \cos(\theta)$. Cela assure que φ est bien à valeurs dans $[-1;1]$.

e) Puisque $N \neq \{id\}$, la question c) assure que $N_0 \neq \{\mathrm{id}\}$. Donc il existe $g \neq \mathrm{id}$ dans N_0. Notons $\varphi(g) = \cos(\theta)$, avec $\theta \in]-\pi;\pi] \setminus \{0\}$. Or $g^{-1} \in N_0$, et $\varphi(g^{-1}) = -\theta$, donc on supposer que $\theta \in]0;\pi]$.
Si $\frac{\pi}{2} \leq \theta \leq \pi$, le résultat est démontré.
Sinon, on pose $N := E\left(\frac{\pi}{2\theta}\right)$. On a alors

$$N\theta \leq \frac{\pi}{2} < (N+1)\theta \leq \frac{\pi}{2} + \theta \leq \pi,$$

donc $s := g^{N+1} \in N_0$ convient.

f) Le groupe N_0 est connexe, et φ est clairement continue, donc $\varphi(N_0)$ est un connexe de $[-1,1]$ contenant $\varphi(g) \leq 0$ et $\varphi(\mathrm{id}) = 1$. Or, les connexes de $\mathbb{R}$ sont les intervalles, donc il existe $g \in N$ tel que $\varphi(g) = 0$, c'est-à-dire que N_0 contient une rotation d'angle $\pm\frac{\pi}{2}$. Alors l'élément $R := g^2 \in N_0$ est donc un renversement. Donc la question a) assure que $N = \mathrm{SO}(V,f)$, donc $\mathrm{SO}(V,f)$ est un groupe simple.

Exercice 5 : $\star\star$

Soit V un $\mathbb{R}$-espace vectoriel de dimension $n \geq 5$ muni de la forme quadratique définie positive $f(x_1,\ldots,x_n) = x_1^2 + \cdots + x_n^2$. Le but de cet exercice est de montrer que $\mathrm{PSO}(V,f)$ est simple. Soit $\overline{N}$ un sous-groupe distingué non trivial de $\mathrm{PSO}(V,f)$ et soit N le sous-groupe de $\mathrm{SO}(V,f)$ lui correspondant.

a) Montrer que si N contient un renversement, alors $\overline{N} = \mathrm{PSO}(V,f)$.

b) Supposons qu'il existe un sous-espace U de V de dimension 3 tel que $N \cap \mathrm{SO}(U, f|_U) \neq \{\mathrm{id}\}$. Montrer qu'alors $\overline{N} = \mathrm{PSO}(V,f)$.

c) Conclure (on pourra considérer le commutateur d'un élément $r \in N \setminus \{\pm\mathrm{id}\}$ ayant un vecteur fixe non nul avec la composée de deux réflexions bien choisies).

Solution de l'exercice 5.

a) C'est exactement le même raisonnement que la question a) de l'exercice 4 : les renversements engendrent $\mathrm{SO}(V,f)$ et sont tous conjugués dans $\mathrm{SO}(V,f)$.

b) Par hypothèse, $N' := N \cap \mathrm{SO}(U,f)$ est un sous-groupe distingué non trivial de $\mathrm{SO}(U,f)$. Donc l'exercice 4 assure que $N' = \mathrm{SO}(U,f)$, donc N' contient un renversement r de (U,f). Il suffit alors de prolonger r en $r' \in \mathrm{SO}(V,f)$ en demandant que $r'_{|_{U^\perp}} = \mathrm{id}_{U^\perp}$, ce qui fournit un renversement $r' \in N$, donc par la question a), on a $\overline{N} = \mathrm{PSO}(V,f)$.

c) On cherche à construire un sous-espace U de dimension 3 satisfaisant les hypothèses de la question précédente. Comme $N \neq \{\pm id\}$, il existe $u \in N$ tel que $u \neq \pm\mathrm{id}$. Par conséquent, il existe un plan $P \subset V$ tel que $u(P) \neq P$. Notons $r \in \mathrm{SO}(V,f)$ le renversement de plan P. On pose $\rho := [u,r]$. Alors $\rho \in N$ car N est distingué, et ρ est le produit de deux renversements, à savoir uru^{-1} renversement de plan $u(P)$, et r^{-1} renversement de plan P. Donc cela assure que la restriction de ρ à $P^\perp \cap u(P)^\perp$ est l'identité. Or $\dim(P^\perp \cap u(P)^\perp) \geq n-4 \geq 4$ (car $n \geq 5$). Donc ρ a un vecteur fixe $a \in V \setminus \{0\}$. Remarquons également que $\rho \neq \pm\mathrm{id}$ car $u(P) \neq P$.

Il existe également $b \in V$ tel que la famille $(b, \rho(b))$ soit libre. On note $c := \rho(b)$.

Définissons $\sigma := s_b \circ s_a$ (où s_x désigne la réflexion orthogonale d'hyperplan $x^\perp$), et considérons $s := [\rho, \sigma]$. Alors comme N est distingué, on voit que $s \in N$. Et on vérifie que

$$s = s_{\rho(b)} s_{\rho(a)} s_a s_b = s_c s_a s_a s_b = s_c s_b$$

est un produit de deux réflexions distinctes, donc $s \in N$ fixe un sous-espace $W \subset V$ de dimension $n-2$ et $s \neq \pm\mathrm{id}$. Alors il suffit de considérer un sous-espace $U \subset V$ de dimension 3 contenant $H^\perp$, et de considérer l'élément $s \in N \cap \mathrm{SO}(U,f)$, puis de conclure via la question b).

Exercice 6 : $\star\star$

On note $\mathbb{Z}_{(2)}$ le sous-anneau de $\mathbb{Q}$ formé des rationnels à dénominateur impair. On note $G = \mathrm{O}_3(\mathbb{Q})$.

a) Montrer que $G \subset \mathrm{Mat}_3(\mathbb{Z}_{(2)})$.

b) Pour tout $n \in \mathbb{N}^*$, on pose $G_n := \{A \in G : \exists B \in \mathrm{Mat}_3(\mathbb{Z}_{(2)}),\ A = I_3 + 2^n B\}$. Montrer que G_n est un sous-groupe distingué de G.

c) Montrer que $\bigcap_{n\in\mathbb{N}^*} G_n = \{I_3\}$.

d) Montrer que $G_1 \subsetneq G$ et que $G_1 \not\subset \mathrm{SO}_3(\mathbb{Q})$.

e) Montrer que pour tout $n \geq 1$, $G_{n+1} \subsetneq G_n$.

f) Montrer que pour tout $n \geq 2$, $G_n \subset \mathrm{SO}_3(\mathbb{Q})$.

g) Pour tout $n \geq 2$, montrer que $G_n/G_{n+1} \cong (\mathbb{Z}/2\mathbb{Z})^3$.

h) Montrer que $G/G_1 \cong \mathfrak{S}_3$.

i) Montrer que $G_1/G_2 \cong (\mathbb{Z}/2\mathbb{Z})^4$.

j) Comparer la structure de $\mathrm{O}_3(\mathbb{Q})$ avec celle de $\mathrm{O}_3(\mathbb{R})$.

Solution de l'exercice 6. Remarquons pour commencer que le quotient de l'anneau $\mathbb{Z}_{(2)}$ par l'idéal (2^n) engendré par l'élément 2^n est canoniquement isomorphe à $\mathbb{Z}/2^n\mathbb{Z}$, ce qui permet de formuler certaines démonstrations qui suivent de façon un peu plus concise. Par soucis de simplicité, on n'utilisera pas explicitement cette description dans ce corrigé.

a) Soit $A \in G$, et soit $(x,y,z) \in \mathbb{Q}^3$ un vecteur colonne de A. Alors on a $x^2+y^2+z^2 = 1$. Supposons que l'un des rationnels x,y,z ait un dénominateur pair. On multiplie alors l'égalité précédente par le ppcm des dénominateurs pour obtenir une inégalité du type

$$a^2 + b^2 + c^2 = d^2$$

avec $a,b,c,d \in \mathbb{Z}$, d pair et a, b ou c impair. Par symétrie, supposons a impair. On réduit cette égalité modulo 4. On obtient

$$1 + b^2 + c^2 \equiv 0\,[4]\,.$$

Or les seuls carrés dans $\mathbb{Z}/4\mathbb{Z}$ sont 0 et 1, donc l'égalité précédente modulo 4 est contradictoire. Cela assure que tous les dénominateurs des coefficients de A sont impairs, donc $A \in \mathrm{Mat}_3(\mathbb{Z}_{(2)})$.

b) Un calcul simple assure que G_n est un sous-groupe distingué de G.

c) Soit $A = (a_{i,j}) \in \bigcap_{n\in\mathbb{N}^*} G_n$. Alors pour tout $i \neq j$, pour tout $n \geq 1$, le numérateur de $a_{i,j}$ est divisible par 2^n, donc $a_{i,j} = 0$. Et pour tout i, il existe $b \in \mathbb{Z}_{(2)}$ tel que $a_{i,i} = 1 + 4b$, et $a_{i,i} \in \{\pm 1\}$, donc $a_{i,i} = 1$. Donc $A = I_3$.

d) On considère la matrice de permutation suivante

$$A := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} .$$

Il est clair que $A \in G$ et $A \notin G_1$.
De même, la matrice

$$B := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

est dans G_1 mais pas dans $\mathrm{SO}_3(\mathbb{Q})$.

e) L'inclusion $G_{n+1} \subset G_n$ est évidente. Montrons qu'elle est stricte. Pour cela, on considère, dans le cas $n \geq 2$, la matrice

$$A_n := \begin{pmatrix} \frac{1-4^{n-1}}{1+4^{n-1}} & \frac{2^n}{1+4^{n-1}} & 0 \\ -\frac{2^n}{1+4^{n-1}} & \frac{1-4^{n-1}}{1+4^{n-1}} & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3 + 2^n \begin{pmatrix} -\frac{2^{n-1}}{1+4^{n-1}} & \frac{1}{1+4^{n-1}} & 0 \\ -\frac{1}{1+4^{n-1}} & -\frac{2^{n-1}}{1+4^{n-1}} & 0 \\ 0 & 0 & 0 \end{pmatrix} .$$

On voit donc que $A_n \in G_n \setminus G_{n+1}$.
Dans le cas $n = 1$, on considère la matrice

$$A_1 := \begin{pmatrix} \frac{1}{3} & \frac{2}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} & -\frac{2}{3} \\ \frac{2}{3} & -\frac{2}{3} & \frac{1}{3} \end{pmatrix} = I_3 + 2 \begin{pmatrix} -\frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} \\ \frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} \end{pmatrix} .$$

Donc $A_1 \in G_1$ et $A_1 \notin G_2$. Une variante est donnée par la matrice $B_1 := \mathrm{diag}(1, 1, -1)$.

f) Soit $A \in G_n$, avec $n \geq 2$. Par définition, il existe $B \in \mathrm{Mat}_3(\mathbb{Z}_{(2)})$ tel que $A = I_3 + 4B$. La multilinéarité du déterminant assure que $\det(A) = 1 + 4d$, pour un certain $d \in \mathbb{Z}_{(2)}$. Or A est orthogonale, donc $\det(A) \in \{\pm 1\}$, et l'égalité précédente assure que $\det(A) = 1$ (car 4 ne divise pas 2 dans l'anneau $\mathbb{Z}_{(2)}$). Donc $G_n \subset \mathrm{SO}_3(\mathbb{Q})$.

g) On considère l'application $\pi_n : G_n \to \mathrm{Mat}_3(\mathbb{Z}/2\mathbb{Z})$ définie par $\pi_n(I_3 + 2^n B) := \overline{B}$, où si $B = (b_{i,j})$, les coefficients $(\overline{b_{i,j}})$ de $\overline{B}$ sont définis par $\overline{b_{i,j}} = 0$ si le numérateur de $b_{i,j}$ est pair, et $\overline{b_{i,j}} = 1$ si celui-ci est impair. On vérifie que π_n est un morphisme de groupes, notamment que $\pi_n(AA') = \pi_n(A) + \pi_n(B)$. En outre, il est clair que $\mathrm{Ker}(\pi_n) = G_{n+1}$, donc le théorème de factorisation assure que π_n induit un morphisme injectif

$$\overline{pi}_n : G_n/G_{n+1} \to \mathrm{Mat}_3(\mathbb{Z}/2\mathbb{Z}) .$$

Or pour tout $A = I_3 + 2^n B \in G_n$, on a $A^t A = I_3$, donc $B + {}^t B + 2^n B^t B = 0$. Par conséquent, en regardant cette égalité modulo 2, on voit que

$$\mathrm{Im}\,(\overline{\pi}_n) \subset \{B \in \mathrm{Mat}_3(\mathbb{Z}/2\mathbb{Z}) : b_{i,j} = b_{j,i} \text{ et } b_{i,i} = 0 \,\forall i, j\} \cong (\mathbb{Z}/2\mathbb{Z})^3 .$$

Enfin, on voit que cette inclusion est une égalité en regardant l'image par π_n de la matrice A_n introduite à la question e), ainsi que les matrices obtenues à partir de A_n en permutant les vecteurs de la base. Donc finalement $G_n/G_{n+1} \cong (\mathbb{Z}/2\mathbb{Z})^3$

h) On considère le morphisme de groupes $\pi_0 : G \to \mathrm{O}_3(\mathbb{F}_2)$ défini par $\pi_0(A) := \overline{A}$, où $\overline{A}$ est défini comme en g) et $\mathrm{O}_3(\mathbb{F}_2)$ désigne l'ensemble des matrices A de $\mathrm{Mat}_3(\mathbb{F}_2)$ telles que ${}^t AA = A^t A = I_3$. Un calcul simple assure que $\mathrm{O}_3(\mathbb{F}_2) \cong \mathfrak{S}_3$ via les matrices de permutations. Or toute matrice de permutations dans G s'envoie par π_0 sur la matrice de permutations correspondante dans $\mathrm{O}_3(\mathbb{F}_2)$, ce qui assure que π_0 est surjectif. Enfin, par définition, on a bien $\mathrm{Ker}(\pi_0) = G_1$, donc $G/G_1 \cong \mathfrak{S}_3$.

i) On raisonne comme en g). On considère le morphisme de groupes $\pi_1 : G_1 \to \mathrm{Mat}_3(\mathbb{Z}/2\mathbb{Z})$ définie par $\pi_1(I_3 + 2B) := \overline{B}$. On a toujours $\mathrm{Ker}(\pi_1) = G_2$, et l'image de π_1 se calcule en réduisant modulo 2 l'égalité déjà rencontrée $B + {}^tB + 2B{}^tB = 0$: on voit que $\mathrm{Im}\,(\pi_1)$ est contenu dans $\{B \in \mathrm{Mat}_3(\mathbb{Z}/2\mathbb{Z}) : b_{i,j} = b_{j,i} \text{ et } \sum_{k\neq i} b_{i,k} = 0\,\forall i,j\}$. Or ce dernier sous-groupe de $\mathrm{Mat}_2(\mathbb{Z}/2\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^4$, engendré par les trois matrices ayant un unique coefficient non nul, situé sur la diagonale, et par la matrice dont tous les coefficients valent 1. Et ces quatre matrices sont bien dans l'image de π_1, ce que l'on voit en utilisant les matrices A_1 et B_1 de la question e). Donc $G_1/G_2 \cong (\mathbb{Z}/2\mathbb{Z})^4$.

j) Il suffit de reprendre toutes les questions précédentes. Le groupe $\mathrm{O}_3(\mathbb{Q})$ n'est pas du tout un groupe simple (ni $\mathrm{SO}_3(\mathbb{Q})$), contrairement à $\mathrm{SO}_3(\mathbb{R})$. En fait, on a montré que $G = \mathrm{O}_3(\mathbb{Q})$ est un groupe pro-résoluble, au sens où la suite de sous-groupes $D^n(G)$ vérifie $\bigcap_{n\in\mathbb{N}} D^n(G) = \{\mathrm{id}\}$. Plus précisément, on peut dire que G est une limite (projective dénombrable) de groupes résolubles finis.

Exercice 7 : $\star\star\star$

Soient $K = \mathbb{F}_q$ un corps fini de caractéristique impaire et $n \in \mathbb{N}^*$. On note $\mathrm{P}\Omega_n^{\pm}(K)$ le quotient du groupe dérivé de $\mathrm{O}_n^{\pm}(K)$ par son centre.

a) Déterminer $\mathrm{O}_1(K)$, $\mathrm{SO}_1(K)$ et $\mathrm{P}\Omega_1(K)$.

b) Montrer que $\mathrm{O}_2^+(K)$ est isomorphe au groupe diédral D_{q-1}. Identifier $\mathrm{SO}_2^+(K)$ et $\mathrm{P}\Omega_2^+(K)$.

c) En considérant le corps $\mathbb{F}_{q^2}$, montrer que $\mathrm{O}_2^-(K)$ est isomorphe à D_{q+1} et identifier $\mathrm{SO}_2^-(K)$ et $\mathrm{P}\Omega_2^-(K)$.

d) On suppose $n = 3$. On note V le K-espace vectoriel des matrices 2×2 de trace nulle.

i) Exhiber une base naturelle de V comme K-espace vectoriel.

ii) Montrer que $\mathrm{GL}_2(K)$ agit naturellement sur V.

iii) En déduire un morphisme de groupes $\rho : \mathrm{GL}_2(K) \to \mathrm{GL}(V) \cong \mathrm{GL}_3(K)$ que l'on explicitera.

iv) Montrer que $Ker(\rho) = K^*I_2$.

v) Montrer que pour tout $A \in \mathrm{GL}_2(K)$, $\det(\rho(A)) = 1$.

vi) Vérifier que le déterminant définit une forme quadratique non dégénérée sur V.

vii) En déduire des isomorphismes $\mathrm{PGL}_2(K) \cong \mathrm{SO}(V, \det) \cong \mathrm{SO}_3(K)$.

viii) Montrer que l'on a des isomorphismes $\mathrm{PGL}_2(K) \times \{\pm 1\} \cong \mathrm{O}(V, \det) \cong \mathrm{O}_3(K)$.

ix) Montrer que $\mathrm{P}\Omega_3(K) \cong \mathrm{PSL}_2(K)$.

e) On suppose $n = 4$. On note $W := \mathrm{Mat}_2(K)$, et pour tout $M \in W$, on note $Q(M) := \det(M)$.

i) Montrer que Q est une forme quadratique sur W qui est somme de deux plans hyperboliques.

ii) Montrer que $\mathrm{GL}_2(K) \times \mathrm{GL}_2(K)$ agit naturellement sur W.

iii) Soit $A, B \in \mathrm{GL}_2(K)$. Montrer que l'action de (A, B) sur W préserve Q si et seulement si $\det(A) = \det(B)$, et que cette action est triviale si et seulement s'il existe $\lambda \in K^*$ tel que $A = B = \lambda I_2$.

iv) En déduire un morphisme de groupes injectif $i : ((\mathrm{SL}_2(K) \times \mathrm{SL}_2(K)) \rtimes K^*)/K^* \to \mathrm{O}(W, Q)$, où l'on explicitera le groupe de gauche.

v) Montrer que $\langle \mathrm{Im}\,(i), T\rangle = \mathrm{O}(W, Q)$, où $T : W \to W$ est défini par $T(M) := {}^tM$ et décrire $\mathrm{SO}(W, Q)$.

vi) En déduire que $\mathrm{P}\Omega_4^+(K) \cong \mathrm{PSL}_2(K) \times \mathrm{PSL}_2(K)$ si $|K| > 3$.

vii) Décrire $\mathrm{P}\Omega_4^+(\mathbb{F}_3)$.

Solution de l'exercice 7.

a) Il est clair que $\mathrm{O}_1(K) = \{\pm 1\}$, $\mathrm{SO}_1(K) = \{1\}$ et $\mathrm{P}\Omega_1(K) = \{1\}$.

b) Le cours (ou un calcul simple) assure que

$$\mathrm{O}_2^+(K) = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} : \lambda \in K^* \right\} \bigcup \left\{ \begin{pmatrix} 0 & \mu \\ \mu^{-1} & 0 \end{pmatrix} : \mu \in K^* \right\}.$$

Or K^* est un groupe cyclique, donc en notant ζ un générateur de ce groupe, on pose

$$R := \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \text{ et } S := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

On voit alors que $\mathrm{O}_2^+(K) = \langle R, S \rangle$, que $\mathrm{O}_2^+(K)$ est d'ordre $2(q-1)$, que R est d'ordre $q-1$, S est d'ordre 2, et $RS = SR^{-1}$, ce qui assure que $\mathrm{O}_2^+(K)$ est isomorphe au groupe diédral D_{q-1} (groupe des isométries planes réelles d'un polygone régulier à $q-1$ côtés), l'isomorphisme envoyant R sur la rotation de centre O (isobarycentre des sommets du polygone) et d'angle $\frac{2\pi}{q-1}$ et S sur une symétrie axiale d'axe joignant deux sommets du polygone. On en déduit que $\mathrm{SO}_2^+(K) = \langle R \rangle \cong \mathbb{Z}/(q-1)\mathbb{Z}$ et $\mathrm{P}\Omega_2^+(K) = \{1\}$.

c) On fixe un élément $\varepsilon \in K^* \setminus (K^*)^2$, et on définit $L := K(\sqrt{\varepsilon}) := \{x + y\sqrt{\varepsilon} : x, y \in K\}$ (que l'on peut aussi définir comme $L := K[X]/(X^2 - \varepsilon)$). Il est clair que L est un corps contenant K comme sous-corps, de sorte que L est un K-espace vectoriel de dimension 2. On munit L de l'application "norme" $N : L \to K$ définie par $N(x + y\sqrt{\varepsilon}) := x^2 - \epsilon y^2$. Il est clair que N est une form quadratique sur le K-espace vectoriel L, de sorte que $\mathrm{O}(L, N) \cong \mathrm{O}_2^-(K)$. En outre, on voit que N induit un morphisme de groupes $N : L^* \to K^*$ tel que $N(x) = x^{q+1}$ pour tout $x \in L^*$. Puisque L^* est cyclique de cardinal $q^2 - 1$, on voit que N est surjectif de noyau $A := \{x \in L^* : x^{q+1} = 1\}$ cyclique de cardinal $q+1$. Or, pour tout $x \in A$, on définit $m_x : L \to L$ par $m_x(y) := xy$. Il est clair que m_x est K-linéaire et pour tout $y \in L$, on a bien $N(m_x(y)) = N(xy) = N(x)N(y) = N(y)$, donc $m_x \in \mathrm{O}(L, N)$. On en déduit donc un morphisme de groupes injectif $A \hookrightarrow \mathrm{SO}(L, N)$ défini par $x \mapsto m_x$ (il est clair que $\det(m_x) = 1$). On dispose également de l'automorphisme de Frobenius $\mathrm{Fr} : L \to L$ défini par $\mathrm{Fr}(x) := x^q$: on voit que $\mathrm{Fr} \in \mathrm{O}(L, N) \setminus \mathrm{SO}(L, N)$ et que Fr est d'ordre 2. Par cardinalité (voir exercice 3), on en déduit que $\langle A, \mathrm{Fr} \rangle = \mathrm{O}(L, N)$. On vérifie enfin que $m_x \circ \mathrm{Fr} = \mathrm{Fr} \circ m_x^{-1}$, ce qui assure que $\mathrm{O}_2^-(K) \cong D_{q+1}$, $\mathrm{SO}_2^-(K) \cong \mathbb{Z}/(q+1)\mathbb{Z}$ et $\mathrm{P}\Omega_2^-(K) = \{1\}$.

d) i) Une base de V est donnée par les matrices suivantes :

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

ii) L'action de $\mathrm{GL}_2(K)$ sur V est définie par $A \cdot M := AMA^{-1}$ pour tout $A \in \mathrm{GL}_2(K)$ et $M \in V$.

iii) Le morphisme est induit par l'action précédente, qui est bien linéaire. Explicitement, on voit que dans la base donnée en d)i), on a :

$$\rho\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \frac{1}{ad - bc} \begin{pmatrix} a^2 & -b^2 & -2ab \\ -c^2 & d^2 & 2cd \\ -ac & bd & ad + bc \end{pmatrix}.$$

iv) La formule explicite de la question d)iii) assure que $\mathrm{Ker}(\rho) = K^* I_2$.

v) C'est un calcul avec la formule de la question d)iii).

vi) Soit $A = \begin{pmatrix} z & x \\ y & -z \end{pmatrix} \in V$. Alors $\det(A) = -z^2 - xy$ est clairement une forme quadratique non dégénérée (de rang 3) sur V.

vii) Les questions d)iii), d)iv), d)v), et le fait que l'action considérée préserve le déterminant sur V, assurent que le morphisme ρ induit un morphisme de groupes injectif

$$\overline{\rho} : \mathrm{PGL}_2(K) \hookrightarrow \mathrm{SO}(V, \det) \cong \mathrm{SO}_3(K).$$

En calculant les cardinaux des deux groupes, on voit que ceux-ci ont tous les deux pour cardinal $q(q-1)(q+1)$, donc $\overline{\rho}$ est un isomorphisme de groupes.

viii) Comme V est de dimension impaire, on voit que $-\mathrm{id}_V \in \mathrm{O}(V,\det) \setminus \mathrm{SO}(V,\det)$, ce qui permet d'obtenir l'isomorphisme $\mathrm{O}_3(K) \cong \mathrm{SO}_3(K) \times \{\pm I_3\}$. On conclut en utilisant la question d)viii).

ix) Avec les questions précédentes, il suffit de dire que le groupe de dérivé de $\mathrm{GL}_2(K)$ est $\mathrm{SL}_2(K)$ pour conclure que $\Omega_3(K) \cong \mathrm{PSL}_2(K)$. Enfin, le centre de $\mathrm{PSL}_2(K)$ est trivial, ce qui assure que $\mathrm{P}\Omega_3(K) \cong \mathrm{PSL}_2(K)$.

e) i) Soit $M = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in W$. On a $\det(M) = xt - yz$, donc on voit que $Q = \det$ est une forme quadratique sur W qui est somme de deux plans hyperboliques : les plans $\{x = t = 0\}$ et $\{y = z = 0\}$.

ii) Pour tout $(A, B) \in \mathrm{GL}_2(K) \times \mathrm{GL}_2(K)$ et tout $M \in W$, on pose $(A, B) \cdot M := AMB^{-1}$. Cela définit bien une action de groupe.

iii) Soient $(A, B) \in \mathrm{GL}_2(K) \times \mathrm{GL}_2(K)$ et $M \in W$. On a $Q((A, B) \cdot M) = \det(A) \det(B)^{-1} Q(M)$. Donc (A, B) préserve Q si et seulement si $\det(A) = \det(B)$.

En outre, (A, B) agit trivialement sur W si et seulement si pour tout $M \in W$, on a $AM = MB$ si et seulement si $A = B$ et pour tout $M \in W$, $AM = MA$ si et seulement si $A = B$ et $A \in Z(\mathrm{GL}_2(K)) = K^* I_2$.

iv) On note G le sous-groupe de $\mathrm{GL}_2(K) \times \mathrm{GL}_2(K)$ formé des couples de matrices $(A, B) \in \mathrm{GL}_2(K) \times \mathrm{GL}_2(K)$ tels que $\det A = \det B$. On dispose d'une action de K^* sur $\mathrm{SL}_2(K)$ donnée par une section de la suite exacte

$$A \to \mathrm{SL}_2(K) \to \mathrm{GL}_2(K) \xrightarrow{\det} K^* \to 1\,.$$

Par exemple, on peut considérer l'action donnée par $\lambda \cdot A := \mathrm{diag}(\lambda, 1) A \mathrm{diag}(\lambda^{-1}, 1)$, pour tout $\lambda \in K^*$ et $A \in \mathrm{SL}_2(K)$. Pour simplifier, on notera $s(\lambda) := \mathrm{diag}(\lambda, 1)$.

On en déduit une action diagonale de K^* sur $\mathrm{SL}_2(K) \times \mathrm{SL}_2(K)$, ce qui permet de définir un produit semi-direct $(\mathrm{SL}_2(K) \times \mathrm{SL}_2(K)) \rtimes K^*$. On voit facilement que l'on a un isomorphisme naturel $G \cong (\mathrm{SL}_2(K) \times \mathrm{SL}_2(K)) \rtimes K^*$. Considérons alors le morphisme de groupes $\varphi : G \to \mathrm{O}(W, Q)$ défini par $\varphi(A, B) : M \mapsto AMB^{-1}$.

Alors la question e)iii) assure que $\mathrm{Ker}(\varphi) = \cong K^*$, donc φ induit un morphisme de groupes injectif $i = \overline{\varphi} : G/K^* \to \mathrm{O}(W, Q)$.

v) Un calcul simple (utilisant par exemple le produit de Kronecker des matrices, i.e. le produit tensoriel des matrices) assure que le déterminant de $\varphi(A, B)$ vaut $\det(A)^2 \det(B)^{-2} = 1$. Donc φ est à valeur dans $\mathrm{SO}(W, Q)$. On a donc un morphisme de groupes injectif $i = \overline{\varphi} : G/K^* \to \mathrm{SO}(W, Q)$, et on voit que $T \in \mathrm{O}(W, Q) \setminus \mathrm{SO}(W, Q)$. Donc $\langle \mathrm{Im}\,(i), T \rangle \subset \mathrm{O}(W, Q)$.

On calcule alors les cardinaux des groupes en question (en utilisant notamment l'exercice 3) : on a $|G/K^*| = |\mathrm{SL}_2(K)|^2 = q^2(q-1)^2(q+1)^2$, $|\mathrm{SO}(W, Q)| = |\mathrm{SO}_4^+(K)| = q^2(q^2-1)(q^2-1)$, donc l'égalité des cardinaux assure que $i : G/K^* \to \mathrm{SO}(W, Q)$ est un isomorphisme.

Or $\mathrm{SO}(W, Q)$ est un sous-groupe d'indice 2 dans $\mathrm{O}(W, Q)$, donc $\langle \mathrm{Im}\,(i), T \rangle = \mathrm{O}(W, Q)$.

vi) La question précédente assure que $\Omega_4^+(K) \cong D((\mathrm{SL}_2(K) \times \mathrm{SL}_2(K))/K^*$, donc si $|K| > 3$, on a $\Omega_4^+(K) \cong (\mathrm{SL}_2(K) \times \mathrm{SL}_2(K))/K^*$. On en déduit alors $\mathrm{P}\Omega_4^+(K) \cong \mathrm{PSL}_2(K) \times \mathrm{PSL}_2(K)$ si $|K| > 3$.

vii) On a vu que $\mathrm{SO}_4^+(\mathbb{F}_3) \cong G/K^*$. Comme $D(\mathrm{SL}_2(\mathbb{F}_3)) \subset \mathrm{SL}_2(\mathbb{F}_3)$ est isomorphe au groupe $\mathbf{H}_8$ des quaternions d'ordre 8 (voir par exemple TD4, exercice 10), et comme $D(\mathrm{GL}_2(\mathbb{F}_3)) = \mathrm{SL}_2(\mathbb{F}_3)$, on constate que $\Omega_4^+(\mathbb{F}_3) \cong (\mathrm{SL}_2(\mathbb{F}_3) \times \mathrm{SL}_2(\mathbb{F}_3))/\mathbb{F}_3^*$, donc $\mathrm{P}\Omega_4^+(\mathbb{F}_3) \cong \mathrm{PSL}_2(\mathbb{F}_3) \times \mathrm{PSL}_2(\mathbb{F}_3)$.

Exercice 8 :

On considère $V = \mathbb{F}_2^6$ muni de la forme bilinéaire $x \cdot y = \sum_{i=1}^6 x_i y_i$. On note $x_0 := (1, \ldots, 1) \in V$.

a) Donner la définition des groupes $\mathrm{Sp}_n(K)$ lorsque K est un corps de caractéristique 2.

b) Montrer que $W := x_0^\perp / \mathbb{F}_2 x_0$ est naturellement muni d'une forme bilinéaire alternée non dégénérée.

c) En déduire un morphisme naturel $\mathfrak{S}_6 \to \mathrm{Sp}_4(\mathbb{F}_2)$.

d) Conclure que $\mathrm{Sp}_4(\mathbb{F}_2) \cong \mathfrak{S}_6$.

Solution de l'exercice 8.

a) voir le cours.

b) Pour tout $x \in V$, on a $x \cdot x = x \cdot x_0$. Donc pour tout $x \in x_0^\perp$, $x \cdot x = 0$. Cela assure que la restriction de la forme bilinéaire au sous-espace $x_0^\perp$ de dimension 5 est une forme bilinéaire alternée. Son noyau est exactement la droite engendré par x_0, donc cette forme alternée induit une forme alternée b non dégénérée sur $W = x_0^\perp/\mathbb{F}_2 x_0$.

c) L'action de $\mathfrak{S}_6$ sur V par permutation des coordonnées induit une action de $\mathfrak{S}_6$ sur W, dont on voit facilement qu'elle préserve la forme symplectique précédente. On en déduit donc un morphisme de groupes injectif $\mathfrak{S}_6 \to \mathrm{Sp}(W, b) \cong \mathrm{Sp}_4(\mathbb{F}_2)$.

d) On calcule les cardinaux et on voit que $|\mathfrak{S}_6| = 6! = 720$ et $|\mathrm{Sp}_4(\mathbb{F}_2)| = 15.8.3.2 = 720$ (le cardinal des groupes $\mathrm{Sp}2n(\mathbb{F}_q)$ se calcule de façon analogue à celui des groupes orthogonaux : cf exercice 3). On en déduit donc que le morphisme de la question précédente est un isomorphisme, i.e. $\mathrm{Sp}_4(\mathbb{F}_2) \cong \mathfrak{S}_6$.

Exercice 9 : $\star\star\star$

Soit K un corps de caractéristique différente de 2 et soit $m \geq 3$. On munit $V = K^{2m}$ de la forme bilinéaire alternée usuelle B ; on note $\mathrm{Sp}_{2m}(K)$ le groupe symplectique correspondant. Soient $s, t \in \mathrm{Sp}_{2m}(K)$ des involutions.

a) Montrer qu'il existe une décomposition $V = E_+(s) \overset{\perp}{\oplus} E_-(s)$, où $E_+(s)$ et $E_-(s)$ désignent les espaces propres de s associées aux valeurs propres 1 et -1, respectivement.

b) En déduire une bijection entre l'ensemble des involutions de $\mathrm{Sp}_{2m}(K)$ et l'ensemble des sous-espaces non dégénérés de V.

On dit que l'involution s est de type $(2r, 2m-2r)$ si l'espace $E_+(s)$ est de dimension $2r$. On parle d'*involution extrémale* pour une involution de type $(2, 2m-2)$ ou $(2m-2, 2)$. Dans ce cas-là, on note $E_2(s)$ l'espace $E_\pm(s)$ de dimension 2.

c) En considérant les familles commutatives maximales d'involutions conjuguées dans $\mathrm{Sp}_{2m}(K)$, montrer que tout automorphisme de $\mathrm{Sp}_{2m}(K)$ envoie une involution extrémale sur une involution extrémale.

On dit que des involutions extrémales s et t forment un *couple minimal* si on a $\dim(E_2(s) \cap E_2(t)) = 1$. Si $\mathcal{S} \subseteq \mathrm{Sp}_{2m}(K)$ est un ensemble d'involutions extrémales, on note $C(\mathcal{S})$ l'ensemble des involutions extrémales qui commutent à tout élément de $\mathcal{S}$.

d) Montrer que s et t forment un couple minimal si et seulement si ($st \neq ts$ et pour tous $s', t' \in C(C(\{s,t\}))$ avec $s't' \neq t's'$ on a $C(C(\{s,t\})) = C(C(\{s',t'\}))$).

e) Déterminer les ensembles maximaux I d'involutions extrémales tels que toute paire d'éléments de I forme un couple minimal ou commute.

Soit $n \geq 3$. Une application $\phi : K^n \to K^n$ est dite semi-linéaire s'il existe un automorphisme de corps $\theta : K \to K$ tel que ϕ soit θ-linéaire, c'est-à-dire :

- On a $\phi(v + v') = \phi(v) + \phi(v')$, pour tous $v, v' \in K^n$.
- On a $\phi(\lambda v) = \theta(\lambda)\phi(v)$, pour tout $v' \in K^n$ et tout $\lambda \in K$.

L'ensemble des applications semi-linéaires inversibles forment un groupe, noté $\Gamma\mathrm{L}_n(K)$ et appelé le groupe des transformations semi-linéaires de K^n.

On admet le théorème fondamental de la géométrie projective, qui est l'énoncé suivant : *soit* $\phi : \mathbb{P}^n(K) \to \mathbb{P}^n(K)$ *une bijection telle que trois points* A_1, A_2, A_3 *de* $\mathbb{P}^n(K)$ *sont alignés si et seulement si* $\phi(A_1), \phi(A_2), \phi(A_3)$ *le sont. Alors il existe un automorphisme de corps* $\sigma : K \to K$ *et une transformation* σ*-linéaire* $\gamma \in \Gamma\mathrm{L}_{n+1}(K)$ *telle que* ϕ *soit induite par* γ.

On définit enfin $\Gamma\mathrm{Sp}_{2m}(K)$ comme le sous-groupe de $\Gamma\mathrm{L}_{2m}(K)$ des éléments préservant la forme B.

f) Montrer que tout automorphisme de $\mathrm{Sp}_{2m}(K)$ est de la forme $x \mapsto axa^{-1}$ pour un certain élément $a \in \Gamma\mathrm{Sp}_{2m}(K)$.

Solution de l'exercice 9.

a) Une involution annule le polynôme $X^2 - 1$, d'où une décomposition $V = E_+(s) \oplus E_-(s)$. Cette dernière est B-orthogonale puisque si e_+ et e_- sont des éléments respectivement de $E_+(s)$ et $E_-(s)$, alors on a

$$-B(e_+, e_-) = B(s(e_+), s(e_-)) = B(e_+, e_-)\,,$$

donc $B(e_+, e_-) = 0$.

b) L'application $s \mapsto E_+(s)$ est la bijection souhaitée.

c) Soit $\mathcal{F}$ une telle famille. Elle est composée d'involutions de type $(2r, 2m-2r)$ pour un r fixé (puisque les éléments de $\mathcal{F}$ sont conjugués). Comme ils commutent, tous les éléments de $\mathcal{F}$ se diagonalisent dans une base symplectique commune. Aussi, il convient de remarquer que si V a pour base symplectique $(e_1, e_2, \ldots, e_{2m})$ avec $b(e_{2i-1}, e_{2i}) = -b(e_{2i}, e_{2i-1}) = 1$, et $b(e_i, e_j) = 0$ sinon, alors on a $e_{2j} \in E_+(s) \Leftrightarrow e_{2j-1} \in E_+(s)$. De ce fait, $E_+(s)$ est déterminé par un choix de r vecteurs, et on a $|\mathcal{F}| \leq \binom{m}{r}$.
En particulier si s est une involution extrémale, alors elle est incluse dans une famille maximale, à m éléments, d'involutions conjuguées commutant deux-à-deux. Parce que cette dernière propriété est conservée par un automorphisme de $\mathrm{Sp}_{2m}(K)$ et parce que l'on a $\binom{m}{r} \neq m$ pour $r \notin \{1, m-1\}$, tout automorphisme de $\mathrm{Sp}_{2m}(K)$ envoie involutions extrémales sur involutions extrémales.

d) Si s et t sont deux involutions extrémales avec $s \neq \pm t$, on a

$$C(\{s,t\}) = \{u \text{ extrémale} \mid E_2(u) \subseteq E_{2m-2}(s) \cap E_{2m-2}(t),\ E_{2m-2}(u) \supseteq E_2(s) + E_2(t)\}.$$

On en déduit

$$C(C(\{s,t\})) = \{u \text{ extrémale} \mid E_2(u) \subseteq E_2(s) + E_2(t),\ E_{2m-2}(u) \supseteq E_{2m-2}(s) \cap E_{2m-2}(t)\}.$$

Si s et t forment un couple minimal, alors on a $st \neq ts$ puisqu'on a $\dim(E_2(t) \cap E_2(s)) = 1$ non paire. De plus, si $s', t' \in C(C(\{s,t\}))$ vérifient $s't' \neq t's'$, alors $E_2(s') + E_2(t') \subseteq E_2(s) + E_2(t)$, qui est de dimension 3. Ainsi on a $\dim(E_2(s') \cap E_2(t')) = 1$ et (s', t') est un autre couple minimal avec $E_2(s') + E_2(t') = E_2(s) + E_2(t)$. Il s'ensuit $E_{2m-2}(s') \cap E_{2m-2}(t') = E_{2m-2}(s) \cap E_{2m-2}(t)$ et $C(C(\{s', t'\})) = C(C(\{s,t\}))$.
Si s et t ne sont pas un couple minimal, alors on a $\dim(E_2(s) \cap E_2(t)) \in \{0, 2\}$. Dans le cas où cette dimension vaut 2, la question (b) donne $s = \pm t$ et on a alors $st = ts$. Supposons donc $E_2(s) \cap E_2(t) = \emptyset$. Dans ce cas-là, $E_2(s) + E_2(t)$ est de dimension 4, et on peut trouver s' et t' un couple minimal avec $E_2(s') + E_2(t') \subsetneqq E_2(s) + E_2(t)$ et $E_{2m-2}(s') \cap E_{2m-2}(t') \supsetneqq E_{2m-2}(s) \cap E_{2m-2}(t)$. On a alors $C(C(\{s', t'\})) \neq C(C(\{s,t\}))$.

e) Si $\pm s, \pm t, \pm u$ sont six éléments distincts de I, l'espace $E_2(s) \cap E_2(t) \cap E_2(u)$ est de dimension 1 ou 0. Dans le premier cas, on note V_1 la droite obtenue et dans le second cas, on a $E_2(u) \subseteq E_2(s) + E_2(t) =: V_3$. Les ensembles maximaux correspondants sont alors respectivement

$$I_1(V_1) := \{v \text{ involution extrémale} \mid V_1 \subseteq E_2(v)\},$$

$$I_3(V_3) := \{v \text{ involution extrémale} \mid E_2(v) \subseteq V_3\}.$$

Et tous les ensembles maximaux I sont de l'un de ces deux types.

f) Si V_3 est de dimension 3, on peut trouver $V_4 \supseteq V_3$ de dimension 4 et non isotrope. Alors si w est une involution extrémale avec $V_4 \subseteq E_{2m-2}(w)$, tout élément v de $I_3(V_3)$ vérifie $E_2(v) \subseteq E_{2m-2}(w)$ et $E_2(w) \subseteq V_4^\perp \subseteq E_{2m-2}(v)$. De ce fait, w commute avec tout élément de $I_3(V_3)$. Or il n'existe pas d'élément non trivial de $\mathrm{Sp}_{2m}(K)$ commutant avec tout élément de $I_1(V_1)$. On en déduit que tout automorphisme de $\mathrm{Sp}_{2m}(K)$ préserve $\{I_1(x) \mid x \in \mathbb{P}^{2m-1}(K)\}$.
Soit ϕ un automorphisme de $\mathrm{Sp}_{2m}(K)$. On lui associe la bijection $\theta_\phi : \mathbb{P}^{2m-1}(K) \to \mathbb{P}^{2m-1}(K)$

via $\phi(I_1(x)) = I_1(\theta_\phi x)$. Maintenant, $x, y \in \mathbb{P}^{2m-1}(K)$ sont deux droites orthogonales si et seulement si elles engendrent un plan anisotrope ; ceci est encore équivalent à $I(x) \cap I(y) = \emptyset$. Cette dernière propriété est conservée par ϕ, de sorte que θ_ϕ préserve l'orthogonalité. On en déduit que θ_ϕ préserve l'alignement, et par le théorème fondamental de la géométrie projective, il existe $a \in \Gamma\mathrm{L}_{2m}(K)$ tel que l'on ait $\theta_\phi(Kx) = K(ax)$ pour tout $x \in K^{2m} \smallsetminus \{0\}$. Comme a préserve l'orthogonalité, on a même $a \in \Gamma\mathrm{Sp}_{2m}(K)$. Si s est une involution extrémale, on a $\{s\} = I_1(e_1) \cap I_1(e_2)$ si e_1 et e_2 sont deux droites engendrant $E_2(s)$. On en déduit que $\phi(s) = asa^{-1}$. Si g est un élément de $\mathrm{Sp}_{2m}(K)$, gsg^{-1} est une involution extrémale et on a

$$agsg^{-1}a^{-1} = \phi(gsg^{-1}) = \phi(g)\phi(s)\phi(g)^{-1} = \phi(g)asa^{-1}\phi(g)^{-1}.$$

Ceci s'écrit encore $g^{-1}a^{-1}\phi(g)as = sg^{-1}a^{-1}\phi(g)a$; autrement dit, $g^{-1}a^{-1}\phi(g)a$ commute à toute involution extrémale et préserve donc tout plan hyperbolique. Il s'ensuit que $g^{-1}a^{-1}\phi(g)a$ préserve les droites et est donc une homothétie, disons $\lambda(g)I_{2m}$. Mais alors, $g \mapsto \lambda(g)$ fournit un morphisme $\mathrm{Sp}_{2m}(K) \to K^\times$. Par simplicité de $\mathrm{PSp}_{2m}(K)$, le noyau de ce dernier est $\{1\}$, $Z(\mathrm{Sp}_{2m}(K))$ ou $\mathrm{Sp}_{2m}(K)$. Les deux premiers cas ne permettent pas de factoriser λ par l'abélianisé ; c'est donc le dernier cas qui se présente, et λ est trivial.